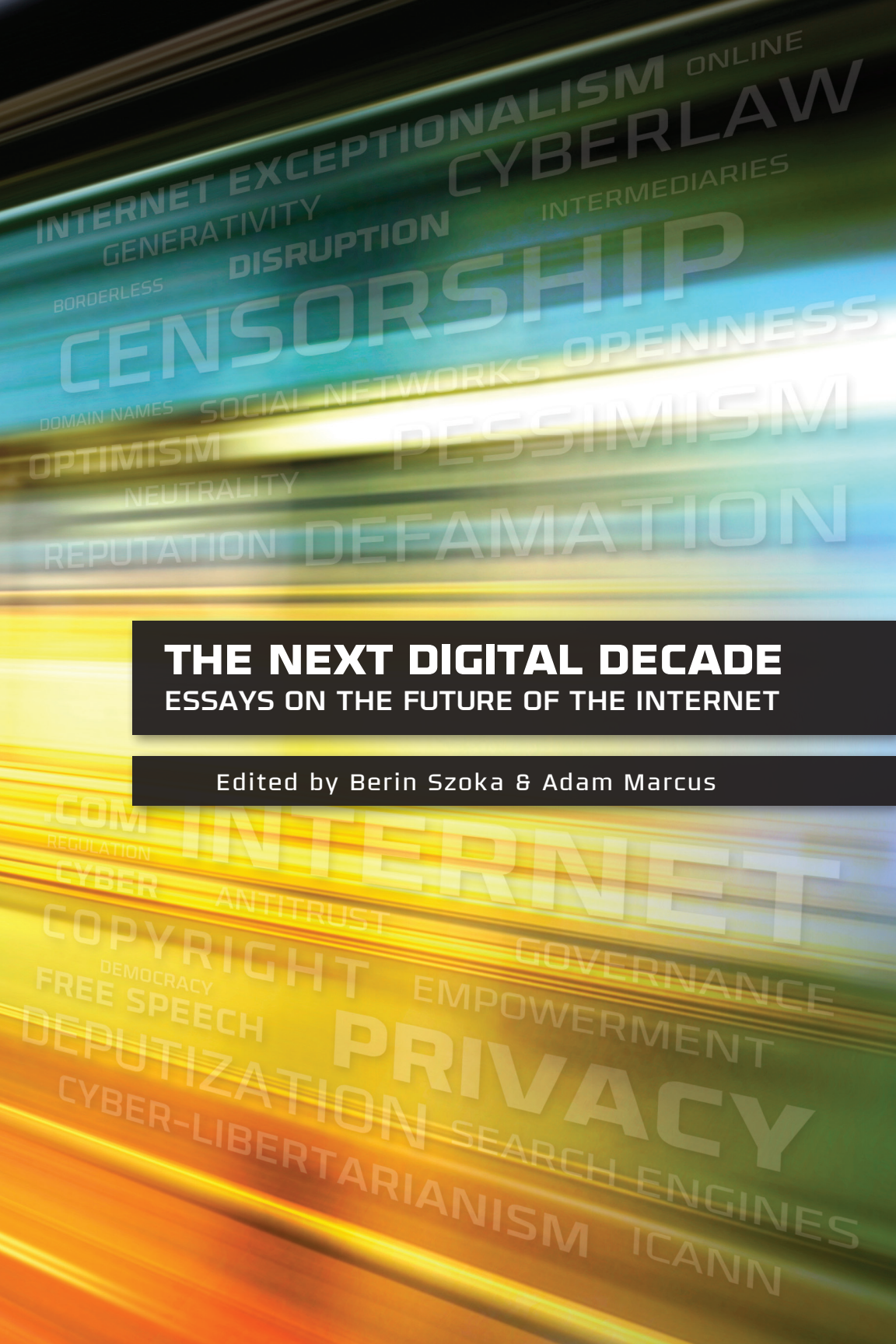



# THE NEXT DIGITAL DECADE

## ESSAYS ON THE FUTURE OF THE INTERNET

Edited by Berin Szoka & Adam Marcus

# THE NEXT DIGITAL DECADE

## ESSAYS ON THE FUTURE OF THE INTERNET

Edited by Berin Szoka & Adam Marcus

# TECH FREEDOM

NextDigitalDecade.com

TechFreedom
techfreedom.org
Washington, D.C.

This work was published by TechFreedom (**TechFreedom.org**), a non-profit public policy think tank based in Washington, D.C. TechFreedom's mission is to unleash the progress of technology that improves the human condition and expands individual capacity to choose. We gratefully acknowledge the generous and unconditional support for this project provided by VeriSign, Inc.

More information about this book is available at **NextDigitalDecade.com**

ISBN 978-1-4357-6786-7



Cover Designed by Jeff Fielding.

# TABLE OF CONTENTS

# Foreword

## Berin Szoka

This book is both a beginning and an end. Its publication marks the beginning of TechFreedom, a new non-profit think tank that will launch alongside this book in January 2011. Our mission is simple: to unleash the progress of technology that improves the human condition and expands individual capacity to choose. This book also marks an end, having been conceived while I was Director of the Center for Internet Freedom at The Progress & Freedom Foundation—before PFF ceased operations in October 2010, after seventeen years.

Yet this book is just as much a continuation of the theme behind both PFF and TechFreedom: "progress *as* freedom." As the historian Robert Nisbet so elegantly put it: "the condition as well as the ultimate purpose of progress is the greatest possible degree of freedom of the individual."[1] This book's twenty-six contributors explore this theme and its interaction with relentless technological change from a wide variety of perspectives.

Personally, this book is the perfect synthesis of the themes and topics that set me down the path of studying Internet policy in the late 1990s, and weaves together most of the major books and authors that have influenced the evolution of my own thinking on cyberlaw and policy. I hope this collection of essays will offer students of the field the kind of authoritative survey that would have greatly accelerated my own studies. Even more, I hope this volume excites and inspires those who may someday produce similar scholarship of their own—perhaps to be collected in a similar volume celebrating another major Internet milestone.

I am deeply grateful to Shane Tews, Vice President for Global Public Policy and Government Relations at VeriSign, who first suggested publishing this sort of a collection to commemorate the 25th anniversary of the first .COM domain name (registered in 1985) by asking what the future might bring for the Internet. Just as I hope readers of this book will be, she had been inspired by reading *Who Rules the Net? Internet Governance & Jurisdiction*, a collection of cyberlaw essays edited by Adam Thierer and Clyde Wayne Crews, and published by the Cato Institute in 2003. This book would not exist without the unconditional and generous support of VeriSign, the company that currently operates the .COM registry.

---

1 ROBERT NISBET, HISTORY OF THE IDEA OF PROGRESS 215 (1980).

Nor would the book exist without the superb intellectual contributions and patience of our twenty-six authors, and all those who assisted them. I must also thank PFF Summer Fellows Alexis Zayas, Jeff Levy and Zach Brieg for their invaluable assistance with editing and organization, and Jeff Fielding for the book's stunning cover artwork and design.

Most of all, I must thank Adam Thierer and co-editor Adam Marcus. The two and a half years I spent working closely with them on a wide range of technology policy topics at PFF were the highlight of my career thus far.

I look forward to helping, in some small way, to discover the uncertain future of progress, freedom, and technology in the next digital decade—and beyond.

Berin Szoka
December 16, 2010

# 25 Years After .COM: Ten Questions

## Berin Szoka

While historians quibble over the Internet's birth date, one date stands out as the day the Internet ceased being a niche for a limited number of universities, governments and military organizations, and began its transformation into a medium that would connect billions: On March 15, 1985, Symbolics, a Massachusetts computer company, registered symbolics.com, the Internet's first commercial domain name.[2] This book celebrates that highly "symbolic" anniversary by looking not to the Internet's past, but to its future. We have asked twenty-six thought leaders on Internet law, philosophy, policy and economics to consider what the next digital decade might bring for the Internet and digital policy.

Our ten questions are all essentially variations on the theme at the heart of TechFreedom's mission: Will the Internet, on its own, "improve the human condition and expand individual capacity to choose?" If not, what is required to assure that technological change *does* serve mankind? Do the benefits of government intervention outweigh the risks? Or will digital technology itself make digital markets work better? Indeed, what would "better" mean? Can "We the Netizens," acting through the digital equivalent of what Alexis de Tocqueville called the "intermediate institutions" of "civic society," discipline both the Internet's corporate intermediaries (access providers, hosting providers, payment systems, social networking sites, search engines, and even the Domain Name System operators) and our governments?

Part I focuses on five "Big Picture & New Frameworks" questions:

1. Has the Internet been good for our culture and society?
2. Is the open Internet at risk from the drive to build more secure, but less "generative" systems and devices? Will the Internet ultimately hinder innovation absent government intervention?
3. Is the Internet really so exceptional after all, or will—and should—the Internet be regulated more like traditional communications media?
4. To focus on one aspect of the Internet exceptionalism, has the Internet fundamentally changed economics? What benefits and risks does this change create?
5. Who—and what ideas—will govern the Net in 2020—at the end of the next digital decade?

---

[2] John C Abell, *Dot-Com Revolution Starts With a Whimper*, WIRED MAGAZINE, March 15, 2010, **http://www.wired.com/thisdayintech/2010/03/0315-symbolics-first-dotcom/**

Part II tackles five "Issues & Applications" questions:

6. Should intermediaries be required to police more—or be disciplined in *how* they police their networks, systems and services? Whether one thinks the Internet is truly exceptional, and whether it has changed economics largely determines one's answer to these questions.
7. While debates about the role of online intermediaries and the adequacy of their self-regulation focused on net neutrality in the last digital decade, the battle over "search neutrality" may be just as heated in the next digital decade. Are search engines now the "essential facilities" of the speech industry that can be tamed only by regulation? Or are they engines of empowerment that will address the very concerns they raise by ongoing innovation?
8. As the Internet accelerates the flow of information, what future is there for privacy, both from governments and private companies? Is privacy a right? How should it be protected—from both government and private companies?
9. The book concludes with two Chapters regarding the Internet in a borderless world. The first focuses on governments' regulation of speech.
10. The second focuses on the potential for governments' "disruption" *by* speech—by unfettered communication and collaboration among the citizenry. In both cases, our authors explore the consequences—and limits—of the Internet's empowerment of users for democracy, dissent and pluralism.

# Part I: Big Picture & New Frameworks

## The Internet's Impact on Culture & Society: Good or Bad?

Andrew Keen, the self-declared "Anti-Christ of Silicon Valley"[3] is scathing in his criticism of the Internet, especially "Web 2.0." Keen declares we must avoid the siren song of "democratized media," citizen journalism, and, as the title of his first book puts it, the *Cult of the Amateur*. He laments the "technology that arms every citizen with the means to be an opinionated artist or writer" as producing a techno-utopian delusion little different from Karl Marx's fantasies of a communist society—"where nobody has one exclusive sphere of activity but each can become accomplished in any branch he wishes."

Keen recognizes the reality of Moore's Law—the doubling of computing capability every two years—but refuses to accept the idea that "each advance in

---

[3] Tim Dowling, *I don't think bloggers read*, THE GUARDIAN, July 20, 2007, **http://www.guardian.co.uk/technology/2007/jul/20/computingandthenet.books**

technology is accompanied by an equivalent improvement in the condition of man." Information technology is leading us into an oblivion of cultural amnesia, narcissism, and a childish rejection of the expertise, wisdom and quality of creative elites. For Keen, a "flatter" world is one in which genius can no longer rise above a sea of mediocrity, noise and triviality. His message on the verge of the next digital decade might as well be: "Abandon all hope, ye who enter here!" Keen's pessimism is as strident as a certain Pollyannaish utopianism on the other side.

Is there a middle ground? Adam Thierer, Senior Research Fellow at George Mason University's Mercatus Center, insists there must be. In two related essays, Thierer describes two schools of Internet pessimism: net skeptics generally pessimistic about technology and "net lovers" who think the "good ol' days" of the Internet were truly great but are nonetheless pessimistic about the future. This first essay responds to Net skeptics like Keen—putting him in the context of centuries of techno-pessimism, beginning with the tale from Plato's *Phaedrus* of Theuth and Thamus. Thierer's response is Pragmatic Optimism: "We should embrace the amazing technological changes at work in today's Information Age but with a healthy dose of humility and appreciation for the disruptive impact and pace of that change. We need to think about how to mitigate the negative impacts associated with technological change without adopting the paranoid tone or Luddite-ish recommendations of the pessimists."

## Is the Generative Internet at Risk?

Harvard Law Professor Jonathan Zittrain summarizes the themes from his influential 2008 book, *The Future of the Internet—And How to Stop It*. Zittrain is Thierer's prototypical Net-loving pessimist who worries how technology will evolve absent intervention by those capable of steering technology in better directions. Zittrain worries that consumer demand for security will drive the developers and operators of computer networks, services and devices to reduce what he calls the "generativity" of their offerings. Thus, unregulated markets will tend to produce closed systems that limit experimentation, creativity and innovation. In particular, Zittrain decries the trend towards "appliancized" devices and services—which, unlike the traditional personal computer, can load only those applications or media authorized by the developer. Not only does this diminish user control in the immediate sense, greater "regulability" also creates the potential for the Internet's "gatekeepers" to abuse their power. Thus, Zittrain echoes the prediction made by Larry Lessig in *Code*—without a doubt the most influential Internet policy book ever—that "Left to itself, cyberspace will become a perfect tool of control."[4]

---

[4] Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE 5-6 (1999).

In the end, he proposes essentially two kinds of solutions for "Protecting the Internet without Wrecking It." The first is essentially an appeal to the civic virtues of "netizenship." Second, regulation may be required to force companies to "provide basic tools of transparency that empower users to understand exactly what their machines are doing," as well as "data portability policies." More radically, he proposes to impose liability on device manufacturers who do not respond to takedown requests regarding vulnerabilities in their code that could harm users. And, returning to his core fear of appliancized devices, he proposes that "network neutrality-style mandates" be imposed on "that subset of appliancized systems that seeks to gain the generative benefits of third-party contribution at one point in time while reserving the right to exclude it later."

Ann Bartow, Professor at the University of South Carolina School of Law, offers a stinging rebuke of Zittrain's *The Future of the Internet*. She summarizes the book as follows: "We have to regulate the Internet to preserve its open, unregulated nature." Her essay draws an analogy to James Joyce's 1916 novel, *A Portrait of the Artist as a Young Man*—emphasizing Zittrain's desire for the independence of his digital homeland, much as Joyce wrote about Ireland. But as a leading cyber-feminist, she is especially critical of what she characterizes as Zittrain's call for "an elite circle of people with computer skills and free time who share his policy perspective" to rule his preferred future (which she calls the "Zittrainet") as "Overlords of Good Faith."

As Bartow characterizes Zittrain's philosophy, "The technologies should be generative, but also monitored to ensure that generativity is not abused by either the government or by scoundrels; elite Internet users with, as one might say today, 'mad programming skilz' should be the supervisors of the Internet, scrutinizing new technological developments and establishing and modeling productive social norms online; and average, non–technically proficient Internet users should follow these norms, and should not demand security measures that unduly burden generativity." In the end, she finds Zittrain's book lacking in clear definitions of "generativity" and in specific proposals for "how to avoid a bad future for people whose interests may not be recognized or addressed by what is likely to be a very homogeneous group of elites" composed primary by male elites like Zittrain.

Like Bartow, Adam Thierer rejects Zittrain's call for rule by a Platonic elite of philosopher/programmer kings in the "Case for Internet Optimism, Part 2: Saving the Net from Its *Supporters*." Thierer connects the work of Larry Lessig, Jonathan Zittrain and Tim Wu as the dominant forces in cyberlaw, all united by an over-riding fear: "The wide-open Internet experience of the past decade is giving way to a new regime of corporate control, closed platforms, and walled gardens." Thierer argues that they overstate the threats to openness and

generativity. Because "companies have strong incentives to strike the right openness/closedness balance…. things are getting more open all the time anyway, even though the Internet was never quite so open or generative as the "Openness Evangelicals" imagine. In the end, he concludes it is "significantly more likely that the [regulated] 'openness' they advocate will devolve into expanded government control of cyberspace and digital systems than that unregulated systems will, as the Openness Evangelicals fear, become subject to 'perfect control' by the private sector." Thus, Thierer rejects what Virginia Postrel called, in her 1998 book *The Future and its Enemies*, the "stasis mentality."[5] Instead, he embraces Postrel's evolutionary dynamism: "the continuum [between openness and closedness] is constantly evolving and … this evolution is taking place at a much faster clip in this arena than it does in other markets." In the end, he argues for the freedom to experiment—a recurring theme of this collection.

## Is Internet Exceptionalism Dead?

Eric Goldman, professor at Santa Clara University School of Law, provides a three-part historical framework for understanding the Internet Exceptionalism debate. In the mid-1990s, Internet Utopianism reigned triumphant, exemplified in the 1996 "Declaration of the Independence of Cyberspace" by John Perry Barlow, lyricist for the Grateful Dead.[6] Despite its radicalism, this First Wave of Internet Exceptionalism succeeded in getting Congress to add the only section of the Communications Decency Act that would survive when the Supreme Court struck down the rest of the Act on First Amendment grounds: Section 230, which "categorically immunizes online providers from liability for publishing most types of third party content" and thus "is clearly exceptionalist because it treats online providers more favorably than offline publishers—even when they publish identical content." That law lies at the heart of the philosophical debate in this Chapter and Chapter 6: "Should Online Intermediaries Be Required to Police More?" The Second Wave ("Internet Paranoia") led regulators to treat the Internet more harshly than analogous offline activity. The Third Wave ("Exceptionalism Proliferation") proposed laws treating specific sites and services differently, especially social networks.

The Deadhead Barlow was dead wrong, declare—essentially—the Hon. Alex Kozinski, Chief Judge of the Ninth Circuit Court of Appeals, and Josh Goldfoot, Department of Justice litigator—each writing only in their private capacity—in "A Declaration of the *Dependence* of Cyberspace." While they agree

---

5 VIRGINIA POSTREL, THE FUTURE AND ITS ENEMIES (1998).

6 Declaration of John P. Barlow, Cognitive Dissident, Co-Founder, Elec. Frontier Found., *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), *available at* **http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration**.

that online anonymity and long-distance communications indeed make it harder for governments to punish law-breakers, governments are not helpless: "By placing pressure on [intermediaries like hosting companies, banks and credit card companies] to cut off service to customers who break the law, we can indirectly place pressure on Internet wrong-doers." They illustrate their point with the examples of secondary liability for copyright infringement and Judge Kozinski's *Roommates.com* decision. Indeed. they reject "the conceit that [cyberspace] exists at all" as a distinct, let alone exceptional place, as well as arguments that the costs to Internet companies of handling traditional regulations are too high.

Columbia Law Professor Tim Wu concurs that governments can, and do, regulate the Internet because of what he and Jack Goldsmith called, in their 2006 book *Who Controls the Internet?*, the "persistence of physicality." This is not necessarily something to be celebrated, as he notes, pointing to China's very innovativeness in finding ways to repress its citizens online—a subject addressed in this collection's final Chapter. Another of Thierer's "Net-Loving Pessimists," Wu professes Internet optimism but insists we must be "realistic about the role of government."

Wu summarizes the lengthy account in his 2010 book *The Master Switch* of how government is both responsible for creating information monopolists and yet also the only force ultimately capable of dethroning them. For Wu, the Internet is *not* exceptional—from "The Cycle" of alternation between centralization/closedness and decentralization/openness. Yet Wu agrees the Internet is indeed an exception to the general trend of traditional media: "[t]echnologically, and in its effects on business, culture and politics." Thus, he compares the "ideology as expressed in its technology" and the American exceptionalism of Alexis de Tocqueville. Yet such exceptionalism, Wu warns, "cannot be assumed, but must be defended." Wu closes with a very useful bibliography of leading works in this ongoing debate.

H. Brian Holland, Professor at Texas Wesleyan School of Law, responds with a full-bore defense of what he calls the "modified Internet Exceptionalism" encapsulated in Section 230—"modified" to be less audacious than Goldman's First Wave ("the Internet is inherently unregulable"), but still bold in its insistence that granting broad immunity to online intermediaries for the conduct of their users is vital to the flourishing of "cyber-libertarian" Web 2.0 communities—such as wikis and social networks, capable of evolving their own norms and enforcement mechanisms for policing behavior. Holland provides a history of Section 230 and the debate over Internet exceptionalism that frames the discussion of intermediary deputization in Chapter 6. He explains how Larry Lessig's conviction that private power leads to perfect control, as mentioned above, ultimately split the Internet Exceptionalist consensus against

regulation of the 1990s into two camps. Both camps carried the banner of Internet freedom but reached opposite conclusions about whether the real threat comes from government or the private sector—most notably, regarding Net Neutrality. Despite this fracturing, Holland notes that the exceptional deregulation made possible by Section 230 has grown, not contracted, in its interpretation by the courts since 1996.

Similarly, Mark MacCarthy, Adjunct Professor in the Communications Culture and Technology Program at Georgetown University, explains how "[t]he initial demand from Internet exceptionalists that the online world be left alone by governments has morphed into the idea that governments should create a global framework to protect and spur the growth of the Internet." Once the exaggerated claims about the impossibility of regulating the Net made by First Wave Internet Exceptionalists proved false, the question became not whether "[i]ntermediaries can control illegal behavior on the Internet and governments can control intermediaries, but *should* they?"

Based on his first-hand experience at Visa (described in Chapter 6), MacCarthy seems willing to accept more intermediary deputization than Holland but insists that "[t]he establishment of these laws needs to follow all the rules of good policymaking, including imposing an obligation only when the social benefits exceed the social costs." Furthermore, he warns that "a bordered Internet in which each country attempts to use global intermediaries to enforce its local laws will not scale. This is the fundamentally correct insight of the Internet exceptionalists." Thus, MacCarthy concludes, "If governments are going to use intermediaries to enforce local laws, they are going to have to harmonize the local laws they want intermediaries to enforce."

## Has the Internet Fundamentally Changed Economics?

Google's chief economist Hal Varian provides a coda to the 1998 book *Information Rules: A Strategic Guide to the Network Economy* (with Carl Shapiro of the University of California at Berkeley). That book pioneered the exploration of the unique aspects of information economics, and their implications for both business and policy. Here, Varian argues that the Internet's most underappreciated impact on our economy lies in the obvious yet under-appreciated ubiquity of computers in our economic transactions, facilitating four broad categories of "combinatorial innovation": new forms of contract; data extraction and analysis; controlled experimentation; and personalization and customization. Varian celebrates the transformative potential of cloud computing technology to allow even tiny companies working internationally to launch innovative new applications and services that, in turn, "can serve as

building blocks for new sorts of combinatorial innovation in business processes that will offer a huge boost to knowledge worker productivity in the future."

Harvard Law Professor Yochai Benkler is best known for his book *The Wealth of Networks*—a clear allusion to Adam Smith's 1776 classic *The Wealth of Nations*.[7] Those familiar with this part of Smith's work view him narrowly as an economist focused solely on what has traditionally been characterized as economic exchange. But Smith in fact was equal parts economist, moral philosopher, and jurisprudentialist—and so is Benkler. Benkler's essay, "Decentralization, Freedom to Operate, and Human Sociality," harkens back to Smith's other key work, *The Theory of Moral Sentiments* (1759). For both Smith and Benkler, man's natural sociability means that our distributed interactions tend to benefit society from the bottom-up—as if by Smith's "invisible hand." For Benkler, the Internet is "a global network of communications and exchange that allows much greater flow and conversation, so that many new connections are possible on scales never before seen." Like Varian, Benkler celebrates the potential for cloud computing to facilitate accelerating and unprecedented collaboration.

But the keys to Benkler's future are sociality, voluntarism, widespread experimentation, and the freedom to experiment. The latter insistence makes him highly critical of is intellectual property—copyright, patent, *etc.* Yet he does not address the dangers of propertizing personal data as another form of intellectual property. What does privacy-property mean for data-driven experimentation and the freedom to experiment? This question, unanswered here, offers perhaps the most tantalizing organizing theme for a future successor to this collection of essays.

Larry Downes closes this Chapter with an expanded version of the discussion of digital economics from his 2009 book *The Laws of Disruption*—a book in the same tradition as Varian and Shapiro's *Information Rules* (1998), Postrel's *The Future and its Enemies* (1998), and Clayton Christensen's *The Innovator's Dilemma* (1997). Here, Downes proposes five principles of information economics that make the digital economy different: (1) Renewability: "information cannot be used up"; (2) Universality: "everyone has the ability to use the same information simultaneously;" (3) Magnetism: "Information value grows exponentially as new users absorb it;" (4) Friction-free: "the more easily information flows, the more quickly its value increases;" and (5) Vulnerability: The value of information can be destroyed through misuse or even its own success—information overload.

---

7 ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 18-21 (Edwin Cannan, ed., Methuen & Co., Ltd. 1904) (1776), **http://www.econlib.org/library/Smith/smWN.html**.

For Downes, the Internet has changed economics in a second sense: by relentlessly and ruthlessly cutting transaction costs—*e.g.*, the costs of search, information, bargaining, decision, policing and enforcement. Thus, Varian's computer-mediation promises to dramatically flatten our economy: "As transaction costs in the open market approach zero, so does the size of the firm—if transaction costs are nonexistent, then there is no reason to have large companies"—what Downes calls "The Law of Diminishing Firms."

Downes echoes Postrel's critique of the stasis mentality: "the old rules do little more than hold back innovation for the benefit of those who cannot or do not know how to adapt to the economics of digital life." Like Benkler, Downes particularly worries about copyright law's ability to keep pace, but also explores the implications of lower transactions costs for privacy, asking: "What happens when the cost of deleting information is higher than the cost of retaining it? The answer is that nothing gets deleted." In Chapter 7, both Downes and Stewart Baker explore the costs and benefits of privacy regulation.

Finally, Eric Goldman offers another three-part conceptual framework—this time, for understanding how the Internet has revolutionized markets for reputational information. Goldman argues that "well-functioning marketplaces depend on the vibrant flow of accurate reputational information." The Internet may allow markets to regulate themselves better: If reputational information that was previously "locked in consumers' heads" can flow freely, it can "play an essential role in rewarding good producers and punishing poor ones." Smith's invisible hand alone is not enough, but "reputational information acts like an invisible hand guiding the invisible hand"—the "secondary invisible hand." A "tertiary invisible hand" allows "the reputation system to earn consumer trust as a credible source… or to be drummed out of the market for lack of credibility…."

Goldman cautions against interventions that suppress reputational information, but also highlights the potential unintended consequences of interventions intended to make reputation markets work better—like anti-gaming rules and a right-of-reply. Like Holland, Goldman emphasizes the central importance of Section 230's immunity in allowing reputation systems to flourish without being crushed by intermediary liability or policing obligations.

## Who Will Govern the Net in 2020?

Each of the three authors in this Chapter wisely resists the temptation to make overly specific prophesies and instead considers the broad themes likely to shape the policy debate over the Internet's future. New York School of Law Professor David Johnson and Syracuse Information Studies Professor Milton Mueller focus on who *should* govern the Net in 2020—and could just as easily have responded to our question about Internet Exceptionalism—while Rob

Atkinson, President of the Information Technology and Innovation Foundation, provides a "field guide" to the eight major camps in Internet policy.

Echoing Postrel's dynamist/stasist theme, like Thierer, Mueller predicts "The future of Internet governance will be driven by the clash between its raw technical potential and the desire of various incumbent interests—most notably nation-states—to assert control over that potential]." He hopes the Internet will be governed by a "denationalized liberalism" based on "a universal right to receive and impart information regardless of frontiers, and sees freedom to communicate and exchange information as fundamental, primary elements of human choice and political and social activity." This will require the authority of national and subnational governments must be contained to "domains of law and policy suited to localized or territorialized authority," while Internet governance institutions must be completely detached from nation-state institutions. Defenders of free speech will ultimately have to use global free trade institutions to strike down censorship.

Mueller finds strong grounds for optimism in the Internet's empowering and democratizing nature, and in the rise of new access technologies like unlicensed wireless broadband capable of disrupting existing Internet access bottlenecks. But he worries about the growing technological capabilities of broadband providers to manage and potentially censor traffic on their networks, and admits a darker future of strife, industrial consolidation, censorship and cyber-warfare is possible. Like Zittrain, Mueller fears a splintering of the Internet driven by conflicts over the Internet's "Root Server," and that such conflicts are bound to intensify as the drive to secure the Internet against cyber-threats and cyber-warfare intensifies.

Like Wu, David Johnson, reaches back to Tocqueville's *Democracy in America* (1835). While Mueller proposes a new liberalism, Johnson proposes "Democracy in Cyberspace: Self-Governing Netizens and a New, Global Form of Civic Virtue, Online." Paraphrasing Tocqueville, Johnson argues: "The Internet establishes a new equality of condition and enables us to exercise liberty to form associations to pursue new civic, social, and cultural goals." Thus, the Internet is "inherently democratic"—in ways well beyond politics. But the Internet's nature as an "engine of democratic civic virtue" must be defended daily by "netizens—the global polity of those who collaborate online, seek to use the new affordances of the Internet to improve the world, and care about protecting an Internet architecture that facilitates new forms of civic virtue." Johnson argues against Wu's apparent resignation to some degree of government meddling online: "A world in which every local sovereign seeks to control the activities of netizens beyond its borders violates the true meaning of self-governance and democratic sovereignty." Johnson predicts that technology

will empower users to sidestep the traditional controls imposed by governments—not perfectly, but well *enough*. Thus, the Internet can fulfill the more modest ambitions of First Wave Internet exceptionalists: by making the Internet *exceptionally* democratic and pluralistic.

Johnson's approach resembles Thierer's Pragmatic Optimism staked out by Adam Thierer: "the trajectory of freedom and even civic virtue has been, in broad terms, over time, constantly upward—because everyone who gets a chance to experience an increased level of democratic self-government—a new 'equality of condition.'" Like Varian, Benkler and Downes, Johnson sees the Internet's facilitation of collaboration and communication as the keys to democratic empowerment.

As a think tank veteran, Rob Atkinson offers a "Taxonomy of Information Technology Policy and Politics," describing eight camps and their positions along four key issues. First is perhaps the strongest, yet also the hardest to define: the **Internet Exceptionalists**, the "Netizens" who "believe that they launched the Internet revolution," prefer informal Internet governance, and generally oppose government intervention online—especially copyright. By contrast, **Social Engineers** distrust large corporations even more than government, thus leading them to advocate regulatory solutions. Though Atkinson doesn't draw the connection, this camp might well be unified by Lessig's concept of "code as law"—updated as "choice architecture," in the highly influential 2008 book *Nudge: Improving Decisions about Health, Wealth, and Happiness* by Cass Sunstein and Richard Thaler. **Free Marketers** are those who believe the "Internet empowers people, liberates entrepreneurs, and enables markets"—especially by reducing transactions costs. Atkinson's proposed tent may be rather too large, potentially encompassing some who advocate regulations like net neutrality or antitrust intervention they believe are the key to freeing markets. The term cyber-libertarian, seems both narrower and broader than Atkinson's conception of "free-marketeers."[8] Indeed, it was originally the term Atkinson used for the "Internet Exceptionalist" camp, focused primarily on cyber-*libertinism* and a fanatic rejection of copyright.

**Moral Conservatives**, on the other hand, "have no qualms about enlisting governments to regulate the Internet" to stamp out sin and sedition. **Old Economy Regulators** reject Internet exceptionalism absolutely and insist on continuing to regulate the Internet like all media in the "public interest." **Tech Companies & Trade Associations** are united not by philosophical approach but by their ultimate duty to shareholders, while **Bricks-and-Mortars**

---

8 *See* Adam Thierer & Berin Szoka, *Cyber-Libertarianism: The Case for Real Internet Freedom*, THE TECHNOLOGY LIBERATION FRONT, Aug. 12, 2009, **http://techliberation.com/2009/08/12/cyber-libertarianism-the-case-for-real-internet-freedom/**

companies, professional groups, and unions generally work to thwart the Internet's disruption of their business models—exemplifying Virginia Postrel's "stasis mindset." Atkinson's own camp is that of the **Moderates**, who want government to "do no harm" to information technology innovations, but also to "actively do good' by adopting policies to promote digital transformation" of the economy.

# Part II: Issues & Applications

## Should Online Intermediaries Be Required to Police More?

Seton Hall Law Professor Frank Pasquale argues that the Internet allows intermediaries to shroud their operations in what might be called "perfect opaqueness"—to extend Larry Lessig's feared model of "perfect control." Pasquale uses the example of Google to illustrate the many ways in which online intermediaries choose to police the Internet, even when not required to do by governments. Given the critical policing role played by intermediaries, Pasquale proposes an "Internet Intermediary Regulatory Council" to "help courts and agencies adjudicate controversies concerning intermediary practice" and assure adequate monitoring—a "prerequisite for assuring a level playing field online." The IIRC "could include a search engine division, an ISP division focusing on carriers, and eventually divisions related to social networks or auction sites if their practices begin to raise commensurate concerns."

While leaving open the possibility that the IIRC could be a private entity, Pasquale is unabashed in citing Robert Hale, theoretician of the New Deal's regulatory frenzy: "Hale's crucial insight was that many of the leading businesses of his day were not extraordinary innovators that 'deserved' all the profits they made; rather, their success was dependent on a network of laws and regulation that could easily shift favor from one corporate player to another." But rather than repealing these laws and regulation to allow the "evolutionary dynamism" of competition to play out, as Adam Thierer proposes, Pasquale is willing to "rely on competition-promotion via markets and antitrust only to the extent that (a) the intermediary in question is an economic (as opposed to cultural or political) force; (b) the 'voice' of the intermediary's user community is strong; and (c) competition is likely to be genuine and not contrived." Otherwise, competition is inadequate. "The bottom line," Pasquale concludes, "is that someone needs to be able to look under the hood" of culturally significant automated ranking systems." Thus, the Internet is *not* exceptional: Pasquale believes only careful regulatory oversight can protect us from shadowy corporations, just as in Franklin Delano Roosevelt's telephone-and-radio era.

While Pasquale seems not to object to intermediaries acting as arms of the police state so long as they are properly transparent and regulated, Mark MacCarthy cautions against the practical problems raised by intermediary policing and offers an analytical model for deciding when intermediary deputization is appropriate. Based on his experience as Senior Vice President for Public Policy at Visa Inc., MacCarthy explores how payment systems have handled Internet gambling and copyright infringement as exemplary case studies in intermediary deputization because, unlike most online intermediaries, payment systems are subject neither to Section 230's absolute immunity for third-party content or activities nor to the notice-and-take-down conditional immunity of the Digital Millennium Copyright Act.

MacCarthy finds cause for optimism about self-regulation: "regardless of the precise legal liabilities, intermediaries have a general responsibility to keep their systems free of illegal transactions and they are taking steps to satisfy that obligation." But he insists intermediary liability should be imposed only where real market failures exists, where supported by "an analysis of costs, benefits and equities," where spelled out clearly, and to the extent local laws are harmonized internationally.

The most troubling form of intermediary deputization comes from uncertain secondary copyright liability, writes independent writer, lawyer and programmer Paul Szynol in an expanded version of an essay originally written for the Electronic Frontier Foundation. He challenges the anti-exceptionalist arguments made by Judge Kozinski and Josh Goldfoot. Szynol argues that the failure to clearly define such liability chills innovation and investment in innovative start-ups—and that that this problem *is* unique to the Internet, given the vastly larger scale of competition facilitated by digital markets.

Most intriguingly, Szynol argues that Kozinski and Goldfoot contradict their argument against Internet Exceptionalism by insisting on a standard for secondary liability online that is not actually applied offline. Szynol asks, "should a car company be held liable for drivers who speed? After all, it would be easy enough to add a 'speed limit compliance chip.' Yet auto manufacturers are not forced to pay any portion of a speeding driver's ticket. Offline, in other words, bad actors—the *users* of technology—are punished for their own transgressions. Online, however, the law chases the manufacturers—and applies ad-hoc, ambiguous standards [of secondary liability] to their products." Thus, for all their denunciation of First Wave Exceptionalists like John Perry Barlow, Szynol essentially insists Kozinski and Goldfoot are actually Goldman's "Second Wave" Internet Exceptionalists who want to impose *more* punitive regulations online than offline.

## Is Search Now an "Essential Facility?"

Frank Pasquale brings his theory of intermediary regulation to full fruition with his sweeping call for "search neutrality." Like Tim Wu in *The Master Switch*, Pasquale worries that antitrust law is incapable of protecting innovation and adequately addressing the "the cultural and political concerns that dominant search engines raise." Thus, he aims to "point the way toward a new concept of 'essential cultural and political facility,' which can help policymakers realize the situations where a bottleneck has become important enough that special scrutiny is warranted." In particular, Pasquale sees taming search as inextricably intertwined with protecting privacy—"Engaging in a cost-benefit analysis [as in antitrust law] diminishes privacy's status as a right"—and Google's potential chokehold on information through the Google Books Settlement.

The existence of competition in search, especially from Microsoft's Bing, and the potential for competition from Facebook and other services yet to be invented, are essentially irrelevant to Pasquale, while the First Amendment's protection of search engine operators are a complication to be addressed down the road. He concludes by insisting that regulation should be supplemented by a publicly funded alternative to the dominant private sector search engine—something the French government has heavily subsidized a European "Quaero" search engine. Similarly, in Chapter 6, Pasquale proposed to model his Internet Intermediary Regulatory Council on the French Data Protection Authority. Thus, Pasquale's over-arching vision seems to be that of a Digital New Deal—*a la française.*

Geoffrey Manne, Professor at Lewis & Clark Law and Executive Director of the International Center for Law & Economics, explains that search engines are not the bottlenecks Pasquale suggests—and thus why even the traditional essential facilities doctrine, which he says "has been relegated by most antitrust experts to the dustbin of history," should not apply to them. In essence, he argues that "search neutrality" would protect only competitors, not consumers, because even a popular search engine like Google cannot foreclose advertisers' access to consumers' attention. Google, like any company, has no legal duty to help its rivals. More to the point, even if Google entirely dominated search, it could not block *consumers'* access to its competitors. This, argues Manne, is the relevant market to analyze—quoting Supreme Court Justice Abe Fortas's famous admonition about excessively narrow market definitions: "This Court now approves this strange red-haired, bearded, one-eyed man-with-a-limp classification."

Like Manne, New York Law School Professor James Grimmelmann expresses "Skepticism about Search Neutrality," and the significant practical problems it

would create. As the author of the definitive law review article, *The Structure of Search Engine Law*,[9] Grimmelmann is keenly aware of the concerns raised by search, yet he concludes that "the case for search neutrality is a muddle" because its "ends and means don't match." Echoing Johnson, Mueller, Holland, and Thierer's view of the Internet as a liberating, democratizing force, Grimmelmann is clear that the lodestar of search is user autonomy: "If search did not exist, then for the sake of human freedom it would be necessary to invent it." He deconstructs eight search neutrality principles—equality, objectivity, bias, traffic, relevance, self-interest, transparency and manipulation—and finds each lacking, but cautions that "it doesn't follow that search engines deserve a free pass under antitrust, intellectual property, privacy, or other well-established bodies of law," and that some *other* "form of search-specific legal oversight" might be appropriate.

Eric Goldman once again puts the debate in the context of its intellectual history. Always focused on questions of exceptionalism, Goldman concludes search engines are neutral only in theory ("Search Engine Utopianism") but must "make editorial judgments just like any other media company." He explains that, while "search engine *bias* sounds scary, … such bias is both necessary and desirable"—and the remedy of "search neutrality" is probably worse than whatever adverse consequences come with search engine bias. Ultimately, he predicts that "emerging personalization technology will soon ameliorate many concerns about search engine bias."

## What Future for Privacy Online?

Michael Zimmer, Professor of Information Studies at School of the University of Wisconsin-Milwaukee, concedes that "the Internet has become a platform for the open flow of personal information—flows that are largely voluntarily provided by users." Yet Zimmer discusses lingering reasons for concern about the Internet as a "potent infrastructure for the flow and capture of personal information."

Zimmer explores the conflicts among privacy laws in the U.S., Europe, Canada and elsewhere, but concludes that "Companies are, on the whole, not moving around in order to avoid strict privacy regulations… instead, there has been a gradual increase in awareness and action on the issue of privacy." Still, Zimmer worries that the "'trading up' to an increased level of protection of personal information flows on our transnational digital networks has not materialized as quickly or clearly as one might expect." Zimmer's answer is to demand a "renewed commitment to the rights of data subjects embodied in the Canadian and European Union approach to data protection."

---

9 James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1 (2007).

Zimmer writes from the perspective that views privacy as a "right." This is, to put it mildly, not a perspective shared by the other two authors in this Chapter: Stewart Baker, a Partner at Steptoe & Johnson LLP and former Assistant Secretary for Policy at the Department of Homeland Security (DHS), and Larry Downes, who has expanded his essay from his 2009 book *The Laws of Disruption.*

Baker spent his time at DHS battling privacy advocates over programs he felt justified to protect Americans against terrorism—leading him to ask, "What's Wrong with Privacy?" He traces the answer back to the 1890 law review article, "The Right to Privacy" by Supreme Court Justice Louis Brandeis and Samuel Warren that gave birth to modern privacy law. Baker rejects their "reactionary defense of the status quo" as Boston elites who didn't much like the news media reporting on the details of their *private* parties. In essence, Baker finds in the privacy "movement" the same "stasis mentality" defined by Virginia Postrel. Like Postrel, Baker argues for dynamism: "Each new privacy kerfuffle inspires strong feelings precisely because we are reacting against the effects of a new technology. Yet as time goes on, the new technology becomes commonplace. Our reaction dwindles away. The raw spot grows a callous. And once the initial reaction has passed, so does the sense that our privacy has been invaded. In short, we get used to it."

Baker rejects the concept of "predicates" for government access to data (*e.g.*, requiring "probable cause" for a warrant), the "Brandeisian notion that we should all 'own' our personal data," and attempting to limit uses of information. Baker has little to say about the private sector's use of data but proposes a system of auditing government employees to rigorously monitor their use of private information.

Larry Downes, too, rejects the concept of intellectual property in personal information—but is willing to concede that Warren and Brandeis "weren't entirely wrong" in that "'private' information can also be used destructively." He thus leaves open the possibility of narrow laws tailored to limiting specific, destructive uses of information—such as anti-discrimination laws. But Downes is highly skeptical about governmental enforcement of "privacy rights," and ultimately echoes John Perry Barlow's optimism about the potential for Netizens to solve their own problems: "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means."[10] Specifically, Downes argues that "the same technologies that create the privacy problem are also proving to be the source of its solution. Even without government intervention, consumers increasingly have the ability to organize, identify their common demands, and enforce their will on enterprises"—detailing examples of how reputational pressure can discipline corporate privacy

---

[10] Barlow, *supra* note 6.

practices. Three cheers for the sound of Eric Goldman's three invisible hand clapping, perhaps? Ultimately, Downes vests his greatest hope in the Internet's potential to create new markets by lowering transactions costs—this time, a market for private data in which an explicit *quid pro quo* rewards consumers for sharing their personal data for beneficial, rather than destructive uses.

## Can Speech Be Policed in a Borderless World?

John Palfrey, Harvard Law Professor and co-director of Harvard's influential Berkman Center for Internet & Society, speaks with unique authority on censorship as one of the co-authors of exhaustive surveys of global censorship conducted by himself, Jonathan Zittrain and others at Berkman. These studies confirm Tim Wu's conclusion that governments can and do censor speech effectively, contrary to the hopes of First Wave Internet Exceptionalists. Palfrey provides a beginner's guide to the techniques used in, goals of, and practical problems created by content filtering. Most disturbingly, he notes the growing use of "soft controls" through governmental pressure and government-fostered social norms intended to squelch dissent.

Like Zittrain, Mueller and Johnson, Palfrey fears "we may be headed toward a localized version of the Internet, governed in each instance by local laws." He thus demands a greater international debate about speech controls that forces states to discuss whether they "actually *want* their citizens to have full access to the Internet or not." In particular, he echoes Mueller's call for international free trade institutions to strike down censorship barriers to free speech.

Christopher Wolf, Partner at Hogan Hartson LLP, focuses not on speech that governments hate, but on "hate speech" we all—or nearly all—would find objectionable. Yet he notes how difficult it can be to distinguish these two categories of censorship. Furthermore, he concludes, after much crusading against hate speech, that "laws against hate speech have not demonstrably reduced hate speech or deterred haters." Thus, he concludes that "Hate speech can be 'policed' in a borderless world, but not principally by the traditional police of law enforcement. The Internet community must continue to serve as a 'neighborhood watch' against hate speech online, 'saying something when it sees something,' and working with online providers to enforce community standards." Thus, like Johnson, Mueller and Barlow, Wolf looks to Netizens to combat hate speech.

## Can the Net Liberate the World?

The book closes by discussing the most tragic disappointment of the First Wave Internet Exceptionalists' vision. Where John Perry Barlow insisted, defiantly, that governments those "weary giants of flesh and steel… [did not] possess any methods of enforcement we have true reason to fear," the reality is that oppressive governments continue to reign, sometimes even using the Internet to serve their agenda. Can the Net liberate the world—or will it, too, become another tool of "perfect control," as Larry Lessig feared? Or will imperfect controls work well enough to allow tyrants to hang on to power?

Evgeny Morozov is a leading commentator on foreign affairs, a visiting scholar at Stanford University and a Schwartz fellow at the New America Foundation. He praises the Internet's ability to quickly disseminate information and allow dissidents to organize. Yet, having grown up in the Soviet Union, he is deeply skeptical about the much-hyped potential for Web media to live up to the hype about democratization. He rejects two critical assumptions underlying this hype. First, he concludes that the legitimacy of undemocratic regimes is derived less from "brainwashing" that can be cured by exposure to the alternative views online and more from popular support for authoritarian regimes that promise to deliver economic growth or play effectively on other concerns, such as nationalism or religion. Second, he suggests the Internet can actually facilitate surveillance, fuel genuine support for existing regimes, allow government to subtly manipulate public opinion, or simply make authoritarianism more efficient.

John Palfrey's acid observation in the previous Chapter bolsters Morozov's suggestion that much of the world may not actually *want* to be liberated: "In China and in parts of the former Soviet Union, very often the most fearsome enforcer of the state's will is the old woman on one's block, who may or may not be on the state's payroll."

Optimists like Johnson, Mueller, Thierer and Holland would likely differ from Morozov—and the U.S. State Department has tended in this direction, too. In January 2010, Secretary of State Hillary Clinton gave a bold speech embracing this optimism about the liberating potential of the Internet, and announcing a commitment to "supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship."[11]

---

[11] Hillary Rodham Clinton, *Remarks on Internet Freedom*, Jan. 21, 2010, **http://www.state.gov/secretary/rm/2010/01/135519.htm**

Internet entrepreneur Ethan Zuckerman is a senior researcher at the Berkman Center and founder of Geekcorps, a non-profit dedicated to building computer infrastructure in developing countries. He joined John Palfrey in the study of censorship circumvention tools mentioned above.[12] Despite his passionate commitment to promoting such tools, as Secretary Clinton proposed, he concludes that "We can't circumvent our way around Internet censorship" because of the costs and practical challenges of attempting to circumvent censorship on a scale sufficient to make a real difference. Thus, he views circumvention as just one of many tools required to thwart "soft censorship, website blocking, and attacks on dissident sites. But ultimately, what is most required is building the right "theory of change" to inform the multi-pronged strategy necessary for the Internet to achieve its democratizing potential.

## Conclusion: Discovering the Future of the Internet & Digital Policy

In these thirty-one essays, our authors paint a complex picture of the future of the Internet and digital policy: Technological change inevitably creates new problems, even as it solves old ones. In the end, one's perspective ultimately depends on whether one thinks the "net" effect of that change is positive or negative—depending on how much, and in what ways, government intervenes online.

Personally, this collection brings me back to where I started my study of Internet policy—reading John Perry Barlow's "Declaration of the Independence of Cyberspace" in 1996, and Virginia Postrel's *The Future and Its Enemies* in 1998. Despite its now-obviously excessive utopian naïveté about the Internet's crippling of the State, Barlow's poetry still resonates deeply with many, including myself, as a powerful synthesis of Internet exceptionalism and cyber-libertarianism, a vision of progress as empowerment and uplifting of the user.

Yet like my former colleague Adam Thierer, it is Postrel's evolutionary dynamism that most guides me, with its emphasis not on a "carefully outlined future" or "build[ing] a single bridge from here to there, for neither here nor there is a single point," but on the *process* of discovery by which the future evolves.[13] Like Postrel, I do not imagine that the disruption and transformation wrought by the Digital Revolution will always be rosy or easy. But we cannot—

---

12 HAL ROBERTS, ETHAN ZUCKERMAN & JOHN PALFREY, 2007 CIRCUMVENTION LANDSCAPE REPORT: METHODS, USES, AND TOOLS (March 2009), **http://dash.harvard.edu/bitstream/handle/1/2794933/2007_Circumvention_Landscape.pdf?sequence=2**.

13 Postrel, s*upra* note 5 at 218.

as the legendary King Canute once tried with the English Channel—command the tides of technological change to halt.

Thierer's "Pragmatic Optimism" demands much more than a resignation to the inevitability of change. At its heart, it is requires a cheery confidence in what David Johnson dubs the "Trajectory of Freedom"—"in broad terms, over time, constantly upward"—but also a commitment to the process by which that trajectory is discovered. *This* is progress—progress *as* freedom.[14] But progress also *requires* freedom, the freedom to discover, innovate and experiment, if technology is to achieve its full potential to improve the human condition and expand individual capacity to choose.

I leave it to you, the reader, to choose—to discover—your own answers to the many questions of law, economics, philosophy and policy explored in this unique book.

---

[14] ROBERT NISBET, HISTORY OF THE IDEA OF PROGRESS 215 (1980).

# CONTRIBUTORS

## Robert D. Atkinson

Robert Atkinson is the founder and president of the Information Technology and Innovation Foundation, a Washington, D.C.-based technology policy think tank. He is also author of the *State New Economy Index* series and the book, *The Past And Future Of America's Economy: Long Waves Of Innovation That Power Cycles Of Growth* (Edward Elgar, 2005). He has an extensive background in technology policy, he has conducted ground-breaking research projects on technology and innovation, is a valued adviser to state and national policy makers, and a popular speaker on innovation policy nationally and internationally.

Before coming to ITIF, Dr. Atkinson was Vice President of the Progressive Policy Institute and Director of PPI's Technology & New Economy Project. While at PPI he wrote numerous research reports on technology and innovation policy, including on issues such as broadband telecommunications, Internet telephony, universal service, e-commerce, e-government, middleman opposition to e-commerce, privacy, copyright, RFID and smart cards, the role of IT in homeland security, the R&D tax credit, offshoring, and growth economics.

Previously Dr. Atkinson served as the first Executive Director of the Rhode Island Economic Policy Council, a public-private partnership including as members the Governor, legislative leaders, and corporate and labor leaders. As head of RIEPC, he was responsible for drafting a comprehensive economic strategic development plan for the state, developing a ten-point economic development plan, and working to successfully implement all ten proposals through the legislative and administrative branches. Prior to that he was Project Director at the former Congressional Office of Technology Assessment. While at OTA, he directed *The Technological Reshaping of Metropolitan America*, a seminal report examining the impact of the information technology revolution on America's urban areas.

## Stewart Baker

**Stewart A. Baker** is a partner in the Washington office of Steptoe & Johnson LLP. He returned to the firm following 3½ years at the Department of Homeland Security as its first Assistant Secretary for Policy.

At Homeland Security, Mr. Baker created and staffed the 250-person DHS Policy Directorate. He was responsible for policy analysis across the Department, as well as for the Department's international affairs, strategic planning and relationships with law enforcement and public advisory committees. While at DHS, Mr. Baker led successful negotiations with European and Middle Eastern governments over travel data, privacy, visa waiver and related issues. He devised a new approach to visa-free travel, forged a congressional and interagency consensus on the plan and negotiated acceptance with key governments.

Mr. Baker manages one of the nation's premier technology and security practices at Steptoe. Mr. Baker's practice covers national security, electronic surveillance, law enforcement, export control encryption, and related technology issues. He has been a key advisor on U.S. export controls and on foreign import controls on technology. He has also advised companies on the requirements imposed by CFIUS.

Mr. Baker's practice includes issues relating to government regulation of international trade in high-technology products, and advice and practice under the antidumping and countervailing duty laws of United States, European Community, Canada, and Australia. He also counsels clients on issues involving foreign sovereign immunity, and compliance with the Foreign Corrupt Practices Act.

Mr. Baker has handled the arbitration of claims exceeding a billion dollars, is a member of national and international rosters of arbitrators, and is the author of articles and a book on the United Nations Commission on International Trade Law arbitration rules.

Mr. Baker has had a number of significant successes in appellate litigation and appearances before the United States Supreme Court. He developed—and persuaded the Court to adopt—a new theory of constitutional federalism that remains the most vibrant 10th Amendment doctrine of the past 30 years.

## Ann Bartow

**Ann Bartow** is a Professor of Law at the University of South Carolina School of Law in Columbia, South Carolina. She holds a Bachelor of Science from Cornell University and a Juris Doctor from the University of Pennsylvania Law School. She currently teaches an Intellectual Property Survey, Copyright Law, Trademarks and Unfair Competition Law, Patent Law and a seminar entitled Pornography, Prostitution, Sex Trafficking and the Law. Her scholarship focuses on the intersection between intellectual property laws and public policy concerns, privacy and technology law, and feminist legal theory. She also co-administers the **Feminist Law Professors** blog, is a regular blogger at Madisonian.net and a contributing editor at Jotwell.com.

## Yochai Benkler

**Yochai Benkler** is the Berkman Professor of Entrepreneurial Legal Studies at Harvard, and faculty co-director of the Berkman Center for Internet and Society. Before joining the faculty at Harvard Law School, he was Joseph M. Field '55 Professor of Law at Yale. He writes about the Internet and the emergence of networked economy and society, as well as the organization of infrastructure, such as wireless communications.

In the 1990s he played a role in characterizing the centrality of information commons to innovation, information production, and freedom in both its autonomy and democracy senses. In the 2000s, he worked more on the sources and economic and political significance of radically decentralized individual action and collaboration in the production of information, knowledge and culture. His books include THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006), which received the Don K. Price award from the American Political Science Association for best book on science, technology, and politics.

In civil society, Benkler's work was recognized by the Electronic Frontier Foundation's Pioneer Award in 2007, and the Public Knowledge IP3 Award in 2006. His articles include *Overcoming Agoraphobia* (1997/98, initiating the debate over spectrum commons); *Commons as Neglected Factor of Information Production* (1998) and *Free as the Air to Common Use* (1998, characterizing the role of the commons in information production and its relation to freedom); *From Consumers to Users* (2000, characterizing the need to preserve commons as a core policy goal, across all layers of the information environment); *Coase's Penguin, or Linux and the Nature of the Firm* (characterizing peer production as a basic phenomenon of the networked economy) and *Sharing Nicely* (2002, characterizing shareable goods and explaining sharing of material resources online). His work can be freely accessed at **benkler.org**.

## Larry Downes

**Larry Downes** is an Internet analyst and consultant, helping clients develop business strategies in an age of constant disruption caused by information technology.

Downes is author of *Unleashing the Killer App: Digital Strategies for Market Dominance* (Harvard Business School Press, 1998), which was named by the Wall Street Journal as one of the five most important books ever published on business and technology.

His new book, *The Laws of Disruption: Harnessing the New Forces that Govern Lie and Business in the Digital Age* (Basic Books 2009) offers nine strategies for success in navigating the accident-prone intersection of innovation and the law.

From 2006-2010, Downes was a nonresident Fellow at the Stanford Law School Center for Internet and Society. Before that, he held faculty positions at the University of California-Berkeley, Northwestern University School of Law, and the University of Chicago Graduate School of Business. Downes is a Partner with the Bell-Mason Group, which works with Global 1000 corporations, providing corporate venturing methodologies, tools, techniques and support that accelerate corporate innovation and venturing programs.

He has written for a variety of publications, including U.S.A Today, Harvard Business Review, Inc., Wired, CNet, Strategy & Leadership, CIO, The American Scholar *and the* Harvard Journal of Law and Technology. He was a columnist for both The Industry Standard and CIO Insight. He blogs for the **Technology Liberation Front**.

## Josh Goldfoot

Josh Goldfoot is Senior Counsel with the Computer Crime & Intellectual Property Section of the U.S. Department of Justice. He prosecutes hackers and other computer criminals, and advises investigators and other prosecutors about privacy statutes, the Fourth Amendment, and implications of emerging technologies on law enforcement. In 2010, he was awarded the Assistant Attorney General's Meritorious Service Award. He is an accomplished software developer and computer technician, and received a United States patent in 2008 for shape recognition technology. He is a graduate of Yale University and earned his law degree from the University of Virginia School of Law. He has worked in technology law since 1999, when he advised Internet startups in Silicon Valley on intellectual property issues. Prior to joining the Department of Justice in 2005, he did appellate and civil litigation, and clerked for judge Alex Kozinski on the Ninth Circuit U.S. Court of Appeals. He was a Special Assistant United States Attorney in the Eastern District of Virginia for six months in 2007 and 2008.

## Eric Goldman

**Eric Goldman** is an Associate Professor of Law at Santa Clara University School of Law. He also directs the school's High Tech Law Institute. Before joining the SCU faculty in 2006, he was an Assistant Professor at Marquette University Law School, General Counsel of Epinions.com, and an Internet transactional attorney at Cooley Godward LLP.

Eric teaches Cyberlaw and Intellectual Property and previously has taught courses in Copyrights, Contracts, Software Licensing and Professional Responsibility.

Eric's research focuses on Internet law, intellectual property, marketing, and the legal and social implications of new communication technologies. Recent papers have addressed topics such as search engines and online marketing practices.

Eric received his BA, *summa cum laude* and Phi Beta Kappa, in Economics/Business from UCLA in 1988. He received his JD from UCLA in 1994, where he was a member of the UCLA Law Review, and concurrently received his MBA from the Anderson School at UCLA.

## James Grimmelmann

**James Grimmelmann** is Associate Professor at **New York Law School** and a member of its **Institute for Information Law and Policy**. He received his J.D. from **Yale Law School**, where he was Editor-in-Chief of LawMeme and a member of the **Yale Law Journal**. Prior to law school, he received an A.B. in computer science from **Harvard College** and worked as a programmer for **Microsoft**. He has served as a Resident Fellow of the **Information Society Project** at Yale, as a legal intern for **Creative Commons** and the **Electronic Frontier Foundation**, and as a law clerk to the Honorable Maryanne Trump Barry of the United States Court of Appeals for the Third Circuit.

He studies how the law governing the creation and use of computer software affects individual freedom and the distribution of wealth and power in society. As a lawyer and technologist, he aims to help these two groups speak intelligibly to each other. He writes about intellectual property, virtual worlds, search engines, online privacy, and other topics in computer and Internet law. Recent publications include *The Internet Is a Semicommons*, 78 Fordham L. Rev. 2799 (2010), *Saving Facebook*, 94 Iowa L. Rev. 1137 (2009), *The Ethical Visions of Copyright Law*, 77 Fordham L. Rev. 2005 (2009).

He has been blogging since 2000 at the Laboratorium: **www.laboratorium.net**.

## H. Brian Holland

Professor **H. Brian Holland** joined the faculty of Texas Wesleyan School of Law in 2009. Prior to his arrival, Professor Holland was a Visiting Associate Professor at Penn State University's Dickinson School of Law.

After graduating from law school, Professor Holland spent two years as a judicial clerk in the U.S. Court of Appeals for the Second Circuit in New York. He then joined the Washington, D.C. office of Jones, Day, Reavis & Pogue. His work with the firm consisted primarily of appellate work before the U.S. Supreme Court and federal courts of appeals, as well as international arbitration before the World Bank. Among the significant cases litigated during this period were issues of intellectual property and constitutional law (Eldred v. Reno/Ashcroft and Luck's Music Library, Inc. v. Reno/Ashcroft), privacy and identity theft (TRW v. Andrews), and federal bankruptcy jurisdiction and venue.

Professor Holland's scholarship reflects his interest in technology, governance and social change, with a particular emphasis on issues of authority within the online environment and the development of social norms in mediated communities. He is currently writing on privacy in social networks. His most recent work, *Social Distortion: Regulating Privacy in Social Networks*, has been a featured presentation at privacy conferences both in the United States and Europe.

Professor Holland received a LL.M., with honors, from Columbia University School of Law, completing a self-designed program in technology law. He holds a J.D., summa cum laude, from American University's Washington College of Law, and a B.A. from Tufts University. Professor Holland is currently pursuing his Ph.D. in Digital Media and Mass Communications at Penn State University. His dissertation, now in progress, applies social semiotic theories to the concept of fair use in intellectual property law.

## David R. Johnson

David Johnson joined New York Law School's faculty in spring 2004 as a visiting professor of law. He is a faculty member of the Institute for Information Law and Policy.

Professor Johnson joined Wilmer, Cutler & Pickering in 1973 and became a partner in 1980. His practice focused primarily on the emerging area of electronic commerce, including counseling on issues relating to privacy, domain names and Internet governance issues, jurisdiction, copyright, taxation, electronic contracting, encryption, defamation, ISP and OSP liability, regulation, and other intellectual property matters.

Professor Johnson helped to write the Electronic Communications Privacy Act, was involved in discussions leading to the Framework for Global Electronic Commerce, and has been active in the introduction of personal computers in law practice. He co-authored, with David Post, Law and Borders: The Rise of Law in Cyberspace, 48 Stanford Law Review 1367 (1996). He is currently developing online legal games and law practice simulations.

Professor Johnson graduated from Yale College with a B.A. summa cum laude in 1967. He completed a year of postgraduate study at University College, Oxford in 1968, and earned a J.D. from Yale Law School in 1972. Following graduation from law school, Professor Johnson clerked for a year for the Honorable Malcolm R. Wilkey of the United States Court of Appeals for the District of Columbia.

## Andrew Keen

**Andrew Keen** is the author of the international hit CULT OF THE AMATEUR: HOW THE INTERNET IS KILLING OUR CULTURE (2008). Acclaimed by THE NEW YORK TIMES' Michiko Kakutani as having been written "with acuity and passion" and by A.N. Wilson in the DAILY MAIL as "staggering", CULT OF THE AMATEUR has been published in **fifteen different language editions** and was short-listed for the 2008 Higham's Business Technology Book of the Year award.

As a pioneering Internet entrepreneur, Andrew founded Audiocafe.com in 1995 and built it into a popular first generation Internet music company. He was the executive producer of the new media show "MB5 2000" and, between 2001 and 2007, worked as a senior sales and marketing executive at several Silicon Valley-based technology start-ups including Pulse, Santa Cruz Networks and Pure Depth. He is currently the host of the popular "Keen On" show on **Techcrunch.tv** as well as the host of the video interview series "The Future of Creativity" on the Harvard Business Review website.

Andrew was educated at London University where he was awarded a First Class Honors Degree in Modern History, as a British Council Fellow at the University of Sarajevo and at the University of California at Berkeley where he earned a Masters Degree in Political Science.

He is currently writing a second book entitled DIGITAL VERTIGO: ANXIETY, LONELINESS AND INEQUALITY IN THE SOCIAL MEDIA AGE which will be published by St Martins Press.

## Hon. Alex Kozinski

**Chief Judge Alex Kozinski** was appointed United States Circuit Judge for the Ninth Circuit on November 7, 1985. He graduated from UCLA, receiving an A.B. degree in 1972, and from UCLA Law School, receiving a J.D. degree in 1975. Prior to his appointment to the appellate bench, Judge Kozinski served as Chief Judge of the United States Claims Court, 1982-85; Special Counsel, Merit Systems Protection Board, 1981-1982; Assistant Counsel, Office of Counsel to the President, 1981; Deputy Legal Counsel, Office of President-Elect Reagan, 1980-81; Attorney, Covington & Burling, 1979-81; Attorney, Forry Golbert Singer & Gelles, 1977-79; Law Clerk to Chief Justice Warren E. Burger, 1976-77; and Law Clerk to Circuit Judge Anthony M. Kennedy, 1975-76.

## Mark MacCarthy

**Mark MacCarthy** teaches and conducts research at Georgetown University's Communication, Culture, and Technology Program. He teaches courses on the development of the electronic media, technology policy and Internet freedom. He is also an adjunct member of the Department of Philosophy where he teaches courses in political philosophy and philosophy and privacy. He does research and consults in the areas of information privacy and security, Internet intermediary liability, global Internet freedom, the future of the online media, consumer financial protection, open standards, electronic and mobile commerce and other technology policy issues. He is an Affiliate of Georgetown University's McDonough School of Business Center for Business and Public Policy, an investigator with the RFID Consortium for Security and Privacy, and the appointed expert of the American National Standards Institute on the

International Organization For Standardization (ISO) Technical Management Board (TMB) Privacy Steering Committee

From 2000 to 2008, he was Senior Vice President for Global Public Policy at Visa Inc, responsible for policy initiatives affecting electronic commerce, new technology and information security and privacy. He regularly represented Visa before the U.S. Congress, the U.S. Administration, the U.S. Federal Trade Commission, the U.S federal financial regulators and multi-governmental groups such as the Organization for Economic Cooperation and Development and Asia Pacific Economic Cooperation group.

Prior to joining Visa, he spent six years as a principal and senior director with the Wexler-Walker Group, a Washington public policy consulting firm, where he worked with a variety of clients on electronic commerce, financial services, privacy and telecommunications. He was Vice President in charge of Capital Cities/ABC's Washington office from 1988 to 1994, representing the company's interests before Congress, the Federal Communications Commission and other administrative agencies. From 1981 to 1988 he was a professional staff member of the House Committee on Energy and Commerce, where he handled communications policy issues. From 1978 to 1981, he worked as an economist performing regulatory analyses of safety and health regulations at the U.S. Occupational Safety and Health Administration.

Mr. MacCarthy has a Ph.D in philosophy from Indiana University and an MA in economics from the University of Notre Dame.

## Geoffrey Manne

Currently the Executive Director of the International Center for Law & Economics (ICLE), a global think tank, Professor Manne also serves as Lecturer in Law for Lewis & Clark Law School. In this capacity he lends his expertise to various law school endeavors and teaches the school's Law and Economics course. The ICLE's website is at **www.laweconcenter.org**.

Manne was an Assistant Professor of Law at Lewis & Clark from 2003 to 2008. From 2006 to 2008 he took a leave of absence from the school to direct a law and economics academic outreach program at Microsoft, and was Director, Global Public Policy at LECG, an economic consulting firm, until founding the ICLE at the end of 2009. Prior to joining the Lewis & Clark faculty he practiced law at Latham & Watkins in Washington, D.C., where he specialized in antitrust litigation and counseling. Before private practice Manne was a Bigelow Fellow at the University of Chicago Law School, an Olin Fellow at the University of Virginia School of Law and a law clerk to Judge Morris S. Arnold of the U.S. Court of Appeals for the Eighth Circuit. While clerking he taught a seminar on Law & Literature at the University of Arkansas at Little Rock.

During law school Manne was a research assistant to Judge Richard Posner, Comment Editor of the University of Chicago Law School Roundtable and a Staff Member of the University of Chicago Legal Forum. Among his other vocational pursuits was a brief stint at the U.S. Federal Trade Commission. His research has focused broadly on the economic implications of legal constraints on business organizations, particularly in the contexts of antitrust, nonprofit organizations and international law. Manne is a member of the Virginia bar, as well as the Bar of the U.S. Bankruptcy Court for the Eastern District of Virginia. He is also a member of the American Law and Economics Association, the Canadian Law and Economics Association and the International Society for New Institutional Economics.

He blogs for the **Technology Liberation Front**.

## Evgeny Morozov

Evgeny Morozov is the author of THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM (Public Affairs, 2011). He is also a visiting scholar at Stanford University, a fellow at the New America Foundation and a contributing editor to Foreign Policy magazine.

## Milton Mueller

Milton Mueller teaches and does research on the political economy of communication and information. He uses the theoretical tools of property rights analysis, institutional economics and both historical and quantitative social science methods. He has a longstanding interest in the history of communication technologies and global governance institutions. Mueller received the Ph.D. from the University of Pennsylvania in 1989.

Mueller's most recent research projects explore the problem of governing the Internet. His new book NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE (MIT Press, 2010) provides a comprehensive overview of the political and economic drivers of a new global politics. His acclaimed book RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE (MIT Press, 2002) was the first scholarly account of the debates over the governance of the domain name system. His book, UNIVERSAL SERVICE: COMPETITION, INTERCONNECTION AND MONOPOLY IN THE MAKING OF THE AMERICAN TELEPHONE SYSTEM (MIT Press, 1997) set out a dramatic revision of our understanding of the origins of universal telephone service and the role of interconnection in industry development. He is on the international editorial boards of the journals TELECOMMUNICATIONS POLICY, THE INFORMATION SOCIETY, and INFO: THE JOURNAL OF POLICY, REGULATION AND STRATEGY FOR TELECOMMUNICATION, INFORMATION AND MEDIA.

## John Palfrey

**John Palfrey** is Henry N. Ess Professor of Law and Vice Dean for Library and Information Resources at Harvard Law School. He is the co-author of *Born Digital: Understanding the First Generation of Digital Natives* (Basic Books, 2008) and *Access Denied: The Practice and Politics of Internet Filtering* (MIT Press, 2008). His research and teaching is focused on Internet law, intellectual property, and international law. He practiced intellectual property and corporate law at the law firm of Ropes & Gray. He is a faculty co-director of the **Berkman Center for Internet & Society** at Harvard University. Outside of Harvard Law School, he is a Venture Executive at Highland Capital Partners and serves on the board of several technology companies and non-profits. John served as a special assistant at the U.S. EPA during the Clinton Administration. He is a graduate of Harvard College, the University of Cambridge, and Harvard Law School.

## Frank Pasquale

Frank Pasquale is a professor of law at Seton Hall Law School and a visiting fellow at the Princeton University's Center for Information Technology Policy. He has a JD from Yale, was a Marshall Scholar at Oxford, and graduated from Harvard summa cum laude. He has been a visiting professor at Yale and Cardozo Law Schools. He has published widely on information law and policy. In 2010, he was twice invited by the National Academy of Sciences's Committee on Law, Science, and Technology and its Government-University-Industry Roundtable to present on the privacy and security implications of data sensor networks. He also was invited by the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology to present at a roundtable organized to inform ONC's Congressionally mandated report on privacy and security requirements for entities not covered by HIPAA (relating to Section 13424 of the HITECH Act). In 2008, he presented Internet Nondiscrimination Principles for Competition Policy Online before the Task Force on Competition Policy and Antitrust Laws of the House Committee on the Judiciary, appearing with the General Counsels of Google, Microsoft, and Yahoo. He is the Chair of the Privacy & Defamation section of the American Association of Law Schools for 2010.

Pasquale has been quoted in the New York Times, San Francisco Chronicle, Los Angeles Times, Boston Globe, Financial Times, and many other publications. He has appeared on CNN to comment on Google's China policy. He has been interviewed on internet regulation on David Levine's **Hearsay Culture** poD.C.ast, WNYC's **Brian Lehrer Show**, the Canadian BroaD.C.asting Corporation's documentary "Engineering Search," and on National Public Radio's **Talk of the Nation**. His recent publications include "Beyond Innovation and Competition," "Network Accountability for the Domestic Intelligence Apparatus" (with Danielle Citron), "Restoring

Transparency to Automated Authority," and "Data and Power." He is presently working on a book titled "The Black Box Society" which examines and critiques the rise of secret technology in the internet and finance sectors.

## Berin Szoka

Berin Szoka is founder of **TechFreedom**, a non-profit think tank dedicated to unleashing the progress of technology that improves the human condition and expands individual capacity to choose.

Previously, he was a Senior Fellow and the Director of the Center for Internet Freedom at **The Progress & Freedom Foundation**. Before joining PFF, he was an Associate in the Communications Practice Group at Latham & Watkins LLP. Before joining Latham, Szoka practiced at Lawler Metzger Milkman & Keeney, LLC in Washington and clerked for the Hon. H. Dale Cook, Senior U.S. District Judge for the Northern District of Oklahoma.

Szoka received his Bachelor's degree in economics from Duke University and his juris doctor from the University of Virginia School of Law, where he served as Submissions Editor of the Virginia Journal of Law and Technology. He is admitted to practice law in the District of Columbia and California (inactive).

He serves on the Steering Committee for the D.C. Bar's **Computer & Telecommunications Law Section**, and on the FAA's **Commercial Space Transportation Advisory Committee** (COMSTAC). Szoka has chaired, and currently serves on, the Board of Directors of the **Space Frontier Foundation**, a non-profit citizens' advocacy group founded in 1988 and dedicated to advancing commercial opportunity and expansion of human civilization in space.

## Paul Szynol

**Paul Szynol** was born in Warsaw, Poland, and moved to the United States in 1984, the year that New York City's transit fare rose from 75 cents to 90 cents; 33 previously unknown Bach pieces were found in an academic library; and Canon demoed its first digital still camera. He has lived in New York City, San Francisco, Los Angeles, New Haven, Philadelphia, New Jersey, and Warsaw, and, during his six drives across the U.S., visited the vast majority of the contiguous states. He graduated from Columbia University, where he studied history and philosophy, and Yale University, where he studied intellectual property law. He has also taken courses at the International Center of Photography. In the past, Paul played drums and was a computer programmer, and he still tinkers with Pearl drums and Java libraries. He likes dogs, documentary photography, music, San Francisco, Linux, and depressing movies. He is currently based in New York City.

## Adam Thierer

**Adam Thierer** is a senior research fellow at the Mercatus Center at George Mason University where he works with the Technology Policy Program. Thierer covers technology, media, Internet, and free speech policy issues with a particular focus in online child safety and digital privacy policy issues.

Thierer has spent almost two decades in the public policy research community. He previously served as the President of The Progress & Freedom Foundation, the Director of Telecommunications Studies at the Cato Institute, a Senior Fellow at The Heritage Foundation as a Fellow in Economic Policy, and a researcher at the Adam Smith Institute in London.

Thierer is the author or editor of seven books on diverse topics such as media regulation and child safety issues, mass media regulation, Internet governance and jurisdiction, intellectual property, regulation of network industries, and the role of federalism within high-technology markets. He earned his B.A. in journalism and political science at Indiana University, and received his M.A. in international business management and trade theory at the University of Maryland.

Thierer has served on several distinguished online safety task forces, including Harvard Law School's Internet Safety Technical Task Force, a "Blue Ribbon Working Group" on child safety organized by Common Sense Media, the iKeepSafe Coalition, and the National Cable & Telecommunications Association, and the National Telecommunications and Information Administration's "Online Safety and Technology Working Group." He is also an advisor to the American Legislative Exchange Council's Telecom & IT Task Force. In 2008, Thierer received the Family Online Safety Institute's "Award for Outstanding Achievement."

## Hal Varian

**Hal R. Varian** is the Chief Economist at Google. He started in May 2002 as a consultant and has been involved in many aspects of the company, including auction design, econometric analysis, finance, corporate strategy and public policy.

He is also an emeritus professor at the University of California, Berkeley in three departments: business, economics, and information management.

He received his SB degree from MIT in 1969 and his MA in mathematics and Ph.D. in economics from UC Berkeley in 1973. He has also taught at MIT, Stanford, Oxford, Michigan and other universities around the world.

Dr. Varian is a fellow of the Guggenheim Foundation, the Econometric Society, and the American Academy of Arts and Sciences. He was Co-Editor of the American Economic Review from 1987-1990 and holds honorary doctorates from the University of Oulu, Finland and the University of Karlsruhe, Germany.

Professor Varian has published numerous papers in economic theory, industrial organization, financial economics, econometrics and information economics. He is the author of two major economics textbooks which have been translated into 22 languages. He is the co-author of a bestselling book on business strategy, **INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY** and wrote a **monthly column** for the NEW YORK TIMES from 2000 to 2007.

## Christopher Wolf

**Christopher Wolf** is a director of Hogan Lovells' Privacy and Information Management practice group. Chris is widely recognized as one of the leading American practitioners in the field of privacy and data security law. The prestigious Practising Law Institute (PLI) tapped Chris to serve as editor and lead author of its first-ever treatise on the subject, and to serve as co-editor of its guide to the FACTA Red Flags identity theft regulations. Chris recently was heralded for his "lifelong experience as a litigator" by Chambers U.S.A by ranking him as one of the nation's top privacy lawyers. He also was asked to form and co-chair The Future of Privacy Forum, a think tank that focuses on modern privacy issues with a business practical-consumer friendly perspective, collaborating with industry, government, academia, and privacy advocates. When MSNBC labeled Chris "a pioneer in Internet law," it was reflecting on his participation in many of the precedent-setting matters that form the framework of modern privacy law.

Chris has deep experience in the entire range of international, federal, and state privacy and data security laws as well as the many sectoral and geographic regulations. Chris also counsels clients on compliance with self-regulatory regimes.

Chris has appeared as a speaker for the International Association of Privacy Professionals and for the Canadian Association of Chief Privacy Officers. He appears annually at the PLI Institute on Privacy and Security Law. He also has spoken at colleges and universities including Harvard, Stanford, Berkeley, the University of Chicago, George Washington University, Georgetown University, and the Washington & Lee University School of Law. He is a frequent television guest on privacy and related issues, appearing on PBS, NBC, MSNBC, CNN, Fox News, and others.

Chris is a fourth-generation Washingtonian who started his career in Washington, D.C. as law clerk to The Honorable Aubrey E. Robinson, Jr., of the U.S. District Court for the District of Columbia. While in law school, he was a member of the *Washington & Lee Law Review*.

## Tim Wu

**Tim Wu** is a professor at Columbia Law School. He teaches copyright and communications.

He is the chair of media reform organization **Free Press**, and writes for **Slate magazine** on law, media, culture, travel, and dumplings. He has also written for some other publications as a pure freelancer, including the NEW YORKER, the NEW YORK TIMES, WASHINGTON POST WEEKEND, and FORBES.

He is also involved in various other projects, usually related to alternative channels of content distribution. Many are run through the **Columbia Program on Law & Technology.** One example is **Project Posner**, another is **AltLaw**, and another is **Keep Your Copyrights**.

His first book was **WHO CONTROLS THE INTERNET** with Jack Goldsmith. He is writing a new book on the long patterns of media centralization and decentralization; the publisher is Knopf / Random House.

His **topics** of study are: **Network neutrality**, the history and structure of the media and communications industries (the book he is currently working on), international problems faced by the Internet (see **WHO CONTROLS THE INTERNET**, and copyright and innovation policy (***Copyright's Communications Policy***).

His brother is **David Wu**, author of the Xbox 360 game **Full Auto**, and his mother is **Gillian Wu,** a scientist. He is married to Kate Judge. His best friends are the **Famous Five**.

## Michael Zimmer

Michael Zimmer, PhD, is an **assistant professor** in the **School of Information Studies** at the **University of Wisconsin-Milwaukee**, and an associate at the **Center for Information Policy Research**.

With a background in new media and Internet studies, the philosophy of technology, and information policy, Zimmer studies the social, political, and ethical dimensions of new media and information technologies. His research and teaching focuses on:

- Ethics and Information Technology
- Information Policy
- Web Search Engines
- Web 2.0 and Library 2.0
- Privacy and Surveillance Theory
- Information and Web Literacy
- Access to Knowledge
- Internet Research Ethics

Zimmer received his PhD in 2007 from the **Department of Media, Culture, and Communication** at New York University under the guidance of Profs. **Helen Nissenbaum**, **Alex Galloway**, and **Siva Vaidhyanathan**. He was a Student Fellow at the **Information Law Institute** at **NYU Law** from 2004-2007, and was the Microsoft Resident Fellow at the **Information Society Project** at **Yale Law School** for 2007-2008. Zimmer **joined** UW-Milwaukee's School of Information Studies in 2008.

Zimmer earned a B.B.A. in Marketing from the University of Notre Dame in 1994 and worked for an electronic payment processing company in Milwaukee, Wisconsin for several years before moving to New York City to pursue a new career in academia. He earned an M.A. in Media Ecology from NYU in 2002, and his doctoral studies were supported by the Phyllis and Gerald LeBoff Doctoral Fellowship in Media Ecology from the Steinhardt School of Education at New York University. His dissertation research was supported by an **NSF SES Dissertation Improvement Grant**.

Zimmer has published in international journals and delivered talks across North America and Europe. He has been interviewed in ***The New York Times***, on *National Public Radio*'s **Morning Edition** and **Science Friday** programs, *The Huffington Post*, **MSNBC.com**, *GQ Magazine*, *The Montreal Gazette*, ***The Boston Globe***, ***MIT Technology Review***, *The Milwaukee Journal Sentinel*, and in various other national and local print and radio outlets.

Zimmer was also featured in the "Is My Cellphone Spying on Me?" commentary accompanying the **2-disc special edition DVD** for the hit action/thriller movie ***Eagle Eye***.

## Jonathan Zittrain

Jonathan Zittrain is Professor of Law at Harvard Law School and the Harvard Kennedy School of Government, co-founder of the Berkman Center for Internet & Society, and Professor of Computer Science in the Harvard School of Engineering and Applied Sciences. He is a member of the Board of Trustees of the Internet Society and is on the board of advisors for *Scientific American*. Previously he was Professor of Internet Governance and Regulation at Oxford University.

His research interests include battles for control of digital property and content, cryptography, electronic privacy, the roles of intermediaries within Internet architecture, and the useful and unobtrusive deployment of technology in education.

He performed the first large-scale tests of Internet filtering in China and Saudi Arabia in 2002, and now as part of the OpenNet Initiative he has co-edited a study of Internet filtering by national governments, ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING, and its sequel, ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE.

His book THE FUTURE OF THE INTERNET—AND HOW TO STOP IT is available from Yale University Press and Penguin UK—and under a Creative Commons license. His papers may be found at **www.jz.org**.

## Ethan Zuckerman

**Ethan Zuckerman** served as a fellow of the Berkman Center for Internet and Society at Harvard University from 2003 through 2009. Since 2009, he's been a senior researcher at the center, working on projects that focus on the impact of technology and media on the developing world and on quantitative analysis of media. With Hal Roberts, he is working on comparative studies of tools for censorship circumvention, techniques for blocking-resistant publishing for human rights sites and on the Media Cloud framework for quantitative study of digital media.

Ethan and Berkman fellow Rebecca MacKinnon founded Global Voices, a global citizen media network. Beginning at a Berkman conference in 2004, Global Voices has grown into an independent Netherlands-based nonprofit with over 200 employees and volunteers in over 100 countries. Global Voices **maintains an international citizen media newsroom**, **tracks censorship and advocates for freedom of speech online**, **supports grassroots citizen media efforts** and **is a pioneer in the space of social translation**. Global Voices' work has been supported by the MacArthur Foundation, Ford Foundation, Knight Foundation, Hivos, Open Society Institute as well as Google, Reuters and private donors. Ethan chairs Global Voices' global board of directors.

In 2000, Ethan founded Geekcorps, a non-profit technology volunteer corps. Geekcorps pairs skilled volunteers from U.S. and European high tech companies with businesses in emerging nations for one to four month volunteer tours. Volunteers have served in 14 nations, including Ghana, Senegal, Mali, Rwanda, Armenia and Jordan, completing over a hundred projects. Geekcorps became a division of the International Executive Service Corps in 2001, where Ethan served as a vice president from 2001 to 2004.

# PART I

## THE BIG PICTURE & NEW FRAMEWORKS

# CHAPTER 1

## THE INTERNET'S IMPACT ON CULTURE & SOCIETY: GOOD OR BAD?

# Why We Must Resist the Temptation of Web 2.0

By Andrew Keen*

The ancients were good at resisting seduction. Odysseus fought the seductive song of the Sirens by having his men tie him to the mast of his ship as it sailed past the Siren's Isle. Socrates was so intent on protecting citizens from the seductive opinions of artists and writers, that he outlawed them from his imaginary republic.

We moderns are less nimble at resisting great seductions, particularly those utopian visions that promise grand political or cultural salvation. From the French and Russian revolutions to the counter-cultural upheavals of the '60s and the digital revolution of the '90s, we have been seduced, time after time and text after text, by the vision of a political or economic utopia.

Rather than Paris, Moscow, or Berkeley, the grand utopian movement of our contemporary age is headquartered in Silicon Valley, whose great seduction is actually a fusion of two historical movements: the counter-cultural utopianism of the '60s and the techno-economic utopianism of the '90s. Here in Silicon Valley, this seduction has announced itself to the world as the "Web 2.0" movement.

On one occasion, I was treated to lunch at a fashionable Japanese restaurant in Palo Alto by a serial Silicon Valley entrepreneur who, back in the dot.com boom, had invested in my start-up Audiocafe.com. The entrepreneur, a Silicon Valley veteran like me, was pitching me his latest start-up: a technology platform that creates easy-to-use software tools for online communities to publish weblogs, digital movies, and music. It is technology that enables anyone with a computer to become an author, a film director, or a musician. This Web 2.0 dream is Socrates's nightmare: technology that arms every citizen with the means to be an opinionated artist or writer.

"This is historic," my friend promised me. "We are enabling Internet users to author their own content. Think of it as empowering citizen media. We can help smash the elitism of the Hollywood studios and the big record labels. Our technology platform will radically democratize culture, build authentic community, and create citizen media." Welcome to Web 2.0.

---

* Andrew Keen is a veteran Silicon Valley entrepreneur and digital media critic. He blogs at **TheGreatSeduction.com** and has recently launched **AfterTV**, a podcast chat show about media, culture, and technology. He is the author of THE CULT OF THE AMATEUR: HOW TODAY'S INTERNET IS KILLING OUR CULTURE (Crown 2007).

Buzzwords from the old dot.com era—like "cool," "eyeballs," or "burn-rate"—have been replaced in Web 2.0 by language which is simultaneously more militant and absurd: empowering citizen media, radically democratize, smash elitism, content redistribution, authentic community. This sociological jargon, once the preserve of the hippie counterculture, has now become the lexicon of new media capitalism.

Yet this entrepreneur owns a $4 million house a few blocks from Steve Jobs's house. He vacations in the South Pacific. His children attend the most exclusive private academy on the peninsula. But for all of this he sounds more like a cultural Marxist—a disciple of Antonio Gramsci or Herbert Marcuse—than a capitalist with an MBA from Stanford.

In his mind, "big media"—the Hollywood studios, the major record labels and international publishing houses—really did represent the enemy. The promised land was user-generated online content. In Marxist terms, the traditional media had become the exploitative "bourgeoisie," and citizen media, those heroic bloggers and podcasters, were the "proletariat."

This outlook is typical of the Web 2.0 movement, which fuses '60s radicalism with the utopian eschatology of digital technology. The ideological outcome may be trouble for all of us.

So what, exactly, is the Web 2.0 movement? As an ideology, it is based upon a series of ethical assumptions about media, culture, and technology. It worships the creative amateur: the self-taught filmmaker, the dorm-room musician, the unpublished writer. It suggests that everyone—even the most poorly educated and inarticulate amongst us—can and should use digital media to express and realize themselves. Web 2.0 "empowers" our creativity, it "democratizes" media, it "levels the playing field" between experts and amateurs. The enemy of Web 2.0 is "elitist" traditional media.

Empowered by Web 2.0 technology, we can all become citizen journalists, citizen videographers, or citizen musicians. Empowered by this technology, we will be able to write in the morning, direct movies in the afternoon, and make music in the evening.

Sounds familiar? It's eerily similar to Marx's seductive promise about individual self-realization in his German Ideology:

> Whereas in communist society, where nobody has one exclusive sphere of activity but each can become accomplished in any branch he wishes, society regulates the general production and thus makes it possible for me to do one thing today and another tomorrow, to hunt in the morning, fish in the afternoon, rear cattle in the evening, criticise after dinner,

> just as I have a mind, without ever becoming hunter, fisherman, shepherd or critic.[1]

Just as Marx seduced a generation of European idealists with his fantasy of self-realization in a communist utopia, so the Web 2.0 cult of creative self-realization has seduced everyone in Silicon Valley. The movement bridges counter-cultural radicals of the '60s such as Steve Jobs with the contemporary geek culture of Google's Larry Page. Between the book-ends of Jobs and Page lies the rest of Silicon Valley including radical communitarians like Craig Newmark (of Craigslist.com), intellectual property communists such as Stanford Law Professor Larry Lessig, economic cornucopians like *Wired* magazine editor Chris "Long Tail" Anderson, journalism professor Jeff Jarvis, and new media moguls Tim O'Reilly and John Battelle.

The ideology of the Web 2.0 movement was perfectly summarized at the Technology Education and Design (TED) show in Monterey in 2005 when Kevin Kelly, Silicon Valley's über-idealist and author of the Web 1.0 Internet utopia *Ten Rules for The New Economy*, said:

> Imagine Mozart before the technology of the piano. Imagine Van Gogh before the technology of affordable oil paints. Imagine Hitchcock before the technology of film. We have a moral obligation to develop technology.[2]

But where Kelly sees a moral obligation to *develop* technology, we should actually have—if we really care about Mozart, Van Gogh and Hitchcock—a moral obligation to *question* the development of technology.

The consequences of Web 2.0 are inherently dangerous for the vitality of culture and the arts. Its empowering promises play upon that legacy of the '60s—the creeping narcissism that Christopher Lasch described so presciently, with its obsessive focus on the realization of the self.[3]

Another word for narcissism is "personalization." Web 2.0 technology personalizes culture so that it reflects ourselves rather than the world around us. Blogs personalize media content so that all we read are our own thoughts.

---

1 KARL MARX & FRIEDRICH ENGELS, THE GERMAN IDEOLOGY (1845), text available at Marxist Internet Archive, **http://www.marxists.org/archive/marx/works/1845/german-ideology/ch01a.htm**.

2 *See* Dan Frost, *Meeting of Minds in Monterey*, SAN FRANCISCO CHRONICLE, Feb. 27, 2005, **http://articles.sfgate.com/2005-02-27/business/17361312_1_digital-world-edward-burtynsky-robert-fischell/2** (quoting Kevin Kelly).

3 *See* CHRISTOPHER LASCH, THE CULTURE OF NARCISSISM: AMERICAN LIFE IN AN AGE OF DIMINISHING EXPECTATIONS (1978).

Online stores personalize our preferences, thus feeding back to us our own taste. Google personalizes searches so that all we see are advertisements for products and services we already use.

Instead of Mozart, Van Gogh, or Hitchcock, all we get with the Web 2.0 revolution is more of ourselves.

Still, the idea of inevitable technological progress has become so seductive that it has been transformed into "laws." In Silicon Valley, the most quoted of these laws, Moore's Law, states that the number of transistors on a chip doubles every two years, thus doubling the memory capacity of the personal computer every two years. On one level, of course, Moore's Law is real and it has driven the Silicon Valley economy. But there is an unspoken ethical dimension to Moore's Law. It presumes that each advance in technology is accompanied by an equivalent improvement in the condition of man.

But as Max Weber so convincingly demonstrated, the only really reliable law of history is the Law of Unintended Consequences.

We know what happened the first time around, in the dot.com boom of the '90s. At first there was irrational exuberance. Then the dot.com bubble popped; some people lost a lot of money and a lot of people lost some money. But nothing really changed. Big media remained big media and almost everything else—with the exception of Amazon.com and eBay—withered away.

This time, however, the consequences of the digital media revolution are much more profound. Apple, Google and Craigslist really are revolutionizing our cultural habits, our ways of entertaining ourselves, our ways of defining who we are. Traditional "elitist" media is being destroyed by digital technologies. Newspapers are in free-fall. Network television, the modern equivalent of the dinosaur, is being shaken by TiVo's overnight annihilation of the 30-second commercial and competition from Internet-delivered television and amateur video. The iPod is undermining the multibillion dollar music industry. Meanwhile, digital piracy, enabled by Silicon Valley hardware and justified by intellectual property communists such as Larry Lessig, is draining revenue from established artists, movie studios, newspapers, record labels, and song writers.

Is this a bad thing? The purpose of our media and culture industries—beyond the obvious need to make money and entertain people—is to discover, nurture, and reward elite talent. Our traditional mainstream media has done this with great success over the last century. Consider Alfred Hitchcock's masterpiece, *Vertigo* and a couple of other brilliantly talented works of the same name: the 1999 book by Anglo-German writer W.G. Sebald, and the 2004 song by Irish rock star Bono. Hitchcock could never have made his expensive, complex movies outside the Hollywood studio system. Bono would never have become Bono without the music industry's super-heavyweight marketing muscle. And

W.G. Sebald, the most obscure of this trinity of talent, would have remained an unknown university professor, had a high-end publishing house not had the good taste to discover and distribute his work. Elite artists and an elite media industry are symbiotic. If you democratize media, then you end up democratizing talent. The unintended consequence of all this democratization, to misquote Web 2.0 apologist Thomas Friedman, is cultural "flattening."[4] No more Hitchcocks, Bonos, or Sebalds. Just the flat noise of opinion—Socrates's nightmare.

While Socrates correctly gave warning about the dangers of a society infatuated by opinion in Plato's Republic, more modern dystopian writers—Huxley, Bradbury, and Orwell—got the Web 2.0 future exactly wrong. Much has been made, for example, of the associations between the all-seeing, all-knowing qualities of Google's search engine and the Big Brother in Nineteen Eighty-Four.[5] But Orwell's fear was the disappearance of the individual right to self-expression. Thus Winston Smith's great act of rebellion in Nineteen Eight-Four was his decision to pick up a rusty pen and express his own thoughts:

> The thing that he was about to do was open a diary. This was not illegal, but if detected it was reasonably certain that it would be punished by death… Winston fitted a nib into the penholder and sucked it to get the grease off…. He dipped the pen into the ink and then faltered for just a second. A tremor had gone through his bowels. To mark the paper was the decisive act.[6]

In the Web 2.0 world, however, the nightmare is not the scarcity, but the over-abundance of authors. Since everyone will use digital media to express themselves, the only decisive act will be to not mark the paper. Not writing as rebellion sounds bizarre—like a piece of fiction authored by Franz Kafka. But one of the unintended consequences of the Web 2.0 future may well be that everyone is an author, while there is no longer any audience.

Speaking of Kafka, on the back cover of the January 2006 issue of *Poets & Writers* magazine, there is a seductive Web 2.0 style advertisement which reads:

> Kafka toiled in obscurity and died penniless. If only he'd had a website … .

---

4 *See* THOMAS FRIEDMAN, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY (2005).

5 *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

6 *Id.* at 6.

Presumably, if Kafka had had a website, it would be located at kafka.com—which is today an address owned by a mad left-wing blog called *The Biscuit Report*. The front page of this site quotes some words written by Kafka in his diary:

> I have no memory for things I have learned, nor things I have read, nor things experienced or heard, neither for people nor events; I feel that I have experienced nothing, learned nothing, that I actually know less than the average schoolboy, and that what I do know is superficial, and that every second question is beyond me. I am incapable of thinking deliberately; my thoughts run into a wall. I can grasp the essence of things in isolation, but I am quite incapable of coherent, unbroken thinking. I can't even tell a story properly; in fact, I can scarcely talk …[7]

One of the unintended consequences of the Web 2.0 movement may well be that we fall, collectively, into the amnesia that Kafka describes. Without an elite mainstream media, we will lose our memory for things learnt, read, experienced, or heard. The cultural consequences of this are dire, requiring the authoritative voice of at least an Allan Bloom,[8] if not an Oswald Spengler.[9] But here in Silicon Valley, on the brink of the Web 2.0 epoch, there no longer are any Blooms or Spenglers. All we have is the great seduction of citizen media, democratized content and authentic online communities. And blogs, of course. Millions and millions of blogs.

---

7 *See The Biscuit Report*, **http://web.archive.org/web/20080225015716/http://www.kafka.com/**.

8 *See* ALLAN BLOOM, THE CLOSING OF THE AMERICAN MIND (1987).

9 *See* OSWALD SPENGLER, THE DECLINE OF THE WEST (1918).

# The Case for Internet Optimism, Part 1: Saving the Net from Its *Detractors*

By Adam Thierer*

## Introduction: Two Schools of Internet Pessimism

Surveying the prevailing mood surrounding cyberlaw and Internet policy circa 2010, one is struck by the overwhelming sense of pessimism regarding the long-term prospects for a better future. "Internet pessimism," however, comes in two very distinct flavors:

1. **Net Skeptics, Pessimistic about the Internet Improving the Lot of Mankind**: The first variant of Internet pessimism is rooted in general skepticism about the supposed benefits of cyberspace, digital technologies, and information abundance. The proponents of this pessimistic view often wax nostalgic about some supposed "good 'ol days" when life was much better (although they can't seem to agree when those were). At a minimum, they want us to slow down and think twice about life in the Information Age and how it's personally affecting each of us. Occasionally, however, this pessimism borders on neo-Ludditism, with some proponents recommending steps to curtail what they feel is the destructive impact of the Net or digital technologies on culture or the economy. Leading proponents of this variant of Internet pessimism include: Neil Postman (*Technopoly: The Surrender of Culture to Technology*), Andrew Keen, (*The Cult of the Amateur: How Today's Internet is Killing our Culture*), Lee Siegel, (*Against the Machine: Being Human in the Age of the Electronic Mob*), Mark Helprin, (*Digital Barbarism*) and, to a lesser degree, Jaron Lanier (*You Are Not a Gadget*) and Nicholas Carr (*The Big Switch* and *The Shallows*).

2. **Net Lovers, Pessimistic about the Future of Openness**: A different type of Internet pessimism is on display in the work of many leading cyberlaw scholars today. Noted academics such as Lawrence Lessig, (*Code and Other Laws of Cyberspace*), Jonathan Zittrain (*The Future of the Internet—And How to Stop It*), and Tim Wu (*The Master Switch: The Rise and Fall of Information Empires*), embrace the Internet and digital technologies, but argue that they are "dying" due to a lack of sufficient care or collective oversight.

---

* Adam Thierer is a senior research fellow at the **Mercatus Center at George Mason University** where he works with the **Technology Policy Program**.

> In particular, they fear that the "open" Internet and "generative" digital systems are giving way to closed, proprietary systems, typically run by villainous corporations out to erect walled gardens and quash our digital liberties. Thus, they are pessimistic about the long-term survival of the Internet that we currently know and love.

Despite their different concerns, two things unite these two schools of techno-pessimism. First, there is an elitist air to their pronouncements; a veritable "the rest of you just don't get it" attitude pervades much of their work. In the case of the Net skeptics, it's the supposed decline of culture, tradition, and economy that the rest of us are supposedly blind to, but which they see perfectly—and know how to rectify. For the Net Lovers, by contrast, we see this attitude on display when they imply that a Digital Dark Age of Closed Systems is unfolding since nefarious schemers in high-tech corporate America are out to suffocate Internet innovation and digital freedom more generally. The Net Lovers apparently see this plot unfolding, but paint the rest of us out to be robotic sheep being led to the cyber-slaughter: We are unwittingly using services (AOL in the old days; Facebook today) or devices (the iPhone and iPad) that play right into the hands of the very corporate schemers determined to trap us in high and tight walled gardens.

Unsurprisingly, this elitist attitude leads to the second belief uniting these two variants of Net pessimism: *Someone* or *something* must intervene to set us on a better course or protect those things that they regard as sacred. The critics either fancy themselves as the philosopher kings who can set things back on a better course, or imagine that such creatures exist in government today and can be tapped to save us from our impending digital doom—whatever it may be.

## Dynamism vs. the Stasis Mentality

In both cases, these two schools of Internet pessimism have (a) over-stated the severity of the respective problems they've identified and (b) failed to appreciate the benefits of *evolutionary dynamism*. I borrow the term "dynamism" from Virginia Postrel, who contrasted the conflicting worldviews of *dynamism* and *stasis* so eloquently in her 1998 book, *The Future and Its Enemies*. Postrel argued that:

> The future we face at the dawn of the twenty-first century is, like all futures left to themselves, "emergent, complex messiness." Its "messiness" lies not in disorder, but in an order that is unpredictable, spontaneous, and ever shifting, a pattern created by millions of uncoordinated, independent decisions.[1]

---

[1] VIRGINIA POSTREL, THE FUTURE AND ITS ENEMIES, at xv (1998).

"[T]hese actions shape a future no one can see, a future that is dynamic and inherently unstable," Postrel noted.[2] But that inherent instability and the uncomfortable realization that the future is, by its very nature, unknowable, leads to exactly the sort of anxieties we see on display in the works of *both* varieties of Internet pessimists today. Postrel made the case for embracing dynamism as follows:

> How we feel about the evolving future tells us who we are as individuals and as a civilization: Do we search for *stasis*—a regulated, engineered world? Or do we embrace *dynamism*—a world of constant creation, discovery, and competition? Do we value stability and control, or evolution and learning? Do we declare with [Tim] Appelo that "we're scared of the future" and join [Judith] Adams in decrying technology as "a killing thing"? Or do we see technology as an expression of human creativity and the future as inviting? Do we think that progress requires a central blueprint, or do we see it as a decentralized, evolutionary process? Do we consider mistakes permanent disasters, or the correctable by-products of experimentation? Do we crave predictability, or relish surprise? These two poles, stasis and dynamism, increasingly define our political, intellectual, and cultural landscape. The central question of our time is what to do about the future. And that question creates a deep divide.[3]

Indeed it does, and that divide is growing deeper as the two schools of Internet pessimism—unwittingly, of course—work together to concoct a lugubrious narrative of impending techno-apocalypse. It makes little difference whether the two schools disagree on the root cause(s) of all our problems; in the end, it's their common call for a more "regulated, engineered world" that makes them both embrace the same stasis mindset. Again, the air of elitism rears its ugly head, Postrel notes:

> Stasist social criticism… brings up the specifics of life only to sneer at or bash them. Critics assume that readers will share their attitudes and will see contemporary life as a problem demanding immediate action by the powerful and wise. This relentlessly hostile view of how we live, and how we may come to live, is distorted and dangerous. It overvalues the tastes of an articulate elite, compares the real world of trade-offs to fantasies of utopia, omits important details and connections,

---

2 *Id.*

3 *Id.* at xiv.

> and confuses temporary growing pains with permanent catastrophes. It demoralizes and devalues the creative minds on whom our future depends. And it encourages the coercive use of political power to wipe out choice, forbid experimentation, short-circuit feedback, and trammel progress.[4]

In this essay, I focus on the first variant of Internet pessimism (the Net skeptics) and discuss their clash with Internet optimists. I form this narrative using the words and themes developed in various books published by Net optimists and pessimists in recent years. I make the dynamist case for what I call "pragmatic optimism" in that I argue that the Internet and digital technologies are reshaping our culture, economy and society—in most ways for the better (as the optimists argue), but not without some serious heartburn along the way (as the pessimists claim). My bottom line comes down to a simple cost-benefit calculus: *Were we really better off in the scarcity era when we were collectively suffering from information poverty*? Generally speaking, I'll take information abundance over information poverty any day! But we should not underestimate or belittle the disruptive impacts associated with the Information Revolution. We need to find ways to better cope with turbulent change in a dynamist fashion instead of embracing the stasis notion that we can roll back the clock on progress or recapture "the good 'ol days"—which actually weren't all that good.

In another essay in this book, I address the second variant of Internet pessimism (the Net lovers) and argue that reports of the Internet's death have been greatly exaggerated. Although the Net lovers will likely recoil at the suggestion that they are not dynamists, closer examination reveals their attitudes and recommendations to be deeply stasist. They fret about a cyber-future in which the Internet might not as closely resemble its opening epoch. Worse yet, many of them agree with what Lawrence Lessig said in his seminal—by highly pessimistic—1999 book, *Code and Other Laws of Cyberspace*, that "we have every reason to believe that cyberspace, left to itself, will not fulfill the promise of freedom. Left to itself, cyberspace will become a perfect tool of control."[5]

Lessig and his intellectual disciples—especially Zittrain and Wu—have continued to forecast a gloomy digital future unless *something is done* to address the Great Digital Closing we are supposedly experiencing. I will argue that, while many of us share their appreciation of the Internet's current nature and its early history, their embrace of the stasis mentality is unfortunate since it forecloses the spontaneous evolution of cyberspace and invites government

---

4 *Id.* at xvii-xviii.

5 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 5-6 (1999).

But first let us turn to the Net skeptics, who don't share such an appreciation of the potential benefits of cyberspace. Rather, their pessimism cuts deep and is rooted in overt hostility to all things digital.

## The Familiar Cycle of Technological Revolutions

The impact of technological change on culture, learning, and morality has long been the subject of intense debate, and every technological revolution brings out a fresh crop of both pessimists and Pollyannas. Indeed, a familiar cycle has repeat itself throughout history whenever new modes of production (from mechanized agriculture to assembly-line production), means of transportation (water, rail, road, or air), energy production processes (steam, electric, nuclear), medical breakthroughs (vaccination, surgery, cloning), or communications techniques (telegraph, telephone, radio, television) have emerged.

The cycle goes something like this: A new technology appears. Those who fear the sweeping changes brought about by this technology see a sky that is about to fall. These "techno-pessimists" predict the death of the old order (which, ironically, is often a previous generation's hotly-debated technology that others wanted slowed or stopped). Embracing this new technology, they fear, will result in the overthrow of traditions, beliefs, values, institutions, business models, and much else they hold sacred. As Dennis Baron, author of *A Better Pencil*, has noted, "the shock of the new often brings out critics eager to warn us away."[6]

The Pollyannas, by contrast, look out at the unfolding landscape and see mostly rainbows in the air. Theirs is a rose-colored world in which the technological revolution *du jour* improves the general lot of mankind. If something must give, then the old ways be damned! For such "techno-optimists," progress means some norms and institutions must adapt—perhaps even disappear—for society to continue its march forward.

Our current Information Revolution is no different. It too has its share of techno-pessimists and techno-optimists who continue to debate the impact of technology on human existence.[7] Indeed, before most of us had even heard of

---

6 DENNIS BARON, A BETTER PENCIL 12 (2009).

7 William Powers, author of Hamlet's BlackBerry: A Practical Philosophy for Building a Good Life in the Digital Age, reminds us that:

> whenever new devices have emerged, they've presented the kinds of challenges we face today—busyness, information overload, that sense of life being out of control. These challenges were as real two millennia ago as they are today, and throughout history, people have been grappling with them and looking for creative ways to manage life in the crowd.

the Internet, people were already fighting about it—or at least debating what the rise of the Information Age meant for our culture, society, and economy.

## Web 1.0 Fight: Postman vs. Negroponte

In his 1992 anti-technology manifesto *Technopoly: The Surrender of Culture to Technology*, the late social critic Neil Postman greeted the unfolding Information Age with a combination of skepticism and scorn.[8] Indeed, Postman's book was a near-perfect articulation of the techno-pessimist's creed. "Information has become a form of garbage," he claimed, "not only incapable of answering the most fundamental human questions but barely useful in providing coherent direction to the solution of even mundane problems."[9] If left unchecked, Postman argued, America's new technopoly—"the submission of all forms of cultural life to the sovereignty of technique and technology"—would destroy "the vital sources of our humanity" and lead to "a culture without a moral foundation" by undermining "certain mental processes and social relations that make human life worth living."[10]

Postman opened his polemic with the well-known allegorical tale found in Plato's *Phaedrus* about the dangers of the written word. Postman reminded us how King Thamus responded to the god Theuth, who boasted that his invention of writing would improve the wisdom and memory of the masses relative to the oral tradition of learning. King Thamus shot back, "the discoverer of an art is not the best judge of the good or harm which will accrue to those who practice it." King Thamus then passed judgment himself about the impact of writing on society, saying he feared that the people "will receive a quantity of information without proper instruction, and in consequence be thought very knowledgeable when they are for the most part quite ignorant."

And so Postman—fancying himself a modern Thamus—cast judgment on today's comparable technological advances and those who would glorify them:

---

> being out of control. These challenges were as real two millennia ago as they are today, and throughout history, people have been grappling with them and looking for creative ways to manage life in the crowd.
>
> WILLIAM POWERS, HAMLET'S BLACKBERRY: A PRACTICAL PHILOSOPHY FOR BUILDING A GOOD LIFE IN THE DIGITAL AGE 5 (2010). Similarly, Baron notes that "from the first days of writing to the present, each time a new communication technology appeared, people had to learn all over again how to use it, how to respond to it, how to trust the documents it produced." DENNIS BARON, A BETTER PENCIL 5 (2009).

8 NEIL POSTMAN, TECHNOPOLY: THE SURRENDER OF CULTURE TO TECHNOLOGY (1992).

9 *Id.* at 69-70.

10 *Id.* at 52, xii.

> we are currently surrounded by throngs of zealous Theuths, one-eyed prophets who see only what new technologies can do and are incapable of imagining what they will *undo*. We might call such people Technophiles. They gaze on technology as a lover does on his beloved, seeing it as without blemish and entertaining no apprehension for the future. They are therefore dangerous and to be approached cautiously. … If one is to err, it is better to err on the side of Thamusian skepticism.[11]

Nicholas Negroponte begged to differ. An unapologetic Theuthian technophile, the former director of the MIT Media Lab responded on behalf of the techno-optimists in 1995 with his prescient polemic, *Being Digital*.[12] It was a paean to the Information Age, for which he served as one of the first high prophets—with *Wired* magazine's back page serving as his pulpit during the many years he served as a regular columnist.

Appropriately enough, the epilogue of Negroponte's *Being Digital* was entitled "An Age of Optimism" and, like the rest of the book, it stood in stark contrast to Postman's pessimistic worldview. Although Negroponte conceded that technology indeed had a "dark side" in that it could destroy much of the old order, he believed that destruction was both inevitable and not cause for much concern. "Like a force of nature, the digital age cannot be denied or stopped," he insisted, and we must learn to appreciate the ways "digital technology can be a natural force drawing people into greater world harmony."[13] (This sort of techno-determinism is a theme found in many of the Internet optimist works that followed Negroponte.)

To Postman's persistent claim that America's technopoly lacked a moral compass, Negroponte again conceded the point but took the glass-is-half-full view: "Computers are not moral; they cannot resolve complex issues like the rights to life and to death. But being digital, nevertheless, does give much cause for optimism."[14] His defense of the digital age rested on the "four very powerful qualities that will result in its ultimate triumph: decentralizing, globalizing, harmonizing, and empowering."[15] Gazing into his techno-crystal ball in 1995, Negroponte forecast the ways in which those qualities would revolutionize society:

---

11 *Id.* at 5.

12 NICHOLAS NEGROPONTE, BEING DIGITAL (1995).

13 *Id.* at 229, 230.

14 *Id.* at 228-9.

15 *Id.* at 229.

> The access, the mobility, and the ability to effect change are what will make the future so different from the present. The information superhighway may be mostly hype today, but it is an understatement about tomorrow. It will exist beyond people's wildest predictions. As children appropriate a global information resource, and as they discover that only adults need learner's permits, we are bound to find new hope and dignity in places where very little existed before.[16]

In many ways, that's the world we occupy today: one of unprecedented media abundance and unlimited communications and connectivity opportunities.

But the great debate about the impact of digitization and information abundance did not end with Postman and Negroponte. Theirs was but Act I in a drama that continues to unfold, and grows more heated and complex with each new character on the stage. "This conflict between stability and progress, security and prosperity, dynamism and stasis, has led to the creation of a major political fault line in American politics," argues Robert D. Atkinson: "On one side are those who welcome the future and look at the New Economy as largely positive. On the other are those who resist change and see only the risks of new technologies and the New Economy." [17] Atkinson expands on this theme in another essay in this collection.[18]

## Web War II

The disciples of Postman and Negroponte are a colorful, diverse lot. The players in Act II of this drama occupy many diverse professions: journalists, technologists, business consultants, sociologists, economists, lawyers, etc. The two camps disagree with each other even more vehemently and vociferously about the impact of the Internet and digital technologies than Postman and Negroponte did.

In Exhibit 1, I have listed the Internet optimists and pessimists alongside their key works. This very binary treatment obviously cannot do justice to the varying shades of optimism or pessimism in in each, but is nonetheless helpful.

---

16 *Id.* at 231.

17 ROBERT D. ATKINSON, THE PAST AND FUTURE OF AMERICA'S ECONOMY 201 (2004). "As a result," he says, "a political divide is emerging between preservationists who want to hold onto the past and modernizers who recognize that new times require new means."

18 Robert D. Atkinson, *Who's Who in Internet Politics: A Taxonomy of Information Technology Policy & Politics*, infra at 162.

**Exhibit 1**

| Theuthian Technophiles ( "The Internet Optimists") | Thamusian Technophobes ( "The Internet Pessimists") |
|---|---|
| Nicholas Negroponte, ***Being Digital*** (1995) | Neil Postman, ***Technopoly: The Surrender of Culture to Technology*** (1993) |
| Kevin Kelly, ***Out of Control: The New Biology of Machines, Social Systems, and the Economic World*** (1995) | Sven Birkerts, ***The Gutenberg Elegies: The Fate of Reading in an Electronic Age*** (1994) |
| Virginia Postrel, ***The Future and Its Enemies*** (1998) | Clifford Stoll, ***High-Tech Heretic: Reflections of a Computer Contrarian*** (1999) |
| James Surowiecki, ***The Wisdom of Crowds*** (2004) | Cass Sunstein, ***Republic.com*** (2001) |
| Chris Anderson, ***The Long Tail: Why the Future of Business is Selling Less of More*** (2006) | Todd Gitlin, ***Media Unlimited: How the Torment of Images and Sounds Overwhelms Our Lives*** (2002) |
| Steven Johnson, ***Everything Bad is Good For You*** (2006) | Todd Oppenheimer, ***The Flickering Mind: Saving Education from the False Promise of Technology*** (2003) |
| Glenn Reynolds, ***An Army of Davids: How Markets and Technology Empower Ordinary People to Beat Big Media, Big Government, and Other Goliaths*** (2006) | Andrew Keen, ***The Cult of the Amateur: How Today's Internet is Killing our Culture*** (2007) |
| Yochai Benkler, ***The Wealth of Networks: How Social Production Transforms Markets and Freedom*** (2006) | Steve Talbott, ***Devices of the Soul: Battling for Our Selves in an Age of Machines*** (2007) |
| Clay Shirky, ***Here Comes Everybody: The Power of Organizing without Organizations*** (2008) | *Nick Carr,* ***The Big Switch: Rewiring the World, from Edison to Google*** (2008) |
| Don Tapscott & Anthony D. Williams, ***Wikinomics: How Mass Collaboration Changes Everything*** (2008) | |

**Exhibit 1 Continued**

| **Theuthian Technophiles ( "The Internet Optimists")** | **Thamusian Technophobes ( "The Internet Pessimists")** |
|---|---|
| Jeff Howe, ***Crowdsourcing: Why the Power of the Crowd Is Driving the Future of Business*** (2008)<br><br>Tyler Cowen, ***Create Your Own Economy: The Path to Prosperity in a Disordered World*** (2009)<br><br>Dennis Baron, ***A Better Pencil: Readers, Writers, and the Digital Revolution*** (2009)<br><br>Jeff Jarvis, ***What Would Google Do?*** (2009)<br><br>Clay Shirky, ***Cognitive Surplus: Creativity and Generosity in a Connected Age*** (2010)<br><br>Nick Bilton, ***I Live in the Future & Here's How It Works*** (2010)<br><br>*Kevin Kelly,* ***What Technology Wants*** (2010) | Lee Siegel, ***Against the Machine: Being Human in the Age of the Electronic Mob*** (2008)<br><br>Mark Bauerlein, ***The Dumbest Generation: How the Digital Age Stupefies Young Americans and Jeopardizes Our Future*** (2008)<br><br>Mark Helprin, ***Digital Barbarism: A Writer's Manifesto*** (2009)<br><br>Maggie Jackson, ***Distracted: The Erosion of Attention and the Coming Dark Age*** (2009)<br><br>John Freeman, ***The Tyranny of E-Mail: The Four-Thousand-Year Journey to Your Inbox*** (2009)<br><br>Jaron Lanier, ***You Are Not a Gadget*** (2010)<br><br>Nick Carr, ***The Shallows: What the Internet Is Doing to Our Brains*** (2010)<br><br>William Powers, ***Hamlet's BlackBerry: A Practical Philosophy for Building a Good Life in the Digital Age*** (2010) |

In Exhibit 2, I have sketched out the major lines of disagreement between these two camps and divided those disagreements into (1) **Cultural / Social beliefs** vs. (2) **Economic / Business beliefs**.

**Exhibit 2**

| Optimists | Pessimists |
|---|---|
| ***Cultural / Social beliefs*** | |
| Net is **participatory** | Net is **polarizing** |
| Net facilitates **personalization** (welcome of "Daily Me" that digital tech allows) | Net facilitates **fragmentation** (fear of the "Daily Me") |
| "a **global village**" | **balkanization** and fears of "**mob rule**" |
| **heterogeneity** / encourages diversity of thought and expression | **homogeneity** / Net leads to close-mindedness |
| allows **self-actualization** | **diminishes personhood** |
| Net a tool of **liberation & empowerment** | Net a tool of frequent **misuse & abuse** |
| Net can help **educate** the masses | **dumbs down** the masses |
| anonymous communication encourages vibrant debate + whistleblowing (a net good) | anonymity debases culture & leads to lack of accountability |
| welcome **information abundance**; believe it will create new opportunities for learning | concern about **information overload**; esp. impact on learning & reading |
| ***Economic / Business beliefs*** | |
| **benefits of "Free"** (increasing importance of "**gift economy**") | **costs of "Free"** ("free" = threat to quality & business models) |
| **mass collaboration** is generally more important | **individual effort** is generally more important |
| embrace of "**amateur**" creativity | superiority of **"professionalism**" |
| stress importance of "**open systems**" of production | stress importance of "**proprietary**" models of production |
| "wiki" model = **wisdom of crowds;** benefits of **crowdsourcing** | "wiki" model = **stupidity of crowds;** collective intelligence is oxymoron; + "**sharecropper**" concern about exploitation of free labor |

When you boil it all down, there are two major points of contention between the Internet optimists and pessimists:

1. The impact of technology on **learning & culture** and the role of **experts vs. amateurs** in that process.

2. The promise—or perils—of **personalization**, for both individuals and society.

Each dispute is discussed in more detail below.

# Differences Over Learning, Culture & "Truth"

As with Theuth and Thamus, today's optimists and skeptics differ about who is the best judge of what constitutes progress, authority, and "truth" and how technological change will impact these things.

## The Pessimists' Critique

Consider the heated debates over the role of "amateur" creations, user-generation content, and peer-based forms of production. Pessimists tend to fear the impact of the Net and the rise of what Andrew Keen has called "the cult of the amateur."[19] They worry that "professional" media or more enlightened voices and viewpoints might be drowned out by a cacophony of competing—but less compelling or enlightened—voices and viewpoints. Without "enforceable scarcity" and protection for the "enlightened class," the pessimists wonder how "high quality" news or "high art" will be funded and disseminated. Some, like Keen, even suggest the need to "re-create media scarcity" to save culture or professional content creators.[20]

Some of these pessimists clearly think in zero-sum terms: More "amateur" production seems to mean less "professional" content creation will be possible. For example, Lee Siegel, author of *Against the Machine: Being Human in the Age of the Electronic Mob*, says that by empowering the masses to have more of a voice, "unbiased, rational, intelligent, and comprehensive news … will become less

---

19 ANDREW KEEN, THE CULT OF THE AMATEUR: HOW TODAY'S INTERNET IS KILLING OUR CULTURE (2007).

20 Andrew Keen, *Art & Commerce: Death by YouTube*, ADWEEK, Oct. 15, 2007, **http://web.archive.org/web/20080107024552/http:/www.adweek.com/aw/magazine/article_display.jsp?vnu_content_id=1003658204**. For a response, see Adam Thierer, *Thoughts on Andrew Keen, Part 2: The Dangers of the Stasis Mentality*, TECHNOLOGY LIBERATION FRONT, Oct. 18, 2007, **http://techliberation.com/2007/10/18/thoughts-on-andrew-keen-part-2-the-dangers-of-the-stasis-mentality**.

and less available."[21] "[G]iving everyone a voice," he argues, "can also be a way to keep the most creative, intelligent, and original voices from being heard."[22]

The centrality of Wikipedia, the collaborative online encyclopedia, to this discussion serves as a microcosm of the broader debate between the optimists and the pessimists. Almost every major optimist and pessimist tract includes a discussion of Wikipedia; it generally serves as a hero in the works of the former and a villain in the latter. For the pessimists, Wikipedia marks the decline of authority, the death of objectivity, and the rise of "mobocracy" since it allows "anyone with opposable thumbs and a fifth-grade education [to] publish anything on any topic."[23] They fear that "truth" becomes more relativistic under models of peer collaboration or crowd-sourced initiatives.[24]

The pessimists also have very little good to say about YouTube, blogs, social networks, and almost all user-generated content. They treat them with a combination of confusion and contempt. "[S]elf-expression is not the same thing as imagination," or art, Siegel argues.[25] Instead, he regards the explosion of online expression as the "narcissistic" bloviation of the masses and argues it is destroying true culture and knowledge. Echoing Postman's assertion that "information has become a form of garbage," Siegel says that the "Under the influence of the Internet, knowledge is withering away into information."[26] Our new age of information abundance is not worth celebrating, he says, because "information is powerlessness."[27]

Some pessimists argue that all the new information and media choices are largely false choices that don't benefit society. For example, Siegel disputes what he regards as overly-romanticized notions of "online participation" and "personal democracy." Keen goes further referring to them as "the great seduction." He says "the Web 2.0 revolution has peddled the promise of

---

21 LEE SIEGEL, AGAINST THE MACHINE: BEING HUMAN IN THE AGE OF THE ELECTRONIC MOB 165 (2008). For a review of the book, *see* Adam Thierer, *Book Review: Lee Siegel's* Against the Machine, TECHNOLOGY LIBERATION FRONT, Oct. 20, 2008, **http://techliberation.com/2008/10/20/book-review-lee-siegel%E2%80%99s-against-the-machine**.

22 *Id.* at 5.

23 Keen, *supra* note 19, at 4.

24 "Wikipedia, with its video-game like mode of participation, and with its mountains of trivial factoids, of shifting mounds of gossip, of inane personal details, is knowledge in the process of becoming information." Siegel, *supra* note *21,* at 152.

25 *Id.* at 52.

26 *Id.* at 152.

27 *Id.* at 148.

bringing more truth to more people … but this is all a smokescreen."[28] "What the Web 2.0 revolution is really delivering," he argues, "is superficial observations of the world around us rather than deep analysis, shrill opinion rather than considered judgment."[29]

Occasionally, the pessimists resort to some fairly immature name-calling tactics while critiquing Information Age culture. "It would be one thing if such a [digital] revolution produced Mozarts, Einsteins, or Raphaels," says novelist Mark Helprin, "but it doesn't... It produces mouth-breathing morons in backward baseball caps and pants that fall down; Slurpee-sucking geeks who seldom see daylight; pretentious and earnest hipsters who want you to wear bamboo socks so the world won't end … beer-drinking dufuses who pay to watch noisy cars driving around in a circle for eight hours at a stretch."[30]

Some pessimists also claim that proliferating new media choices are merely force-fed commercial propaganda or that digital technologies are spawning needless consumerism. "New technologies unquestionably make purchases easier and more convenient for consumers. To this extent, they do help," says the prolific University of Chicago law professor Cass Sunstein. "But they help far less than we usually think, because they accelerate the consumption treadmill without making life much better for consumers of most goods."[31]

In Siegel's opinion, everyone is just in it for the money. "Web 2.0 is the brainchild of businessmen," and the "producer public" is really just a "totalized 'consumerist' society."[32] Countless unpaid bloggers—in it for the love of the conversation and debate—are merely brainwashed sheep whom Siegel argues just don't realize the harm they are doing. "[T]he bloggers are playing into the hands of political and financial forces that want nothing more than to see the critical, scrutinizing media disappear."[33] He reserves special scorn for Net evangelists who believe that something truly exciting is happening with the new online conversation. According to Siegel, they are simply "in a mad rush to earn profits or push a fervent idealism."[34]

The pessimists also fear that these new technologies and trends could have profound ramifications not just for entertainment culture, but also for the

---

28 Keen, *supra* note 19, at 16.

29 *Id.*

30 MARK HELPRIN, DIGITAL BARBARISM: A WRITER'S MANIFESTO 57 (2009).

31 CASS SUNSTEIN, REPUBLIC.COM 121 (2010).

32 Siegel, *supra* note 21, at 128.

33 *Id.* at 141.

34 *Id.* at 25-6.

future of news and professional journalism. They worry about the loss of trusted intermediaries and traditional authorities. For example, Keen fears that Wikipedia, "is almost single-handedly killing the traditional information business."[35] They also argue that "free culture" isn't free at all; it's often just parasitic copying or blatant piracy.

Similarly, Nick Carr and Jaron Lanier worry about the rise of "digital sharecropping," where a small group of elites make money off the back of free labor. To Carr, many new Web 2.0 sites and services "are essentially agglomerations of the creative, unpaid contributions of their members. In a twist on the old agricultural practice of sharecropping, the site owners provide the digital real estate and tools, let the members do all the work, and then harvest the economic riches."[36] And in opening his book, Lanier says "Ultimately these words will contribute to the fortunes of those few who have been able to position themselves as lords of the computing clouds."[37]

Finally, some pessimists worry deeply about the impact of computers and digital technologies on learning. They fear these trends will inevitably result in a general "dumbing down" of the masses or even the disappearance of reading, writing, and other arts. Typifying this view is Mark Bauerlein's *The Dumbest Generation: How the Digital Age Stupefies Young Americans and Jeopardizes Our Future* (2008), but similar concerns are on display in the works of Sven Birkerts,[38] Clifford Stoll,[39] Todd Gitlin,[40] and Todd Oppenheimer.[41]

## The Optimists' Response

The optimists' response is rooted in the belief that, despite their highly disruptive nature, the Internet and new digital technologies empower and enlighten individuals and, therefore, generally benefit society.

---

35 Keen, *supra* note 19, at 131.

36 NICHOLAS CARR, THE BIG SWITCH: REWIRING THE WORLD, FROM EDISON TO GOOGLE 137-8 (2008).

37 LANIER, YOU ARE NOT A GADGET at 1 (2010).

38 SVEN BIRKERTS, THE GUTENBERG ELEGIES: THE FATE OF READING IN AN ELECTRONIC AGE (1994).

39 CLIFFORD STOLL, HIGH-TECH HERETIC: REFLECTIONS OF A COMPUTER CONTRARIAN (1999).

40 TODD GITLIN, MEDIA UNLIMITED: HOW THE TORMENT OF IMAGES AND SOUNDS OVERWHELMS OUR LIVES (2002).

41 TODD OPPENHEIMER, THE FLICKERING MIND: SAVING EDUCATION FROM THE FALSE PROMISE OF TECHNOLOGY (2003).

The optimists tend to argue that new modes of production (especially peer-based production) will offer an adequate—if not superior—alternative to traditional modalities of cultural or artistic production. Despite displacing some institutions and cultural norms, they claim digital technologies create more opportunities. They speak of "collective intelligence,"[42] the "wisdom of crowds,"[43] the importance of peer production,[44] and the rise of what futurist Alvin Toffler first referred to as "prosumers."[45] "There has been a fundamental shift in the balance of power between consumers and salesmen over the last generation and it points in the direction of consumers," Tyler Cowen argues in his book, *Create Your Own Economy: The Path to Prosperity in a Disordered World.*[46]

The peer production trend is stressed in works such as *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, by Yochai Benkler,[47] and *Wikinomics: How Mass Collaboration Changes Everything*, by Don Tapscott and Anthony D. Williams.[48] "A new economic democracy is emerging in which we all have a lead role," claim Tapscott and Williams,[49] because "the economics of production have changed significantly."[50]

Most optimists also argue that new business models will evolve to support what had previously been provided by professional content creators or news providers. Glenn Reynolds (*An Army of Davids*) and Dan Gillmor (*We the Media*) refer of the rise of "we-dia" (user-generated content and citizen journalism) that is an increasingly important part of the modern media landscape. Gillmor, a former *San Jose Mercury News* columnist, speaks of "a modern revolution … because technology has given us a communications toolkit that allows anyone to become a journalist at little cost and, in theory, with global reach. Nothing like this has ever been remotely possible before," he argues.[51] And the optimists generally don't spend much time lamenting the obliteration of large media

---

42 HENRY JENKINS, CONVERGENCE CULTURE: WHERE OLD AND NEW MEDIA COLLIDE 4 (2006).

43 JAMES SUROWIECKI, THE WISDOM OF CROWDS (2004).

44 DON TAPSCOTT & ANTHONY D. WILLIAMS, WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING 1, 67 (2008).

45 ALVIN TOFFLER, THE THIRD WAVE 265 (1980).

46 TYLER COWEN, CREATE YOUR OWN ECONOMY: THE PATH TO PROSPERITY IN A DISORDERED WORLD 117 (2009).

47 YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006).

48 Tapscott & Williams, *supra* note 44, at 15.

49 *Id.* at 15.

50 *Id.* at 68.

51 DAN GILLMOR, WE THE MEDIA at xii (2004).

institutions, either because they think little of their past performance or, alternatively, believe that whatever "watchdog" role they played can be filled by others. "We are seeing the emergence of new, decentralized approaches to fulfilling the watchdog function and to engaging in political debate and organization," Benkler claims.[52]

Optimists also believe that the Information Age offers real choices and genuine voices, and they vociferously dispute charges of diminished quality by prosumers, amateur creators, new media outlets, and citizen journalists. Moreover, they do not fear the impact of these new trends and technologies on learning or culture. "Surely the technophobes who romanticize the pencil don't want to return us to the low literacy rates that characterized the good old days of writing with pencils and quills," Baron asks. "Still, a few critics object to the new technologies because they enable too many people to join the guild of writers, and they might paraphrase Thoreau's objection to the telegraph: these new computer writers, it may be, have nothing to say to one another."[53]

Finally, in addressing the sharecropper concern raised by Carr and Lanier, the optimists insist most people aren't in it for the money. Shirky notes that "Humans intrinsically value a sense of connectedness," and much of what they do in the social media world is a true labor of love.[54] "Amateurs aren't just pint-sized professionals; people are sometimes happy to do things for reasons that are incompatible with getting paid," he says.[55] Mostly they do it for love of knowledge or a belief in the importance of "free culture," the optimists claim.

## The Debate Over the Promise—or Perils—of Personalization

Optimists and pessimists tend to agree that the Internet and "Web 2.0" is leading to more "personalized" media and information experiences. They disagree vehemently, however, on whether this is good or bad. They particularly disagree on what increased information customization means for participatory democracy and the future of relations among people of diverse backgrounds and ideologies. Finally, they differ on how serious of a problem "information overload" is for society and individuals.

---

52 Benkler, *supra* note 47, at 11.

53 DENNIS BARON, A BETTER PENCIL 159 (2009).

54 CLAY SHIRKY, COGNITIVE SURPLUS: CREATIVITY AND GENEROSITY IN A CONNECTED AGE 58-9 (2010).

55 *Id.*

## The Optimists' Case

Let's take the optimists first this time.

The optimists tend to embrace what Nicholas Negroponte first labeled "The Daily Me" (*i.e.*, hyper-personalized news, culture, and information). In 1995, Negroponte asked us to:

> Imagine a future in which your interface agent can read every newswire and newspaper and catch every TV and radio broadcast on the planet, and then construct a personalized summary. This kind of newspaper is printed in an edition of one.…
>
> Imagine a computer display of news stories with a knob that, like a volume control, allows you to crank personalization up or down. You could have many of these controls, including a slider that moves both literally and politically from left to right to modify stories about public affairs. These controls change your window onto the news, both in terms of size and its editorial tone. In the distant future, interface agents will read, listen to, and look at each story in its entirety. In the near future, the filtering process will happen by using headers, those bits about bits.[56]

That future came about sooner than even Negroponte could have predicted. We all have a "Daily Me" at our disposal today thanks to RSS feeds, Facebook, Google Alerts, Twitter, email newsletters, instant messaging, and so on. These tools, among others, can provide tailored, automated search results served up instantaneously. The optimists argue that this increased tailoring and personalization of our media experiences empowers heretofore silenced masses. This worldview is typified by the title of Glenn Reynolds' book: *An Army of Davids: How Markets and Technology Empower Ordinary People to Beat Big Media, Big Government and Other Goliaths*.[57] The optimists argue that our "participatory culture" promotes greater cultural heterogeneity and gives everyone a better chance to be heard. "In a world of media convergence, every important story gets told, every brand gets sold, and every consumer gets courted across multiple media platforms," says Henry Jenkins, author of *Convergence Culture*.[58]

---

56 Negroponte, *supra* note 12, at 153-54.

57 GLENN REYNOLDS, AN ARMY OF DAVIDS: HOW MARKETS AND TECHNOLOGY EMPOWER ORDINARY PEOPLE TO BEAT BIG MEDIA, BIG GOVERNMENT AND OTHER GOLIATHS (2006).

58 HENRY JENKINS, CONVERGENCE CULTURE: WHERE OLD AND NEW MEDIA COLLIDE 3 (2006). Tapscott & Williams, *supra* note 44, at 41.

Again, they stress the empowering nature of digital technology as a good in and of itself. "The mass amateurization of publishing undoes the limitations inherent in having a small number of traditional press outlets," Shirky claims.[59] This leads to greater openness, transparency, exposure to new thinking and opinions, and a diversity of thought and societal participation. Shirky speaks of the "cognitive surplus" unleashed by these changes and its myriad benefits for society and culture:

> The harnessing of our cognitive surplus allows people to behave in increasingly generous, public, and social ways, relative to their old status as consumers and couch potatoes. The raw material of this change is the free time available to us, time we can commit to projects that range from the amusing to the culturally transformative. … Flexible, cheap, and inclusive media now offers us opportunities to do all sorts of things we once didn't do. In the world of "the media," we were like children, sitting quietly at the edge of a circle and consuming whatever the grown-ups in the center of the circle produced. That has given way to a world in which most forms of communication, public and private, are available to everyone in some form.[60]

Shirky even suggests that "The world's cognitive surplus is so large that small changes can have huge ramifications in aggregate," and have beneficial impacts on politics, advocacy, and "generosity."

When it comes to concerns about "information overload," most optimists see little reason for concern. Tyler Cowen argues that using search tools like Google and other information gathering and processing technologies actually "lengthen our attention spans in another way, namely by allowing greater specialization of knowledge:"[61]

> We don't have to spend as much time looking up various facts and we can focus on the particular areas of interest, if only because general knowledge is so readily available. It's never been easier to wrap yourself up in a long-term intellectual project, yet without losing touch with the world around you.

---

59 CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS 65 (2008).

60 CLAY SHIRKY, COGNITIVE SURPLUS, *supra* note 54, at 63.

61 TYLER COWEN, CREATE YOUR OWN ECONOMY: THE PATH TO PROSPERITY IN A DISORDERED WORLD 55 (2009).

> As for information overload, it is you who chooses how much "stuff" you want to experience and how many small bits you want to put together … . The quantity of information coming our way has exploded, but so has the quality of our filters.[62]

Chris Anderson previously made this point in his book, *The Long Tail*. Anderson defined filters as "the catch-all phrase for recommendations and all the other tools that help you find quality in the Long Tail" and noted that "these technologies and services sift through a vast array of choices to present you with the ones that are most right for you."[63] "The job of filters is to screen out [the] noise" or information clutter, Anderson says.[64] Cowen argues that the filtering technologies are getting better at this sifting and processing process, *but so too are humans*, he says. The key to this, he argues, is that we are getting better at "ordering" information.

On balance, therefore, the optimists argue that personalization benefits our culture and humanity. Dennis Baron concludes, "English survives, conversation thrives online as well as off, and on balance, digital communications seems to be enhancing human interaction, not detracting from it."[65]

## The Pessimists' Response

The pessimists argue that all this Pollyannaish talk about a new age of participatory democracy is bunk. Instead of welcoming increased information and media personalization, they lament it. They fear that "The Daily Me" that the optimists laud will lead to homogenization, close-mindedness, an online echo-chamber, information overload, corporate brainwashing, *etc.* Worst, hyper-customization of websites and online technologies will cause extreme social "fragmentation," "polarization," "balkanization," "extremism" and even the decline of deliberative democracy.[66]

Siegel and Keen are probably the most searing in this critique. To Siegel, for example, the "Daily Me" is little more that the creation of a "narcissistic culture" in which "exaggeration" and the "loudest, most outrageous, or most

---

62 *Id.*

63 CHRIS ANDERSON, THE LONG TAIL 108 (2006).

64 *Id.* at 115.

65 DENNIS BARON, A BETTER PENCIL 135 (2009).

66 Carr worries that every little choice moves us close toward such social isolation: "Every time we subscribe to a blog, add a friend to our social network, categorize an email message as spam, or even choose a site from a list of search results, we are making a decision that defines, in some small way, whom we associate with and what information we pay attention to." NICHOLAS CARR, THE BIG SWITCH: REWIRING THE WORLD, FROM EDISON TO GOOGLE 160 (2008).

extreme voices sway the crowd of voices this way; the cutest, most self-effacing, most ridiculous, or most transparently fraudulent of voices sway the crowd of voices that way."[67] He calls Web 2.0 "democracy's fatal turn" in that, instead of "allowing individuals to create their own cultural and commercial choices," it has instead created "a more potent form of homogenization."[68] Keen fears the rise of "a dangerous form of digital narcissism" and "the degeneration of democracy into the rule of the mob and the rumor mill."[69]

This echoes concerns first raised by Cass Sunstein in his 2001 book *Republic.com*.[70] In that book, Sunstein referred to Negroponte's "Daily Me" in contemptuous terms, saying that the hyper-customization of websites and online technologies was causing extreme social fragmentation and isolation that could lead to political extremism. "A system of limitless individual choices, with respect to communications, is not necessarily in the interest of citizenship and self-government," he wrote.[71] Sunstein was essentially claiming that the Internet is breeding a dangerous new creature: Anti-Democratic Man.[72] "Group polarization is unquestionably occurring on the Internet," he proclaimed, and it is weakening what he called the "social glue" that binds society together and provides citizens with a common "group identity."[73] If that continues unabated, Sunstein argued, the potential result could be nothing short of the death of deliberative democracy and the breakdown of the American system of government.

Some of the pessimists, like Keen, go further and claim that "the moral fabric of our society is being unraveled by Web 2.0. It seduces us into acting on our most deviant instincts and allows us to succumb to our most destructive vices. And it is corroding the values we share as a nation."[74] Nick Carr summarizes the views of the pessimists when he says: "it's clear that two of the hopes most dear to the Internet optimists—that the Web will create a more bountiful culture and that it will promote greater harmony and understanding—should be treated

---

67 Siegel, *supra* note 21, at 79.

68 *Id.* at 67.

69 Keen, *supra* note 19, at 54-5.

70 CASS SUNSTEIN, REPUBLIC.COM (2001).

71 *Id.* at 123.

72 *See* Adam Thierer, *Saving Democracy from the Internet*, REGULATION (Fall 2001) 78-9, **http://www.cato.org/pubs/regulation/regv24n3/inreview.pdf**.

73 Sunstein, *supra*, at 71, 89.

74 Keen, *supra* note 19, at 163.

with skepticism. Cultural impoverishment and social fragmentation seem equally likely outcomes."[75]

Another common theme in the works of the pessimists is summarized by the title of Siegel's book (*Against the Machine*). They fear the "mechanization of the soul"[76] or humanity's "surrender" to "the machine revolution."[77] In opening of *You Are Not a Gadget*, Lanier fears that "these words will mostly be read by nonpersons—automatons or numb mobs composed of people who are no longer acting as individuals."[78] "The trick is not to subject man and nature to the laws of the machine," says Helprin, "but rather to control the machine according to the laws and suggestions of nature and human nature. To subscribe to this does not make one a Luddite."[79]

Finally, the pessimists are also concerned about the impact of online anonymity on human conduct and language. They argue anonymity leads to less accountability or, more simply, just plain bad manners. "If our national conversation is carried out by anonymous, self-obsessed people unwilling to reveal their real identities, then," Keen argues, "community denigrates into anarchy."[80]

## So Who's Right?

On balance, the optimists generally have the better of the argument today. We really are better off in an age of information abundance than we were in the scarcity era we just exited. Nonetheless, the pessimists make many fair points that deserve to be taken seriously. But they need a more reasonable articulation of those concerns and a constructive plan for how to move forward without a call for extreme reactionary solutions.

A hybrid approach here might be thought of as "pragmatic optimism," which attempts to rid the optimist paradigm of its kookier, pollyannish thinking while also taking into account some of the very legitimate concerns raised by the pessimists, but rejecting its caustic, neo-Luddite fringe elements and stasis mentality in the process.

---

75 Carr, *supra* note 36, at 167.

76 Helprin, *supra* note 30, at 100.

77 *Id.* at 9, 100.

78 Lanier, *supra* note 37, at 1.

79 Helprin, *supra* note 30, at 144.

80 Keen, *supra* note 30, at 80.

## Thoughts on the Pessimists

First and foremost, if they hope to be taken more seriously, Net skeptics need better spokespersons. Or, they at least need a more moderated, less hysterical tone when addressing valid concerns raised by technological progress. It's often difficult to take the pessimists seriously when they exude outright hostility to most forms of technological progress. Most of them deny being high-tech troglodytes, but the tone of some of their writing, and the thrust of some of their recommendations, exhibit occasional Luddite tendencies—even if they don't always come out and call for extreme measures to counteract dynamism.

Moreover, the name-calling they sometimes engage in, and their derision for the digital generation can be just as insulting and immature as the online "mob" they repeatedly castigate in their works. Too often, their criticism devolves into philosophical snobbery and blatant elitism, as in the works of Helprin, Siegel, and Keen. Constantly looking down their noses at digital natives and all "amateur" production isn't going to help them win any converts or respect for their positions. Moreover, one wonders if they have fingered the right culprit for civilization's supposed decline, since most of the ills they identify predate the rise of the Internet.

The pessimists are often too quick to proclaim the decline of modern civilization by looking only to the baser elements of the blogosphere or the more caustic voices of cyberspace. The Internet is a cultural and intellectual bazaar where one can find both the best and the worst of humanity on display at any given moment. True, "brutishness and barbarism," as Helprin calls it,[81] can be found on many cyber-corners, but not *all* of its corners. And, contrary to Helprin's assertion that blogging "begins the mad race to the bottom,"[82] one could just as easily cite countless instances of the healthy, unprecedented conversations that blogs have enabled about a diverse array of topics.

Their claim that the "Daily Me" and information specialization will lead to a variety of ills is also somewhat overblown. It's particularly hard to accept Sunstein and Carr's claims that increased personalization is breeding "extremism," "fanaticism" and "radicalization." A recent study by Matthew Gentzkow and Jesse M. Shapiro of the University of Chicago Booth School of Business lent credibility to this, finding "no evidence that the Internet is becoming more segregated over time" or leading to increased polarization as Sunstein and other pessimists fear.[83] Instead, their findings show that the Net

---

81 Helprin, *supra* note 30, at 32.

82 *Id.* at 42.

83 Matthew Gentzkow & Jesse M. Shapiro, *Ideological Segregation Online and Offline*, CHICAGO BOOTH WORKING PAPER No. 10-19, April 5, 2010, **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588920**.

has encouraged more ideological integration and is actually driving us to experience new, unanticipated viewpoints.[84]

While it's true the Internet has given some extremists a new soapbox to stand on and spew their hatred and stupidity, the fact is that such voices and viewpoints have always existed. The difference today is that the Internet and digital platforms have given us a platform to counter such societal extremism. As the old saying goes, the answer to bad speech is more speech—not a crackdown on the underlying technologies used to convey speech. It should not be forgotten that, throughout history, most extremist, totalitarian movements rose to power by taking over the scarce, centralized media platforms that existed in their countries. The decentralization of media makes such a take-over far less plausible to imagine.

Sometimes the pessimists seem to just be suffering from a bit of old-fogeyism. Lanier, for example, dismisses most modern culture as "retro" and "a petty mashup of preweb culture."[85] "It's as if culture froze just before it became digitally open, and all we can do now is mine the past like salvagers picking over a garbage dump."[86] Many pessimists are guilty of such hyper-nostalgia about those mythical "good 'ol days" when all was supposedly much better. It's a common refrain we've heard from many social and cultural critics before. But such cultural critiques are profoundly subjective. Many pessimists simply seem to be well passed the "adventure window."[87] The willingness of humans to try new things and experiment with new forms of culture—our "adventure window"—fades rapidly after certain key points in life, as we gradually settle in our ways. Many cultural critics and average folk alike seem convinced the best days are behind us and the current good-for-nothing generation and their new-fangled gadgets and culture are garbage. At times this devolves into a full-blown moral panic.[88] "It's perfectly normal and probably healthy to examine whether these changes are good or bad," says *New York Times* blogger Nick Bilton, author of *I Live in the Future & Here's How It Works*. "But we'll also no doubt

---

84 "This study suggests that Internet users are a bunch of ideological Jack Kerouacs. They're not burrowing down into comforting nests. They're cruising far and wide looking for adventure, information, combat and arousal." David Brooks, *Riders on the Storm*, NEW YORK TIMES, April 19, 2010, **http://www.nytimes.com/2010/04/20/opinion/20brooks.html**.

85 Lanier, *supra* note 37, at 131.

86 *Id.* at 133.

87 Adam Thierer, *The "Adventure Window," Radio Formats and Media Ownership Rules*, TECHNOLOGY LIBERATION FRONT, Aug. 16, 2006, **http://techliberation.com/2006/08/16/the-adventure-window-radio-formats-and-media-ownership-rules**.

88 *See* Adam Thierer, *Parents, Kids & Policymakers in the Digital Age: Safeguarding Against 'Techno-Panics,'* INSIDE ALEC (July 2009) at 16-7, **http://www.alec.org/am/pdf/Inside_July09.pdf**.

look back at many of the debates a generation from now and see that a lot of these fears were inflated and maybe a bit ridiculous, too."[89]

The "sharecropper" concern raised by Carr and Lanier is also over-stated. This logic ignores the non-monetary benefits that many of us feel we extract from today's online business models and social production processes. Most of us feel we get a lot back as part of this new value exchange. Carr and Lanier are certainly correct that Google, Facebook, MySpace, and a lot of other Net middlemen are getting big and rich based on all the user-generated content flowing across their sites and systems. On the other hand, most cyber-citizens extract enormous benefits from the existence of those (mostly free and constantly improving) platforms and services. It's a very different sort of value exchange and business model than in the past, but we are adjusting to it.

Yet for all of Wikipedia's value as a reference of first (but certainly not final) resort, the pessimists have almost nothing good to say about it. Much the same goes for open source and other collaborative efforts. They don't appear willing to accept the possibility of any benefits coming from collective efforts. And they wrongly treat the rise of collective / collaborative efforts as a zero-sum game; imagining it represents a net loss of individual effort & "personhood." That simply doesn't follow. The masses have been given more of a voice thanks to the rise of Web 2.0 collaborative technologies and platforms, but that doesn't mean that media "professionals" don't still exist. Most bloggers, for example, build their narratives around facts and stories found in respected "mainstream media" outlets. It's true that those outlets must now compete in a broad sense with many new forms of competition for human attention, but it doesn't mean they still won't play a lead role in the new information ecosystem.

Most of all, the pessimists can and must come to terms with the Information Revolution while offering more constructive *and practical* solutions to legitimately difficult transitional problems created by disintermediating influences of the digital technologies and Net. After all, practically speaking, what would the pessimists have us do if we can't mitigate the problems they identify? "Whatever the mix of good and bad," Notes *Wall Street Journal* columnist Gordon Crovitz, "technology only advances and cannot be put back in the bottle."[90] Would the pessimists have us attempt to put the digital genie back in bottle with burdensome restrictions on technology or the creation of a permissions-based system of innovation? "[W]hether it's good for society or

---

89 NICK BILTON, I LIVE IN THE FUTURE & HERE'S HOW IT WORKS 63 (2010).

90 L. Gordon Crovitz, *Is Technology Good or Bad? Yes.* WALL STREET JOURNAL, Aug. 23, 2010, **http://online.wsj.com/article/SB10001424052748703579804575441461191438330.html**.

bad … is somewhat irrelevant at this point," argues Nick Bilton.[91] "There's no turning back the clock." Similarly, Ben Casnocha has correctly noted that:

> the wind at the backs of *all* techno-optimists … [is] the forward momentum of technological development. You cannot turn back the clock. It is impossible to envision a future where there is *less* information and fewer people on social networks. It is very possible to envision increasing abundance along with better filters to manage it. The most constructive contributions to the debate, then, heed Moore's Law in the broadest sense and offer specific suggestions for how to harness the change for the better.[92]

Regrettably, most of the leading Net pessimists have failed to do this in their work. However, good templates for how to accomplish this can be found in recent books by William Powers (*Hamlet's BlackBerry: A Practical Philosophy for Building a Good Life in the Digital Age*)[93] and John Freeman (*The Tyranny of E-Mail: The Four-Thousand-Year Journey to Your Inbox*).[94] These authors, although somewhat pessimistic in their view of technology's impact on life and learning, offer outstanding self-help tips and plans of action about how to reasonably assimilate new information technologies into our lives. Their key insight: the Internet and digital technologies aren't going away, so we must figure out how to deal with them in a responsible manner—both individually and collectively. It's essential other pessimists come to grips with that fact.

The pessimists are at their best when highlighting the very legitimate concerns about the challenges that accompany technological change, including the impact of the digital revolution on "professional" media, the decline of authority

---

91 Bilton, *supra* note 89, at 216.

92 Ben Casnocha, *RSSted Development*, THE AMERICAN, July 1, 2009, **http://www.american.com/archive/2009/june/rssted-development**. Clay Shirky has also noted that "There is never going to be a moment when we as a society ask ourselves, 'Do we want this? Do we want the changes that the new flood of production and access and spread of information is going to bring about?'" Clay Shirky, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS 73 (2008).

93 WILLIAM POWERS, HAMLET'S BLACKBERRY: A PRACTICAL PHILOSOPHY FOR BUILDING A GOOD LIFE IN THE DIGITAL AGE (2010). *See also* Adam Thierer, *Coping with Information Overload: Thoughts on* Hamlet's BlackBerry *by William Powers*, TECHNOLOGY LIBERATION FRONT, Sept. 6, 2010, **http://techliberation.com/2010/09/06/coping-with-information-overload-thoughts-on-hamlets-blackberry-by-william-powers**.

94 JOHN FREEMAN, THE TYRANNY OF E-MAIL: THE FOUR-THOUSAND-YEAR JOURNEY TO YOUR INBOX (2009). For a review of the book, *see* Adam Thierer, *Can Humans Cope with Information Overload? Tyler Cowen & John Freeman Join the Debate,* TECHNOLOGY LIBERATION FRONT, Aug. 23, 2009, **http://techliberation.com/2009/08/23/can-humans-cope-with-information-overload-tyler-cowen-john-freeman-join-the-debate**.

among trusted experts and intermediaries, and the challenge of finding creative ways to fund "professional" media and art going forward.

## Thoughts on the Optimists

Again, the optimists currently have the better of this debate: Web 2.0 is generally benefiting culture and society. It is almost impossible to accept that society has not benefited from the Internet and new digital technologies compared to the past era of information scarcity. The Digital Revolution has greatly empowered the masses and offered them more informational inputs.

But the optimists need to be less pollyannaish and avoid becoming the "technopolists" (or digital utopians) that Postman feared were taking over our society. There's often too much Rousseauian romanticism at work in some optimist writings. Just as the pessimists are often guilty assuming the Net and digital technologies are responsible for far too many ills, the optimists occasionally do the opposite by engaging in what Nick Carr labels "the Internet's liberation mythology." The Internet isn't remaking man or changing human nature in any fundamental way. Nor can it liberate us from all earthly constraints or magically solve all of civilization's problems. Moreover, when it comes to economics, all this talk about the Long Tail being "the future of business" (Chris Anderson) and of "Wikinomics … changing everything through mass collaboration," (Tapscott and Williams) verges on irrational techno-exuberance.

In particular, optimists often overplay the benefits of collective intelligence, collaboration, and the role of amateur production. They are occasionally guilty of "the elevation of information to metaphysical status" as Postman lamented.[95] For example, the optimists could frame "Wiki" and peer-production models as a *complement* to professional media, not a *replacement* for it. Could the equivalent of *The New York Times* really be cobbled together by amateurs daily? It seems highly unlikely. And why aren't there any compelling open source video games? Similarly, free and open source software (FOSS) has produced enormous social / economic benefits, but it would be foolish to believe that FOSS (or "wiki" models) will replace *all* proprietary business models. Each model or mode of production has its place and purpose and they will continue to co-exist and compete.

We wouldn't necessarily be better off if all the "professional" media producers and old intermediaries disappeared, even if it is no doubt true that many of them will. Some optimists play the "old media just doesn't get it" card far too often and snobbishly dismiss many producers' valid concerns and efforts to reinvent themselves.

---

95 Postman, *supra* note 8, at 61.

There's also a big difference between "remix culture" and "rip-off culture." Many optimists turn a blind eye to blatant copyright piracy, for example, or even defend it as either a positive development or simply inevitable. Remix culture generally enhances and extends culture and creativity. But blatant content piracy deprives many of society's most gifted creators of the incentive to produce culturally beneficial works. Likewise, hacking, circumvention, and reverse-engineering all play an important and legitimate role in our new digital economy, but one need not accept the legitimacy of those activities when conducted for nefarious purposes (think identity theft or chip-modding to facilitate video game piracy.)

The optimists should be cautious about predicting sweeping positive changes from the Internet or Web 2.0 technologies. Consider Shirky's generally upbeat assessment of the impact of "cognitive surplus." There's a lot of fluffy talk and anecdotal examples in Shirky's book about how the cognitive surplus spawned by cyber-life has affected politics, advocacy, and "generosity," but I think it's a stretch to imply that the Net is going to upend political systems. In another essay in this collection, Evgeny Morozov challenges Shirky on some of these points, arguing that "the Internet will not automatically preserve—never mind improve—the health of democratic politics."[96] He's right. That digital technology and the Internet will help reshape society and politics to some degree is indisputable. But that doesn't mean the Net will radically reshape political systems or human nature anytime soon.

Finally, the optimists would be wise to separate themselves from those extreme voices in their community who speak of the "noosphere" and "global consciousness" and long for the eventual singularity. While he doesn't go quite so far, *Wired* editor Kevin Kelly often pushes techno-optimism to its extreme. In his latest book, *What Technology Wants*, Kelly speaks of what he calls "the technium" as a "force" or even a living organism that has a "vital spirit" and which "has its own wants" and "a noticeable measure of autonomy."[97] Treating technology as an autonomous force is silly, even dangerous, thinking. It is to imbue it with attributes and feelings that simply do not exist and would probably not be desirable if they did. Yet, some optimists speak in fatalistic terms and make such an outcome seem desirable. They sound like they long for life in *The Matrix*—"Bring on sentient robot masters and the Singularity!" Thus does an optimist cross over into the realm of quixotic techno-utopianism.

Optimists need to place technological progress in context and appreciate that, as Postman argued, there *are* some moral dimensions to technological progress that deserve attention. Not all change is good change. The optimists need to be

---

96 Evgeny Morozov, *Will the Net Liberate the World?*, infra at 443.

97 KEVIN KELLY, WHAT TECHNOLOGY WANTS 198, 41, 15, 13 (2010).

mature enough to understand and address the downsides of digital life without dismissing its critics. On the other hand, some of those moral consequences are profoundly *positive*, which the pessimists usually fail to appreciate or even acknowledge.

## Conclusion: Toward "Pragmatic Optimism"

Again, I believe the optimists currently have the better of this debate. It's impossible for me to believe we were better off in an era of information poverty and un-empowered masses. I'll take information overload over information poverty any day! As Dennis Baron puts it: "The Internet is a true electronic frontier where everyone is on his or her own: all manuscripts are accepted for publication, they remain in virtual print forever, and no one can tell writers what to do."[98]

The rise of the Internet and digital technologies has empowered the masses and given everyone a soapbox on which to speak to the world. Of course, that doesn't necessarily mean all of them will have something interesting to say! We shouldn't exalt user-generated content as a good in and of itself. It's quality, not volume, that counts. But such human empowerment is worth celebrating, despite its occasional downsides.[99] Abundance is better than the old analog world of few choices and fewer voices.

However, the pessimists have some very legitimate concerns regarding how the passing of the old order might leave society without some important things. For example, one need not endorse bailouts for a dying newspaper industry to nonetheless worry about the important public service provided by investigative journalists: Who will take up those efforts if large media institutions go under because of digital disintermediation?

The skeptics are also certainly correct that each of us should think about how to better balance new technologies and assimilate them into our lives and the lives of our families and communities. For example, children need to learn new "digital literacy" and "cyber-citizenship" skills to be savvy Netizens.

To be clear, I am *not* suggesting that these questions should be answered by government. There exist many other ways that society can work to preserve

---

98 DENNIS BARON, A BETTER PENCIL 25 (2009).

99 "Just as well-meaning scientists and consumers feared that trains and comic books and television would rot our brains and spoil our minds, I believe many of the skeptics and worrywarts today are missing the bigger picture, the greater value that access to new and faster information is bringing us." Nick Bilton, I LIVE IN THE FUTURE & HERE'S HOW IT WORKS 136 (2010).

important values and institutions without embracing the stasis mentality and using coercion to accomplish that which should be pursued voluntarily.

As noted, the nostalgia the pessimists typically espouse for the past is a common refrain of cultural and technological critics who fear our best days are behind us. The truth typically proves less cataclysmic, of course. The great thing about humans is that we adapt better than other creatures. When it comes to technological change, resiliency is hard-wired into our genes. "The techno-apocalypse never comes," notes *Slate's* Jack Shafer, because "cultures tend to assimilate and normalize new technology in ways the fretful never anticipate."[100] We learn how to use the new tools given to us and make them part of our lives and culture. Indeed, we have lived through revolutions more radical than the Information Revolution. We *can* adapt and learn to live with some of the legitimate difficulties and downsides of the Information Age.

Generally speaking, the sensible middle ground position is "pragmatic optimism": We should embrace the amazing technological changes at work in today's Information Age but with a healthy dose of humility and appreciation for the disruptive impact and pace of that change. We need to think about how to mitigate the negative impacts associated with technological change without adopting the paranoid tone or Luddite-ish recommendations of the pessimists.

I'm particularly persuaded by the skeptics' call for all of us to exercise some restraint in terms of the role technology plays in our own lives. While pessimists from Plato and Postman certainly went too far at times, there is more than just a kernel of truth to their claim that, taken to an extreme, technology can have a deleterious impact on life and learning. We need to focus on the Aristotelian mean. We must avoid neo-Luddite calls for a return to "the good 'ol days" on the one hand, while also rejecting techno-utopian Pollyannaism on the other. We need not go to "all or nothing" extremes.

In the end, however, I return to the importance of evolutionary dynamism and the importance of leaving a broad sphere for continued experimentation by individuals and organizations alike. Freedom *broadly construed* is valuable in its own right—even if not all of the outcomes are optimal. As Clay Shirky rightly notes:

> This does not mean there will be no difficulties associated with our new capabilities—the defenders of freedom have long noted that free societies have problems peculiar to them. Instead, it assumes that the value of freedom outweighs the

---

[100] Jack Shafer, *Digital Native Calms the Anxious Masses*, SLATE, Sept. 13, 2010, **http://www.slate.com/id/2267161**.

> problems, not based on calculation of net value but because freedom is the right thing to want for society.[101]

Finally, we cannot ignore the practical difficulties of halting or even slowing progress—assuming we somehow collectively decided we wanted to do so. Turning back the clock seems almost unfathomable at this point absent extreme measures that would sacrifice so many of the benefits the Information Age has brought us—not to mention the curtailment of freedom that it would demand.

Regardless, the old Theuth-Thamus debate about the impact of technological change on culture and society will continue to rage. There is no chance this debate will die down anytime soon. (Just wait till new technologies like virtual reality go mainstream!) Despite real challenges in adapting to technological change, I remain generally optimistic about the prospects for technology to improve the human condition.

---

101 Shirky, *supra* note 59, at 298.

# CHAPTER 2

## IS THE GENERATIVE INTERNET AT RISK?

# Protecting the Internet Without Wrecking It: How to Meet the Security Threat

By Jonathan Zittrain*

On November 2, 1988, 5-10% of the 60,000 computers hooked up to the Internet started acting strangely. Inventories of affected computers revealed that rogue programs were demanding processor time. When concerned administrators terminated these programs, they reappeared and multiplied. They then discovered that renegade code was spreading through the Internet from one machine to another. The software—now commonly thought of as the first Internet worm—was traced to a twenty-three-year-old Cornell University graduate student, Robert Tappan Morris, Jr., who had launched it by infecting a machine at MIT from his terminal in Ithaca, New York.

Morris said he unleashed the worm to count how many machines were connected to the Internet, and analysis of his program confirmed his benign intentions. But his code turned out to be buggy. If Morris had done it right, his program would not have drawn attention to itself. It could have remained installed for days or months, and quietly performed a wide array of activities other than Morris's digital headcount.

The mainstream media had an intense but brief fascination with the incident. A government inquiry led to the creation of the Defense Department-funded Computer Emergency Response Team Coordination Center at Carnegie Mellon University, which serves as a clearinghouse for information about viruses and other network threats. A Cornell report on what had gone wrong placed the blame solely on Morris, who had engaged in a "juvenile act" that was "selfish and inconsiderate." It rebuked elements of the media that had branded Morris a hero for dramatically exposing security flaws, noting that it was well known that the computers' Unix operating systems were imperfect. The report called for university-wide committees to provide advice on security and acceptable use. It described consensus among computer scientists that Morris's acts warranted some form of punishment, but not "so stern as to damage permanently the perpetrator's career."

---

* Professor of Law, Harvard Law School and Harvard Kennedy School; Professor of Computer Science, Harvard School of Engineering and Applied Sciences; Co-Founder, Berkman Center for Internet & Society. This chapter originally appeared in the March/April 2008 BOSTON REVIEW.

In the end, Morris apologized, earned three years of criminal probation, performed four hundred hours of community service, and was fined $10,050. He transferred from Cornell to Harvard, founded a dot-com startup with some friends in 1995, and sold it to Yahoo! in 1998 for $49 million. He is now a respected, tenured professor at MIT.

In retrospect, the commission's recommendations—urging users to patch their systems and hackers to grow up—might seem naïve. But there were few plausible alternatives. Computing architectures, both then and now, are designed for flexibility rather than security. The decentralized ownership and non-proprietary nature of the Internet and the computers connected to it made it difficult to implement structural improvements. More importantly, it was hard to imagine cures that would not entail drastic, wholesale, purpose-altering changes to the very fabric of the Internet. Such changes would have been wildly out of proportion to the perceived threat, and there is no record of their having even been considered.

> Generative systems are powerful—they enable extraordinary numbers of people to devise new ways to express themselves in speech, art, or code, perhaps because they lack central coordination and control.

By design, the university workstations of 1988 were generative: Their users could write new code for them or install code written by others. This generative design lives on in today's personal computers. Networked PCs are able to retrieve and install code from each other. We need merely click on an icon or link to install new code from afar, whether to watch a video newscast embedded within a Web page, update our word processing or spreadsheet software, or browse satellite images.

Generative systems are powerful and valuable, not only because they foster the production of useful things like Web browsers, auction sites, and free encyclopedias, but also because they enable extraordinary numbers of people to devise new ways to express themselves in speech, art, or code and to work with other people. These characteristics can make generative systems very successful even though—perhaps especially because—they lack central coordination and control. That success attracts new participants to the generative system.

The flexibility and power that make generative systems so attractive are, however, not without risks. Such systems are built on the notion that they are never fully complete, that they have many uses yet to be conceived of, and that the public can be trusted to invent good uses and share them. But multiplying breaches of that trust threaten the very foundations of the system.

Whether through a sneaky vector like the one Morris used, or through the front door, when a trusting user elects to install something that looks interesting

without fully understanding it, opportunities for accidents and mischief abound. A hobbyist computer that crashes might be a curiosity, but when a home or office PC with years' worth of vital correspondence and papers is compromised, it can be a crisis. And when thousands or millions of individual, business, research, and government computers are subject to attack, we may find ourselves faced with a fundamentally new and harrowing scenario. As the unsustainable nature of the current state of affairs becomes more apparent, we are left with a dilemma that cannot be ignored: How do we preserve the extraordinary benefits of generativity, while addressing the growing vulnerabilities that are innate to it?

* * *

How profound is today's security threat? Since 1988, the Internet has suffered few truly disruptive security incidents. A network designed for communication among academic and government researchers appeared to scale beautifully as hundreds of millions of new users signed on during the 1990s, and three types of controls seemed adequate to address emerging dangers.

First, the hacker ethos frowns upon destructive hacking. Most viruses that followed Morris's worm had completely innocuous payloads: In 2004, Mydoom spread like wildfire and reputedly cost billions in lost productivity, but the worm did not tamper with data, and it was programmed to stop spreading at a set time. With rare exceptions like the infamous Lovebug worm, which overwrote files with copies of itself, the few highly malicious viruses that run contrary to the hacker ethos were so poorly coded that they failed to spread very far.

Second, network operations centers at universities and other institutions became more professionalized between 1988 and the advent of the mainstream Internet. For a while, most Internet-connected computers were staffed by professionals, administrators who generally heeded admonitions to patch regularly and scout for security breaches. Less adept mainstream consumers began connecting unsecured PCs to the Internet in earnest only in the mid-1990s. Then, transient dial-up connections greatly limited both the amount of time during which they were exposed to security threats, and the amount of time that, if compromised and hijacked, they would contribute to the problem.

Finally, bad code lacked a business model. Programs to trick users into installing them, or to sneak onto the machines, were written for amusement. Bad code was more like graffiti than illegal drugs: There were no economic incentives for its creation.

Today each of these controls has weakened. With the expansion of the community of users, the idea of a set of ethics governing activity on the Internet has evaporated. Anyone is allowed online if he or she can find a way to a

computer and a connection, and mainstream users are transitioning rapidly to always-on broadband connections.

Moreover, PC user awareness of security issues has not kept pace with broadband growth. A December 2005 online safety study found 81% of home computers to be lacking first-order protection measures such as current antivirus software, spyware protection, and effective firewalls.[1]

Perhaps most significantly, bad code is now a business. What seemed genuinely remarkable when first discovered is now commonplace: Viruses that compromise PCs to create large zombie "botnets" open to later instructions. Such instructions have included directing PCs to become remotely-controlled e-mail servers, sending spam by the thousands or millions to e-mail addresses harvested from the hard disk of the machines themselves or gleaned from Internet searches, with the entire process typically proceeding behind the back of the PCs' owners. At one point, a single botnet occupied fifteen percent of Yahoo!'s search capacity, running random searches on Yahoo! to find text that could be inserted into spam e-mails to throw off spam filters.[2] Dave Dagon, who recently left Georgia Tech University to start a bot-fighting company named Damballa, pegs the number of botnet-infected computers at close to 30 million.[3] Dagon said, "Had you told me five years ago that organized crime would control one out of every ten home machines on the Internet, I would not have believed that."[4] So long as spam remains profitable, that crime will persist.

Botnets can also be used to launch coordinated attacks on a particular Internet endpoint. For example, a criminal can attack an Internet gambling Web site and then extort payment to make the attacks stop. The going rate for a botnet to launch such an attack is reputed to be about $5,000 per day.[5]

Viruses are thus valuable properties. Well-crafted worms and viruses routinely infect vast swaths of Internet-connected personal computers. Antivirus vendor Eugene Kaspersky of Kaspersky Labs told an industry conference that they "may not be able to withstand the onslaught."[6] IBM's Internet Security Systems

---

1 AOL/NCSA ONLINE SAFETY STUDY 2 (Dec. 2005), **http://www.bc.edu/content/dam/files/offices/help/pdf/safety_study_2005.pdf**

2 Tim Weber, *Criminals 'May Overwhelm the Web,'* BBC NEWS, Jan. 25, 2007, **http://news.bbc.co.uk/2/hi/business/6298641.stm**.

3 Bob Sullivan, *Is Your Computer a Criminal?*, RED TAPE CHRONICLES, Mar. 27, 2007, **http://redtape.msnbc.com/2007/03/bots_story.html**.

4 *Id.*

5 *Id.*

6 *Id.*

reported a 40% increase in software vulnerabilities reported by manufacturers and "white hat" hackers between 2005 and 2006.[7] Nearly all of those vulnerabilities could be exploited remotely, and over half allowed attackers to gain full access to the machine and its contents.

As the supply of troubles has increased, the capacity to address them has steadily diminished. Patch development time increased throughout 2006 for all of the top operating system providers.[8] Times shortened modestly across the board in the first half of 2007, but, on average, enterprise vendors were still exposed to vulnerabilities for 55 days—plenty of time for hazardous code to make itself felt.[9] (The patch intervals for browsers tend to be shorter than those for operating systems.) What is more, antivirus researchers and firms require extensive coordination efforts simply to agree on a naming scheme for viruses as they emerge.[10] This is a far cry from a common strategy for battling them.

In addition, the idea of casually cleaning a virus off a PC is gone. When computers are compromised, users are now typically advised to reinstall everything on them. For example, in 2007, some PCs at the U.S. National Defense University fell victim to a virus. The institution shut down its network servers for two weeks and distributed new laptops to instructors.[11] In the absence of such drastic measures, a truly "mal" piece of malware could be programmed to, say, erase hard drives, transpose numbers inside spreadsheets randomly, or intersperse nonsense text at arbitrary intervals in Word documents found on infected computers—and nothing would stand in the way.

Recognition of these basic security problems has been slowly growing in Internet research communities. Nearly two-thirds of academics, social analysts, and industry leaders surveyed by the Pew Internet & American Life Project in 2004 predicted serious attacks on network infrastructure or the power grid in

---

7 IBM INTERNET SECURITY SYSTEMS, X-FORCE 2006 TREND STATISTICS (Jan. 2007), **http://www.iss.net/documents/whitepapers/X_Force_Exec_Brief.pdf**.

8 SYMANTEC, GLOBAL INTERNET SECURITY THREAT REPORT, TRENDS FOR JULY-DECEMBER 2007 at 24-28 (April 2008), **http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf**.

9 *Id.* at 6.

10 *See, e.g.*, Common Malware Enumeration: Reducing Public Confusion During Malware Outbreaks, **http://cme.mitre.org/** (last visited June 1, 2007).

11 Bill Gertz & Rowan Scarborough, *Inside the Ring—Notes from the Pentagon*, WASH. TIMES, Jan. 5, 2007, at A5, available at **http://www.gertzfile.com/gertzfile/ring011207.html**.

the coming decade.[12] Security concerns will lead to a fundamental shift in our tolerance of the status quo, either by a catastrophic episode, or, more likely, a glacial death of a thousand cuts.

Consider, in the latter scenario, the burgeoning realm of "badware" (or "malware") beyond viruses and worms: Software that is often installed at the user's invitation. The popular file-sharing program KaZaA, though advertised as "spyware-free," contains code that users likely do not want. It adds icons to the desktop, modifies Microsoft Internet Explorer, and installs a program that cannot be closed by clicking "Quit." Uninstalling the program does not uninstall all these extras, and the average user does not know how to get rid of the code itself. What makes such badware "bad" has to do with the level of disclosure made to a consumer before he or she installs it. The most common responses to the security problem cannot easily address this gray zone of software.

Many technologically savvy people think that bad code is simply a Microsoft Windows issue. They believe that the Windows OS and the Internet Explorer browser are particularly poorly designed, and that "better" counterparts (GNU/Linux and Mac OS, or the Firefox and Opera browsers) can help shield a user. But the added protection does not get to the fundamental problem, which is that the point of a PC—regardless of its OS—is to enable its users to easily reconfigure it to run new software from anywhere. When users make poor decisions about what software to run, the results can be devastating to their machines and, if they are connected to the Internet, to countless others' machines as well.

The cybersecurity problem defies easy solution because any of its most obvious fixes will undermine the generative essence of the Internet and PC. Bad code is an inevitable side effect of generativity, and as PC users are increasingly victimized by bad code, consumers are likely to reject generative PCs in favor of safe information appliances—digital video recorders, mobile phones, iPods, BlackBerrys, and video game consoles—that optimize a particular application and cannot be modified by users or third-parties. It is entirely reasonable for consumers to factor security and stability into their choice. But it is an undesirable choice to have to make.

* * *

On January 9, 2007, Steve Jobs introduced the iPhone to an eager audience crammed into San Francisco's Moscone Center. A beautiful and brilliantly

---

12 Susannah Fox et al., *The Future of the Internet: In a Survey, Technology Experts and Scholars Evaluate Where the Network Is Headed in the Next Few Years*, Jan. 9, 2005, at i, **http://www.pewinternet.org/PPF/r/145/report_display.asp**.

engineered device, the iPhone blended three products into one: an iPod, with the highest-quality screen Apple had ever produced; a phone, with cleverly integrated functionality, such as voicemail that came wrapped as separately accessible messages; and a device to access the Internet, with a smart and elegant browser, and built-in map, weather, stock, and e-mail capabilities.

Steve Jobs had no clue how the Apple II would be used. The iPhone—for all its startling inventiveness—is precisely the opposite.

This was Steve Jobs's second revolution. Thirty years earlier, at the First West Coast Computer Faire in nearly the same spot, the twenty-one-year-old Jobs, wearing his first suit, exhibited the Apple II personal computer to great buzz amidst "ten thousand walking, talking computer freaks."[13] The Apple II was a machine for hobbyists who did not want to fuss with soldering irons: all the ingredients for a functioning PC were provided in a convenient molded plastic case. Instead of puzzling over bits of hardware or typing up punch cards to feed into someone else's mainframe, Apple owners faced only the hurdle of a cryptic blinking cursor in the upper left corner of the screen: the PC awaited instructions. But the hurdle was not high. Some owners were inspired to program the machines themselves, but beginners, too, could load software written and then shared or sold by their more skilled counterparts. The Apple II was a blank slate, a bold departure from previous technology that had been developed and marketed to perform specific tasks.

The Apple II quickly became popular. And when programmer and entrepreneur Dan Bricklin introduced the first killer application for the Apple II in 1979—VisiCalc, the world's first spreadsheet program—sales of the ungainly but very cool machine took off. An Apple running VisiCalc helped to convince a skeptical world that there was a place for the PC on everyone's desk.

The Apple II was quintessentially generative technology. It was a platform. It invited people to tinker with it. Hobbyists wrote programs. Businesses began to plan on selling software. Jobs (and Apple) had no clue how the machine would be used. They had their hunches, but, fortunately for them (and the rest of us), nothing constrained the PC to the hunches of the founders.

The iPhone—for all its startling inventiveness—is precisely the opposite. Rather than a platform that invites innovation, the iPhone comes preprogrammed. In its first version, you were not allowed to add programs to the all-in-one device that Steve Jobs sells you except via the Siberia of its Web

---

13 David H. Ahl, *The First West Coast Computer Faire*, in 3 THE BEST OF CREATIVE COMPUTING 98 (David Ahl & Burchenal Green eds., 1980), available at **http://www.atariarchives.org/bcc3/showpage.php?page_98**.

browser. Its functionality was locked in, though Apple could change it through remote updates. Indeed, those who managed to tinker with the code and enable iPhone-support of more or different applications, were on the receiving end of Apple's threat to transform the iPhone into an iBrick.[14] A threat, to be sure, that Apple later at least partially disavowed. The machine was not to be generative beyond the innovations that Apple (and its exclusive carrier, AT&T) wanted. In its second version a year later, the iPhone boasted the App Store. Software developers could code for the phone – but the developers, and then each piece of software, would require approval from Apple before it could be made available to iPhone users. Apple would receive a 30% cut of sales, including "in-app" sales of upgrades, and an app could be banned retroactively after initial approval. This made the iPhone "contingently generative," a hybrid status that, depending on how you look at it, is either the best or the worst of both worlds: a melding of the sterile and the generative.

Jobs was not shy about these restrictions. As he said at the iPhone launch: "We define everything that is on the phone …. You don't want your phone to be like a PC. The last thing you want is to have loaded three apps on your phone and then you go to make a call and it doesn't work anymore."[15]

In the arc from the Apple II to the iPhone, we learn something important about where the Internet has been, and something even more important about where it is going. The PC revolution was launched with PCs that invited innovation by others. So, too, with the Internet. Both were designed to accept any contribution that followed a basic set of rules (either coded for a particular operating system, or respecting the protocols of the Internet). Both overwhelmed their respective proprietary, non-generative competitors: PCs crushed stand-alone word processors and the Internet displaced such proprietary online services as CompuServe and AOL.

But the future is looking very different because of the security situation—not generative PCs attached to a generative network, but appliances tethered to a network of control. These appliances take the innovations already created by Internet users and package them neatly and compellingly, which is good—but only if the Internet and PC can remain sufficiently central in the digital ecosystem to compete with locked-down appliances and facilitate the next round of innovations. The balance between the two spheres is precarious, and it is slipping toward the safer appliance. For example, Microsoft's Xbox 360

---

14 Michael, *Apple Says It May "Brick" Unlocked iPhones With Next Software Update*, Apple Gazette, Sep. 24, 2007, **http://www.applegazette.com/iphone/apple-says-it-may-brick-unlocked-iphones-with-next-software-update/**.

15 *See* John Markoff, *Steve Jobs Walks the Tightrope Again*, N.Y. TIMES, Jan. 12, 2007, available at **http://www.nytimes.com/2007/01/12/technology/12apple.html**.

video game console is a powerful computer, but, unlike Microsoft's Windows operating system for PCs, it does not allow just anyone to write software that can run on it – games must be licensed by Microsoft. Bill Gates sees the Xbox at the center of the future digital ecosystem, rather than its periphery: "It is a general purpose computer . . . [W]e wouldn't have done it if it was just a gaming device. We wouldn't have gotten into the category at all. It was about strategically being in the living room."[16]

Devices like iPhones and Xbox 360s may be safer to use, and they may seem capacious in features so long as they offer a simple Web browser. But by focusing on security and limiting the damage that users can do through their own ignorance or carelessness, these appliances also limit the beneficial tools that users can create or receive from others—enhancements they may be clueless about when they are purchasing the device.

> If the PC ceases to be at the center of the information technology ecosystem, the most restrictive aspects of information appliances will come to the fore.

Security problems related to generative PC platforms may propel people away from PCs and toward information appliances controlled by their makers. If we eliminate the PC from many dens or living rooms, we eliminate the test bed and distribution point of new, useful software from any corner of the globe. We also eliminate the safety valve that keeps those information appliances honest. If TiVo makes a digital video recorder that has too many limits on what people can do with the video they record, people will discover DVR software like MythTV that records and plays TV shows on their PCs. If mobile phones are too expensive, people will use Skype. But people do not buy PCs as insurance policies against appliances that limit their freedoms, even though PCs serve exactly this vital function. People buy them to perform certain tasks at the moment of acquisition. If PCs cannot reliably perform these tasks, most consumers will not see their merit, and the safety valve will be lost. If the PC ceases to be at the center of the information technology ecosystem, the most restrictive aspects of information appliances will come to the fore.

In fact, the dangers may be more subtly packaged. PCs need not entirely disappear as people buy information appliances in their stead. PCs can themselves be made less generative. Users tired of making the wrong choices about installing code on their PCs might choose to let someone else decide what code should be run. Firewalls can protect against some bad code, but they also complicate the installation of new good code. As antivirus, antispyware,

---

16 Ryan Block, *A Lunchtime Chat with Bill Gates*, ENGADGET, Jan. 8, 2007, **http://www.engadget.com/2007/01/08/a-lunchtime-chat-with-bill-gates-at-ces/**.

and anti-badware barriers proliferate, there are new barriers to the deployment of new good code from unprivileged sources. And in order to guarantee effectiveness, these barriers are becoming increasingly paternalistic, refusing to allow users easily to overrule them. Especially in environments where the user of the PC does not own it—offices, schools, libraries, and cyber-cafés—barriers are being put in place to prevent the running of any code not specifically approved by the relevant gatekeeper. Users may find themselves limited to using a Web browser. And while "Web 2.0" promises many more uses for a browser—consumers can now write papers and use spreadsheets through a browser, and software developers now write for Web platforms like Facebook instead of PC operating systems —these Web platforms are themselves tethered to their makers, their generativity contingent on the continued permission of the platform vendors.

Short of completely banning unfamiliar software, code might be divided into first- and second-class status, with second-class, unapproved software allowed to perform only certain minimal tasks on the machine, operating within a digital sandbox. This technical solution is safer than the status quo but imposes serious limits. It places the operating system creator or installer in the position of deciding what software will and will not run. The PC will itself have become an information appliance, not easily reconfigured or extended by its users.

The key to avoiding such a future is to give the market a reason not to abandon or lock down the PCs that have served it so well, also giving most governments reason to refrain from major intervention into Internet architecture in the name of public safety. The solutions to the generative dilemma will rest on social and legal as much as technical innovation, and the best guideposts can be found in other generative successes in those arenas. Mitigating abuses of openness without resorting to lockdown will depend on a community ethos embodied in responsible groups with shared norms and a sense of public purpose, rather than in the hands of a single gatekeeper, whether public or private.

In the medium term, the battle between generative and sterile will be played out between the iPhone and Android, which despite its own version of an App Store, also allows outside code to run that doesn't come from the store; and with projects like Boxee and Google TV, which are seeking to bridge the gap between the PC and the living room. Each device sets the dial set at a different point between complete "open" and completely "closed." And those dials can shift: after a security "spill," Android could be reprogrammed overnight to be more restrictive in the code it runs; and by the same token, Apple could decide to loosen its restrictions on iPhone code.

* * *

We need a strategy that addresses the emerging security troubles of today's Internet and PCs without killing their openness to innovation. This is easier

said than done, because our familiar legal tools are not particularly attuned to maintaining generativity. A simple regulatory intervention—say, banning the creation or distribution of deceptive or harmful code—will not work because it is hard to track the identities of sophisticated wrongdoers, and, even if found, many may not be in cooperative jurisdictions. Moreover, such intervention may have a badly chilling effect: Much of the good code we have seen has come from unaccredited people sharing what they have made for fun, collaborating in ways that would make business-like regulation of their activities burdensome for them. They might be dissuaded from sharing at all.

We can find a balance between needed change and undue restriction if we think about how to move generative approaches and solutions that work at one "layer" of the Internet—content, code, or technical—to another. Consider Wikipedia, the free encyclopedia whose content—the entries and their modifications—is fully generated by the Web community. The origins of Wikipedia lie in the open architecture of the Internet and Web. This allowed Ward Cunningham to invent the wiki, generic software that offers a way of editing or organizing information within an article, and spreading this information to other articles. Unrelated non-techies then used Wikis to form Web sites at the content layer, including Wikipedia. People are free not only to edit Wikipedia, but to take all of its contents and experiment with different ways of presenting or changing the material, perhaps by placing the information on otherwise unrelated Web sites in different formats. When abuses of this openness beset Wikipedia with vandalism, copyright infringement, and lies, it turned to its community—aided by some important technical tools—as the primary line of defense, rather than copyright or defamation law. Most recently, this effort has been aided by the introduction of Virgil Griffith's Wikiscanner, a simple tool that uses Wikipedia's page histories to expose past instances of article whitewashing by interested parties.

Unlike a form of direct regulation that would have locked down the site, the Wikipedian response so far appears to have held many of Wikipedia's problems at bay. Why does it work so well? Generative solutions at the content layer seem to have two characteristics that suggest broad approaches to lowering the risks of the generative Internet while preserving its openness. First, much participation in generating Web content—editing Wikipedia entries, blogging, or even engaging in transactions on eBay and Amazon that ask for reviews and ratings to establish reputations—is understood to be an innately social activity. These services solicit and depend upon participation from the public, and their participation mechanisms are easily mastered. The same possibility for broad participation exists one level down at the technical layer, but it has not yet been as fully exploited: Mainstream users have thus far been eager to have someone else solve underlying problems, which they perceive as technical rather than social. Second, many content-layer enterprises have developed technical tools to support collective participation, augmenting an individualistic ethos with

community-facilitating structures. In the Internet and PC security space, on the other hand, there have been few tools available to tap the power of groups of users to, say, distinguish good code from bad.

The effectiveness of the social layer in Web successes points to two approaches that might save the generative spirit of the Net, or at least keep it alive for another interval. The first is to reconfigure and strengthen the Net's experimentalist architecture to make it fit better with the vast expansion in the number and types of users. The second is to develop new tools and practices that will enable relevant people and institutions to help secure the Net themselves instead of waiting for someone else to do it.

## Generative PCs with Easy Reversion

Wikis are designed so that anyone can edit them. This creates a genuine and ongoing risk of bad edits, through either incompetence or malice. The damage that can be done, however, is minimized by the wiki technology, because it allows bad changes to be quickly reverted. All previous versions of a page are kept, and a few clicks by another user can restore a page to the way it was before later changes were made. So long as there are more users (and automated tools they create) detecting and reverting vandalism than there are users vandalizing, the community wins. (Truly, the price of freedom is eternal vigilance.)

Our PCs can be similarly equipped. For years Windows XP (and now Vista) has had a system restore feature, where snapshots are taken of the machine at a moment in time, allowing later bad changes to be rolled back. The process of restoring is tedious, restoration choices can be frustratingly all-or-nothing, and the system restoration files themselves can become corrupted, but it represents progress. Even better would be the introduction of features that are commonplace on wikis: A quick chart of the history of each document, with an ability to see date-stamped sets of changes going back to its creation. Because our standard PC applications assume a safer environment than really exists, these features have never been demanded or implemented. Because wikis are deployed in environments prone to vandalism, their contents are designed to be easily recovered after a problem.

The next stage of this technology lies in new virtual machines, which would obviate the need for cyber cafés and corporate IT departments to lock down their PCs.

In an effort to satisfy the desire for safety without full lockdown, PCs can be designed to pretend to be more than one machine, capable of cycling from one personality to the next. In its simplest implementation, we could divide a PC into two virtual machines: "Red" and "Green." The Green PC would house reliable software and important data—a stable, mature OS platform and tax

returns, term papers, and business documents. The Red PC would have everything else. In this setup, nothing that happens on one PC can easily affect the other, and the Red PC could have a simple reset button that restores a predetermined safe state. Someone could confidently store important data on the Green PC and still use the Red PC for experimentation. This isn't rocket science – there's already software out there to amount to a Green/Red divide on a Windows machine – but it's not so easy for the average user to deploy and use.

Easy, wiki-style reversion, coupled with virtual PCs, would accommodate the experimentalist spirit of the early Internet while acknowledging the important uses for those PCs that we do not want to disrupt. Still, this is not a complete solution. The Red PC, despite its experimental purpose, might end up accumulating data that the user wants to keep, occasioning the need for what Internet architect David D. Clark calls a "checkpoint Charlie" to move sensitive data from Red to Green without also carrying a virus or anything else undesirable. There is also the question of what software can be deemed safe for Green—which is just another version of the question of what software to run on today's single-identity PCs.

For these and related reasons, virtual machines will not be panaceas, but they might buy us some more time. And they implement a guiding principle from the Net's history: an experimentalist spirit is best maintained when failures can be contained as learning experiences rather than expanding to catastrophes.

## A Generative Solution to Bad Code

The Internet's original design relied on few mechanisms of central control. This lack of control has the generative benefit of allowing new services to be introduced, and new destinations to come online, without any up-front vetting or blocking by either private incumbents or public authorities. With this absence of central control comes an absence of measurement. The Internet itself cannot say how many users it has, because it does not maintain user information. There is no awareness at the network level of how much bandwidth is being used by whom. From a generative point of view this is good because it allows initially whimsical but data-intensive uses of the network to thrive (remember goldfish cams?)—and perhaps to become vital (now-routine videoconferencing through Skype, from, unsettlingly, the makers of KaZaA).

> Because we cannot easily measure the network and the character of the activity on it, we cannot easily assess and deal with threats from bad code without laborious and imperfect cooperation among a limited group of security software vendors.

But limited measurement is starting to have generative drawbacks. Because we cannot easily measure the network and the character of the activity on it, we cannot easily assess and deal with threats from bad code without laborious and imperfect cooperation among a limited group of security software vendors. The future of the generative Net depends on a wider circle of users able to grasp the basics of what is going on within their machines and between their machines and the network.

What might this system look like? Roughly, it would take the form of toolkits to overcome the digital solipsism that each of our PCs experiences when it attaches to the Internet at large, unaware of the size and dimension of the network to which it connects. These toolkits would run unobtrusively on the PCs of participating users, reporting back—to a central source, or perhaps only to each other—information about the vital signs and running code of that PC, which could help other PCs determine the level of risk posed by new code. When someone is deciding whether to run new software, the toolkit's connections to other machines could tell the person how many other machines on the Internet are running the code, what proportion of machines belonging to self-described experts are running it, whether those experts have vouched for it, and how long the code has been in the wild.

Building on these ideas about measurement and code assessment, Harvard University's Berkman Center and the Oxford Internet Institute—multidisciplinary academic enterprises dedicated to charting the future of the Net and improving it—have begun a project called StopBadware (www.stopbadware.org), designed to assist rank-and-file Internet users in identifying and avoiding bad code. The idea is not to replicate the work of security vendors like Symantec and McAfee, which, for a fee, seek to bail new viruses out of our PCs faster than they pour in. Rather, these academic groups are developing a common technical and institutional framework that enables users to devote some bandwidth and processing power for better measurement of the effect of new code. A first step in the toolkit was developed as "Herdict PC." Herdict PC was a small piece of software that assembles vital signs like number of pop-up windows or crashes per hour. [It incorporates that data into a dashboard usable by mainstream PC owners. Efforts like Herdict – including such ventures as Soluto (**www.soluto.com**) – will test the idea that solutions that have worked for generating content might also be applicable to the technical layer. Such a system might also illuminate Internet filtering by governments around the world, as people participate in a system where they can report when they cannot access a Web site, and such reports can be collated by geography.

A full adoption of the lessons of Wikipedia would give PC users the opportunity to have some ownership, some shared stake, in the process of evaluating code, especially because they have a stake in getting it right for their

own machines. Sharing useful data from their PCs is one step, but this may work best when the data goes to an entity committed to the public interest of solving PC security problems and willing to share that data with others. The notion of a civic institution here does not necessarily mean cumbersome governance structures and formal lines of authority so much as it means a sense of shared responsibility and participation. Think of the volunteer fire department or neighborhood watch: While not everyone is able to fight fires or is interested in watching, a critical mass of people are prepared to contribute, and such contributions are known to the community more broadly.

The success of tools drawing on group generativity depends on participation, which helps establish the legitimacy of the project both to those participating and those not. Internet users might see themselves only as consumers whose purchasing decisions add up to a market force, but, with the right tools, users can also see themselves as participants in the shaping of generative space—as netizens.

Along with netizens, hardware and software makers could also get involved. OS makers could be asked or required to provide basic tools of transparency that empower users to understand exactly what their machines are doing. These need not be as sophisticated as Herdict. They could provide basic information on what data is going in and out of the box and to whom. Insisting on getting better information to users could be as important as providing a speedometer or fuel gauge on an automobile—even if users do not think they need one.

Internet Service Providers (ISPs) can also reasonably be asked or required to help. Thus far, ISPs have been on the sidelines regarding network security. The justification is that the Internet was rightly designed to be a dumb network, with most of its features and complications pushed to the endpoints. The Internet's engineers embraced the simplicity of the end-to-end principle for good reasons. It makes the network more flexible, and it puts designers in a mindset of making the system work rather than designing against every possible thing that could go wrong. Since this early architectural decision, "keep the Internet free" advocates have advanced the notion of end-to-end neutrality as an ethical ideal, one that leaves the Internet without filtering by any of its intermediaries, routing packets of information between sender and recipient without anyone looking along the way to see what they contain. Cyberlaw scholars have taken up end-to-end as a battle cry for Internet freedom, invoking it to buttress arguments about the ideological impropriety of filtering Internet traffic or favoring some types or sources of traffic over others.

End-to-end neutrality has indeed been a crucial touchstone for Internet development. But it has limits. End-to-end design preserves users' freedom only because the users can configure their own machines however they like. But this depends on the increasingly unreliable presumption that whoever runs

a machine at a given network endpoint can readily choose how the machine should work. Consider that in response to a network teeming with viruses and spam, network engineers recommend more bandwidth (so the transmission of "deadweights" like viruses and spam does not slow down the much smaller proportion of legitimate mail being carried by the network) and better protection at user endpoints. But users are not well positioned to painstakingly maintain their machines against attack, and intentional inaction at the network level may be self-defeating, because consumers may demand locked-down endpoint environments that promise security and stability with minimum user upkeep.

Strict loyalty to end-to-end neutrality should give way to a new principle asking that any modifications to the Internet's design or the behavior of ISPs be made in such a way that they will do the least harm to generative possibilities. Thus, it may be preferable in the medium-term to screen-out viruses through ISP-operated network gateways rather than through constantly updated PCs. To be sure, such network screening theoretically opens the door to undesirable filtering. But we need to balance this speculative risk against the growing threat to generativity. ISPs are in a good position to help in a way that falls short of undesirable perfect enforcement facilitated through endpoint lockdown, by providing a stopgap while we develop the kinds of community-based tools that can promote salutary endpoint screening.

Even search engines can help create a community process that has impact. In 2006, in cooperation with the Harvard and Oxford StopBadware initiative, Google began automatically identifying Web sites that had malicious code hidden in them, ready to infect browsers. Some of these sites were set up for the purpose of spreading viruses, but many more were otherwise-legitimate Web sites that had been hacked. For example, visitors to chuckroast.com can browse fleece jackets and other offerings and place and pay for orders. However, Google found that hackers had subtly changed the chuckroast.com code: The basic functionalities were untouched, but code injected on the home page would infect many visitors' browsers. Google tagged the problem, and appended to the Google search result: "Warning: This site may harm your computer." Those who clicked on the results link anyway would get an additional warning from Google and the suggestion to visit StopBadware or pick another page.

The site's traffic plummeted, and the owner (along with the thousands of others whose sites were listed) was understandably anxious to fix it. But cleaning a hacked site takes more than an amateur Web designer. Requests for specialist review inundated StopBadware researchers. Until StopBadware could check each site and verify it had been cleaned of bad code, the warning pages stayed up. Prior to the Google/StopBadware project, no one took responsibility for this kind of security. Ad hoc alerts to the hacked sites' webmasters—and their

ISPs—garnered little reaction. The sites were fulfilling their intended purposes even as they were spreading viruses to visitors. With Google/StopBadware, Web site owners have experienced a major shift in incentives for keeping their sites clean.

The result is perhaps more powerful than a law that would have directly regulated them, and it could in turn generate a market for firms that help validate, clean, and secure Web sites. Still, the justice of Google/StopBadware and similar efforts remains rough, and market forces alone might not direct the desirable level of attention to those wrongly labeled as people or Web sites to be avoided, or properly labeled but with no place to seek help.

The touchstone for judging such efforts is whether they reflect the generative principle: Do the solutions arise from and reinforce a system of experimentation? Are the users of the system able, so far as they are interested, to find out how the resources they control—such as a PC—are participating in the environment? Done well, these interventions can encourage even casual users to have some part in directing what their machines will do, while securing those users' machines against outsiders who have not been given permission by the users to make use of them. Automatic accessibility by outsiders—whether by vendors, malware authors, or governments—can deprive a system of its generative character as its users are limited in their own control.

## Data Portability

The generative Internet was founded and cultivated by people and institutions acting outside traditional markets, and later carried forward by commercial forces. Its success requires an ongoing blend of expertise and contribution from multiple models and motivations. Ultimately, a move by the law to allocate responsibility to commercial technology players in a position to help but without economic incentive to do so, and to those among us, commercially inclined or not, who step forward to solve the pressing problems that elude simpler solutions may also be in order. How can the law be shaped if one wants to reconcile generative experimentation with other policy goals beyond continued technical stability? The next few proposals are focused on this question about the constructive role of law.

One important step is making locked-down appliances and Web 2.0 software-as-a-service more palatable. After all, they are here to stay, even if the PC and Internet are saved. The crucial issue here is that a move to tethered appliances and Web services means that more and more of our experiences in the information space will be contingent: A service or product we use at one moment could act completely differently the next, since it can be so quickly reprogrammed by the provider without our assent. Each time we power up a mobile phone, video game console, or BlackBerry, it might have gained some

features and lost others. Each time we visit a Web site offering an ongoing service like e-mail access or photo storage, the same is true.

As various services and applications become more self-contained within particular devices, there is a minor intervention the law could make to avoid undue lock-in. Online consumer protection law has included attention to privacy policies. A Web site without a privacy policy, or one that does not live up to whatever policy it posts, is open to charges of unfair or deceptive trade practices. Similarly, makers of tethered appliances and Web sites keeping customer data ought to be asked to offer portability policies. These policies would declare whether users will be allowed to extract their data should they wish to move their activities from one appliance or Web site to another. In some cases, the law could create a right of data portability, in addition to merely insisting on a clear statement of a site's policies.

A requirement of data portability is a generative insurance policy applying to individual data wherever it might be stored. And the requirement need not be onerous. It could apply only to uniquely provided personal data such as photos and documents, and mandate only that such data ought to readily be extractable by the user in some standardized form. Maintaining data portability will help people pass back and forth between the generative and the non-generative, and, by permitting third-party backup, it will also help prevent a situation in which a non-generative service suddenly goes offline, with no recourse for those who have used the service to store their data.

## Appliance Neutrality

Reasonable people disagree on the value of defining and legally mandating network neutrality. But if there is a present worldwide threat to neutrality in the movement of bits, it comes from enhancements to traditional and emerging "appliancized" services like Google mash-ups and Facebook apps, in which the service provider can be pressured to modify or kill others' applications on the fly. Surprisingly, parties to the network neutrality debate—who have focused on ISPs—have yet to weigh in on this phenomenon.

In the late 1990's, Microsoft was found to possess a monopoly in the market for PC operating systems.[17] Indeed, it was found to be abusing that monopoly to favor its own applications—such as its Internet Explorer browser—over third-party software, against the wishes of PC makers who wanted to sell their hardware with Windows preinstalled but adjusted to suit the makers' tastes. Microsoft was forced by the law to meet ongoing requirements to maintain a

---

17 United States v. Microsoft Corp., 84 F. Supp. 2d 9, 19 (D.D.C. 1999).

level playing field between third-party software and its own by allowing third-party software to be pre-installed on new Windows computers.

We have not seen the same requirements arising for appliances that do not allow, or strictly control, the ability of third parties to contribute from the start. So long as the market's favorite video game console maker never opens the door to generative third-party code, it is hard to see how the firm could be found to be violating competition law. A manufacturer is entitled to make an appliance and to try to bolt down its inner workings so that they cannot be modified by others. So when should we consider network neutrality-style mandates for appliancized systems? The answer lies in that subset of appliancized systems that seeks to gain the generative benefits of third-party contribution at one point in time while reserving the right to exclude it later.

The common law recognizes vested expectations. For example, the law of adverse possession dictates that people who openly occupy another's private property without the owner's explicit objection (or, for that matter, permission) can, after a lengthy period of time, come to legitimately acquire it. More commonly, property law can find prescriptive easements—rights-of-way across territory that develop by force of habit—if the owner of the territory fails to object in a timely fashion as people go back and forth across it. These and related doctrines point to a deeply held norm: Certain consistent behaviors can give rise to obligations, sometimes despite fine print that tries to prevent those obligations from coming about.

Applied to the idea of application neutrality, this norm of protecting settled expectations might suggest the following: If Microsoft wants to make the Xbox a general purpose device but still not open to third-party improvement, no regulation should prevent it. But if Microsoft does welcome third-party contribution, it should not be able to subsequently impose barriers to outside software continuing to work. Such behavior is a bait-and-switch that is not easy for the market to anticipate and that stands to allow a platform maker to exploit habits of generativity to reach a certain plateau, dominate the market, and then make the result proprietary—exactly what the Microsoft Web browser case rightly was brought to prevent.

> The free software movement has produced some great works, but under prevailing copyright law even the slightest bit of "poison," in the form of code from a proprietary source, could amount to legal liability for anyone who copies or even uses the software.

## Generative Software

At the code layer, it is not easy for the law to maintain neutrality between the two models of software production that have emerged with the Net: Proprietary

software whose source code recipe is nearly always hidden, and free software—free not in terms of the price, but the openness of its code to public review and modification. The free software movement has produced some great works, but under prevailing copyright law even the slightest bit of "poison," in the form of code from a proprietary source, could amount to legal liability for anyone who copies or even uses the software. These standards threaten the long-term flourishing of the free software movement: The risks are more burdensome than need be.

But there are some changes to the law that would help. The kind of law that shields Wikipedia and Web site hosting companies from liability for unauthorized copyrighted material contributed by outsiders, at least so long as the organization acts expeditiously to remove infringing material once it is notified, ought to be extended to the production of code itself. Code that incorporates infringing material ought not be given a free pass, but those who have promulgated it without knowledge of the infringement would have a chance to repair the code or cease copying it before becoming liable.

Modest changes in patent law could help as well. If those who see value in software patents are correct, infringement is rampant. And to those who think patents chill innovation, the present regime needs reform. To be sure, amateurs who do not have houses to lose to litigation can still contribute to free software projects—they are judgment proof. Others can contribute anonymously, evading any claims of patent infringement since they simply cannot be found. But this turns coding into a gray market activity, eliminating what otherwise could be a thriving middle class of contributing firms should patent warfare ratchet into high gear.

The law can help level the playing field. For patent infringement in the United States, the statute of limitations is six years; for civil copyright infringement it is three. Unfortunately, this limit has little meaning for computer code because the statute of limitations starts from the time of the last infringement. Every time someone copies (or perhaps even runs) the code, the clock starts ticking again on a claim of infringement. This should be changed. The statute of limitations could be clarified for software, requiring that anyone who suspects or should suspect his or her work is being infringed sue within, for instance, one year of becoming aware of the suspect code. For example, the acts of those who contribute to free software projects—namely, releasing their code into a publicly accessible database like SourceForge—could be enough to start the clock ticking on that statute of limitations. In the absence of such a rule, lawyers who think their employers' proprietary interests have been compromised can wait to sue until a given piece of code has become wildly popular—essentially sandbagging the process in order to let damages rack up.

## Generative Licenses

There is a parallel to how we think about balancing generative and sterile code at the content layer: Legal scholars Lawrence Lessig and Yochai Benkler, as well as others, have stressed that even the most rudimentary mixing of cultural icons and elements, including snippets of songs and video, can accrue thousands of dollars in legal liability for copyright infringement without harming the market for the original proprietary goods.[18] Benkler believes that the explosion of amateur creativity online has occurred despite this system. The high costs of copyright enforcement and the widespread availability of tools to produce and disseminate what he calls "creative cultural bricolage" currently allow for a variety of voices to be heard even when what they are saying is theoretically sanctionable by fines up to $30,000 per copy made, $150,000 if the infringement is done "willfully."[19] As with code, the status quo shoehorns otherwise laudable activity into a sub-rosa gray zone.

As tethered appliances begin to take up more of the information space, making information that much more regulable, we have to guard against the possibility that content produced by citizens who cannot easily clear permissions for all its ingredients will be squeezed out. Even the gray zone will constrict.

* * *

Regimes of legal liability can be helpful when there is a problem and no one has taken ownership of it. No one fully owns today's problems of copyright infringement and defamation online, just as no one fully owns security problems on the Net. But the solution is not to conscript intermediaries to become the Net police.

Under prevailing law, Wikipedia could get away with much less stringent monitoring of its articles for plagiarized work, and it could leave plainly defamatory material in an article but be shielded in the United States by the Communications Decency Act provision exempting those hosting material from responsibility for what others have provided. Yet Wikipedia polices itself according to an ethical code that encourages contributors to do the right thing rather than the required thing or the profitable thing.

To harness Wikipedia's ethical instinct across the layers of the generative Internet, we must figure out how to inspire people to act humanely in digital environments. This can be accomplished with tools—some discussed above, others yet to be invented. For the generative Internet to come fully into its

---

18 LAWRENCE LESSIG, REMIX: MAKING ART AND COMMERCE THRIVE IN A HYBRID ECONOMY (2008); YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006).

19 YOCHAI BENKLER, THE WEALTH OF NETWORKS 275 (2006).

own, it must allow us to exploit the connections we have with each other. Such tools allow us to express and live our civic instincts online, trusting that the expression of our collective character will be one at least as good as that imposed by outside sovereigns—sovereigns who, after all, are only people themselves.

Our generative technologies need technically skilled people of good will to keep them going, and the fledgling generative activities—blogging, wikis, social networks—need artistically and intellectually skilled people of goodwill to serve as true alternatives to a centralized, industrialized information economy that asks us to identify only as consumers of meaning rather than as makers of it. The deciding factor in whether our current infrastructure can endure will be the sum of the perceptions and actions of its users. Traditional state sovereigns, pan-state organizations, and formal multi-stakeholder regimes have roles to play. They can reinforce conditions necessary for generative blossoming, and they can also step in when mere generosity of spirit cannot resolve conflict. But that generosity of spirit is a society's crucial first line of moderation.

Our fortuitous starting point is a generative device on a neutral Net in tens of millions of hands. Against the trend of sterile devices and services that will replace the PC and Net stand new architectures like those of Boxee and Android. To maintain that openness, the users of those devices must experience the Net as something with which they identify and belong. We must use the generativity of the Net to engage a constituency that will protect and nurture it.

# A Portrait of the Internet as a Young Man

By Ann Bartow*

## Introduction

The core theory of Jonathan Zittrain's 2008 book *The Future of the Internet—And How to Stop It* is this: Good laws, norms, and code are needed to regulate the Internet, to prevent bad laws, norms, and code from compromising its creative capabilities and fettering its fecund flexibility. A far snarkier, if less alliterative, summary would be "We have to regulate the Internet to preserve its open, unregulated nature."

Zittrain uses brief, informal accounts of past events to build two main theories that dominate the book. First, he claims that open access, which he calls generativity, is under threat by a trend toward closure, which he refers to as tetheredness, which is counterproductively favored by proprietary entities. Though consumers prefer openness and the autonomy it confers, few take advantage of the opportunities it provides, and therefore undervalue it and too readily cede it in favor of the promise of security that tetheredness brings. Second, he argues that if the Internet is to find salvation it will be by the grace of "true netizens," volunteers acting collectively in good faith to cultivate positive social norms online.

One of the themes of the James Joyce novel first published in 1916, *A Portrait of the Artist as a Young Man*[1] is the Irish quest for autonomous rule. Jonathan Zittrain's *The Future of the Internet—And How to Stop It* is similarly infused with the author's desire for principled, legitimate governance—only of the place called cyberspace, rather than the author's meatspace homeland.

*Portrait*'s protagonist, Stephen Dedalus, internally defines himself as an artist through a nonlinear process of experiences and epiphanies. He consciously decides that it should be his mission to provide a voice for his family, friends, and community through his writing. Though Dedalus opts out of the

---

* Professor of Law, University of South Carolina School of Law. This essay was adapted from *A Portrait of the Internet as a Young Man*, 108 MICH. L. REV. 1079 (2010), available at **http://www.michiganlawreview.org/articles/a-portrait-of-the-internet-as-a-young-man**. The author dedicates this essay to her son Casey, and to the memory of C. Edwin Baker.

1 JAMES JOYCE, A PORTRAIT OF THE ARTIST AS A YOUNG MAN (1916).

traditional forms of participation in society, he envisions his writing as a way to productively influence society. Jonathan Zittrain charts the development of the Internet as a nonlinear process wrought by both conscious hard work and sweeping serendipity. He also strives to provide a voice for technologically elite Internet users, and to influence the development of online culture. He paints a portrait of the future Internet as chock full of so many enigmas and puzzles that it will keep the cyberlaw professors busy for decades, even though according to Zittrain, law as traditionally conceptualized will not be important.

In addition to invoking Joyce, I chose the title of this essay for its decisive invocation of maleness. Embedded within Zittrain's theories of generativity, there is also a perplexing gender story, in which men are fertile, crediting themselves with helping to "birth" the field of cyberlaw,[2] and engaging in stereotypically domestic pursuits such as "baking" restrictions into gadgetry.[3] Non-generative appliances are deemed "sterile"[4] by Zittrain, sterility being the conceptual opposite of generativity. His deployment of reproductive imagery is odd. A metaphor equating an author's creative output to a child is often invoked in the context of copyright law by people arguing that authors should have extensive control over the works they create.[5] Zittrain's variation characterizes controlled technological innovations as unable to produce progeny at all. The metaphor works better if tetheredness is instead envisaged as a form of birth control, preventing unwanted offspring only. Certainly the producers of closed devices or locked software are able to provide, and generally enthusiastic about providing, new and improved versions of their goods and services to paying customers.

---

2 *See, e.g.*, Lawrence Lessig, Amazon.com Customer Review of THE FUTURE OF THE INTERNET—AND HOW TO STOP IT, *Cyberlaw 2.0*, **http://www.amazon.com/review/R131R71HS3YJVG/ref=cm_cr_rdp_perm** (Dec. 4, 2008) ("The field of cyberlaw, or the law of the Internet—*a field I helped birth* … has suffered because people like me have spent too much time cheerleading, and not enough time focusing the world on the real problems and threats that the Internet has produced.") (emphasis added); *see also* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1416–17 (2001) (noting that Roger Clarke is credited with coining the term "dataveillance"). Roger Clarke published suggestions for Internet regulations as early as 1988. *See* Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498, 508–11 (1988).

3 JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 2 (2008). ("Jobs was not shy about these restrictions baked into the iPhone."). [*hereinafter* ZITTRAIN, THE FUTURE OF THE INTERNET].

4 *See, e.g., id.* at 2 ("The iPhone is the opposite. It is sterile."), 73 ("Generative tools are not inherently better than their non-generative ('sterile') counterparts.").

5 See Malla Pollack, *Towards a Feminist Theory of the Public Domain, or Rejecting the Gendered Scope of the United States Copyrightable and Patentable Subject Matter*, 12 WM. & MARY J. WOMEN & L. 603, 606–07 (2006); see William Patry, *Gender and Copyright*, THE PATRY COPYRIGHT BLOG, Jun. 20, 2008, **http://williampatry.blogspot.com/2008/06/gender-and-copyright.html**.

Zittrain offers a well-executed collection of stories that are intended to anchor his global theories about how the Internet should optimally function, and how two classes of Internet users should behave: The technologies should be generative, but also monitored to ensure that generativity is not abused by either the government or by scoundrels; elite Internet users with, as one might say today, "mad programming skilz" should be the supervisors of the Internet, scrutinizing new technological developments and establishing and modeling productive social norms online; and average, non–technically proficient Internet users should follow these norms, and should not demand security measures that unduly burden generativity.

The anecdotes are entertaining and educational, but they do not constructively cohere into an instruction manual on how to avoid a bad future for people whose interests may not be recognized or addressed by what is likely to be a very homogeneous group of elites manning (and I do mean man-ning, given the masculine dominance of the field) the virtual battlements they voluntarily design to defend against online forces of evil. And some of the conclusions Zittrain draws from his stories are questionable. So, I question them below.

## Generativity Versus Tetheredness Is a False Binary

Pitting generativity against tetheredness creates a false binary that drives a lot of Zittrain's theorizing. The book was published in May of 2008, but its origins can be found in his earlier legal scholarship and mainstream media writings. In 2006, Jonathan Zittrain published an article entitled *The Generative Internet*.[6] In it, he asserted the following:

> Cyberlaw's challenge ought to be to find ways of regulating—though not necessarily through direct state action—which code can and cannot be readily disseminated and run upon the generative grid of Internet and PCs, lest consumer sentiment and preexisting regulatory pressures prematurely and tragically terminate the grand experiment that is the Internet today.[7]

Like the article, the book is useful for provoking thought and discussion, and it teaches the reader many disparate facts about the evolution of a number of different technologies. But it does not provide much direction for activists, especially not those who favor using laws to promote order. Zittrain has come

---

6 Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974 (2006) [hereinafter Zittrain, *The Generative Internet*].

7 *Id.* at 1979.

to bury cyberspace law as promulgated by governments, not to praise it. "Cyberlaw" as redefined by Zittrain is no longer the science of adapting existing real-space legal constructs to the online environment. Instead it is a collection of best practices chosen by people with the technological proficiency to impose them, top down, on the ignorant folks who are selfishly driven by their shallow consumer sentiments (*viz.*, a desire for simplicity and security over openness and generativity).

An abstract for the book, featured at its dedicated website, states:

> The Internet's current trajectory is one of lost opportunity. Its salvation, Zittrain argues, lies in the hands of its millions of users. Drawing on generative technologies like Wikipedia that have so far survived their own successes, this book shows how to develop new technologies and social structures that allow users to work creatively and collaboratively, participate in solutions, and become true "netizens."[8]

I will bluntly state (splitting an infinitive in the process) that I did not learn how to develop new technologies or new social structures from reading this book. It convinced me that new technologies and new social structures could contribute productively to the Internet if they develop appropriately, but Zittrain does not provide road maps or an instruction manual for developing them. He calls for "[c]ivic technologies [that] seek to integrate a respect for individual freedom and action with the power of cooperation," but doesn't paint a clear picture of which precise qualities these technologies or social structures would have, beyond cultivating generativity.[9]

Zittrain relentlessly informs the reader that generativity is a very good thing—except when it is abused by malefactors. But what, exactly, is generativity? Zittrain invokes the terms generative, non-generative, and generativity constantly throughout the book (over 500 times), but the definition of generative doesn't remain constant. Sometimes it means creative or innovative, while other times it connotes openness, accessibility, or freedom.[10]

---

8 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3.

9 Jonathan Zittrain, *How to Get What We All Want*, CATO UNBOUND, May 6, 2009, **http://www.cato-unbound.org/2009/05/06/jonathan-zittrain/how-to-get-what-we-all-want/**.

10 *Compare* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 84 ("Generative systems allow users at large to try their hands at implementing and distributing new uses, and to fill a crucial gap when innovation is undertaken only in a profit-making model …"), *with id.* at 113 ("[T]he PC telephone program Skype is not amenable to third-party changes and is tethered to Skype for its updates. Skype's distribution partner in China has agreed to censor words

Zittrain had written previously that "Generativity denotes a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences."[11] Similarly, in the book he says, "*Generativity is a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences.*"[12] He lists five elements of generativity:

> (1) how extensively a system or technology leverages a set of possible tasks; (2) how well it can be adapted to a range of tasks; (3) how easily new contributors can master it; (4) how accessible it is to those ready and able to build on it; and (5) how transferable any changes are to others— including (and perhaps especially) non-experts.[13]

Generative also seems to mean idiot-resistant. In his article *The Generative Internet* he explains that PCs are highly adaptable machines that are connected to a network with little centralized control, resulting in "a grid that is nearly completely open to the creation and rapid distribution of the innovations of technology-savvy users to a mass audience that can enjoy those innovations without having to know how they work."[14] In the book, he makes the same point repeatedly—that most "mainstream" or "rank-and-file" computer users are either passive beneficiaries or victims of generativity, rather than generative actors.[15] There is a highly influential generative class of individuals who use generativity in socially productive ways. There is a nefarious group of reprobates who abuse generativity to create online havoc. And then there are the rest of the people online, sending and receiving emails, reading and writing blogs, participating on social-networking sites, renewing antivirus subscriptions, banking, shopping, and reading newspapers online. These users are blithely unaware of the generativity that provided this vast electronic bounty and complacently believe that, as long as they continue to pay an Internet service provider ("ISP") for Internet access, its delivery will remain relatively smooth

---

like 'Falun Gong' and 'Dalai Lama' in its text messaging for the Chinese version of the program. Other services that are not generative at the technical layer have been similarly modified …").

11 Zittrain, *The Generative Internet*, *supra* note 6, at 1980.

12 JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT, *supra* note 3 at 70 (emphasis in original).

13 *Id.* p. 71.

14 Zittrain, *The Generative Internet*, *supra* note 6.

15 *See, e.g.*, *id.* at 3; *see also* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 4, 8, 43, 44–45, 51, 56, 59, 78, 100, 102, 130, 151–52, 155, 59–60, 198, 243, 245.

and uninterrupted. When they call for more security for electronic devices, they themselves are the "damage" that generativity has to "route around."[16]

The anti-generative concept of tetheredness also does some definitional shape-shifting throughout the tome. Sometimes it means unmodifiable, while other times it means controlled by proprietary entities, who may or may not facilitate, or even tolerate, alterations of their wares by end users. According to Zittrain, the dangers of tethers are twofold: Private companies can regulate how consumers use their products, and services and governments can use them to censor or spy on their citizens.[17]

Tethers can be good things if you are a mountain climber, or if you don't want your horse to run off without you. And far more pertinently, tethers facilitate software updating for flaw-fixing and hole-patching purposes. Untethered software would require manual updates, a labor-intensive prospect that would require a degree of technical proficiency that many Internet users may lack. How many people are prepared to give up the advantages of tetheredness in the interest of preserving generativity is unclear. Without tethered appliances, the functionality of the Internet will be compromised. Try using a program that is no longer updated or supported by its vendor. Its obsolescence may render it untethered, but unless you have some pretty good programming chops, its usefulness will decline rapidly. Zittrain fears people will exchange generativity for security in binary fashion, but the relationship between tetheredness and convenience needs to be taken into account, as these variables will also affect consumer preferences and behaviors.

The fundamental security most people seek is probably operability. Any threat to serviceability, whether from too much generativity or too many tethers, will provoke a call for action from users. I couldn't have accessed the downloadable version of Zittrain's book without a host of tethered utilities, including my computer's operating system, my Internet browser, and Adobe Acrobat, which all update automatically with great frequency, as I consented to allow them to do when I agreed to the terms of use laid out in the associative end user license agreements ("EULAs"). The same with my printer software, my antivirus program, my online media players, the online games I play, and every other Internet-related utility I use. In a sense, this proves Zittrain's assertion that we have ceded control over the mechanisms of online interface to electronic leash-

---

16 This is a sideways reference to the John Gilmore quote, "The Net interprets censorship as damage and routes around it." *See* Philip Elmer-DeWitt, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, at 62, 64, *available at* **http://www.time.com/time/magazine/article/0,9171,979768,00.html**.

17 *See, e.g.*, ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 56–57, 113 (discussing Skype), 109–10, 113 (discussing OnStar), 113 (discussing China's use of Google.cn), 210–14 (discussing mobile phones).

wielding tyrants. But, he may have the timing as well as motivation wrong. I suspect most of us deferred to tethering commercial enterprises very early in the evolution of the mainstream Internet, rather than recently. Zittrain references pioneering ISPs CompuServe and AOL as proprietary services that were overwhelmed by the generativity of PCs and the Internet.[18] My initial nonacademic experiences with the Internet comprised waiting anxiously for CompuServe and then AOL to finish installing updates when I needed to check my e-mail, and I had to pay for my Internet time by the minute. Things only went downhill when AOL went to an "all you can eat" payment structure, providing unlimited Internet for a fixed monthly fee. Users surged but AOL's capacity could not meet the demand.[19] Users didn't want security, they wanted performance. Tetheredness, or something similar, may have been linked in some way to AOL's difficulties meeting its customers' demand, but overselling and insufficient server capacity were the true culprits in terms of inhibiting operability. In addition, if Zittrain is correct that CompuServe and AOL exemplify the evils of tethering, it's pretty clear the market punished those entities pretty harshly without Internet governance-style interventions.

Software and electronic devices can be simultaneously generative and tethered. And it is unfair to criticize people who quite reasonably rely on tetheredness to keep their computers and electronic equipment updated and fully functional. Many average Internet users might like more transparency about the nature and extent of the tethers that connect their computers to large multinational corporations, but short of having actual laws that require relevant disclosures, this consumer desire is unlikely to be met. For them, generativity is unlikely to be helpful or enlightening, as Zittrain correctly notes, because they are not skilled enough to take advantage of it. In the absence of helpful laws, they are at the mercy of business models.

## Generativity: The Good, the Bad & the Ugly

Zittrain's stories are intended to show that generative technologies are better than tethered ones. But another strand of his narrative illustrates that generativity can be used destructively, to support the contention that it cannot

---

18 The PC revolution was launched with PCs that invited innovation by others. So too with the Internet. Both were generative; they were designed to accept any contribution that followed a basic set of rules (either coded for a particular operating system, or respecting the protocols of the Internet). Both overwhelmed their respective proprietary, non-generative competitors, such as the makers of stand-alone word processors and proprietary online services like CompuServe and AOL. ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 23–25.

19 *See, e.g.*, Timothy C. Barmann, *Judge to rule this week on AOL service*, CYBERTALK, Oct. 26, 1997, **http://www.cybertalk.com/102697b.htm**.

be unfettered. At its worst, he warns, generativity will enable bad actors to exploit tethers for nefarious purposes, while tethers will simultaneously restrain positive generative responses to these challenges. His accounts of degenerate generativity rest uneasily with his exhortation that facilitating generativity should be the guiding principle of Internet governance.

He also suggests deploying the "generative principle to determine whether and when it makes sense to violate the end-to-end principle" in the context of debates about network neutrality.[20] And the quantum of generativity that is promoted becomes the measure for assessing the legitimacy and effectiveness of what he characterizes as the intrusions of cyberlaw. He writes:

> The touchstone for judging such efforts should be according to the generative principle: do the solutions encourage a system of experimentation? Are the users of the system able, so far as they are interested, to find out how the resources they control—such as a PC—are participating in the environ–ment?[21]

Fostering generativity thus becomes the Prime Directive of Internet governance.[22] But there are problems he raises elsewhere in the book that generativity may not address, or may in fact exacerbate. For example, Zittrain references OnStar a number of times, warning that it can be used by law enforcement for surveillance purposes because it is tethered, and can be accessed remotely.[23] Putting aside questions about whether OnStar is accurately described as part of the Internet, one wonders of what practical use OnStar would be to its clients if it wasn't tethered. OnStar seems to be a service that caters to people who want higher levels of proactive information and security when they are driving than the combination of a GPS unit and mobile phone can provide. OnStar customers don't want generativity; they want someone to call the police and an ambulance or tow truck if they have an accident so they

---

20 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 185.

21 *Id.* at 173.

22 "The Prime Directive is a plot device cooked up by a patently optimistic TV writer (either *Trek* producer Gene L. Coon or writer Theodore Sturgeon, depending on who you ask) in the mid-1960s. It's a freshmen-year philosophy student's reaction to the Cold War, when America and the Soviets were playing out their hostilities by proxy third-world conflicts. Effectively, they were interfering in the 'development' of underprivileged countries to further their own ends with some awful immediate and long-term results. In Roddenberry's vision, humanity had evolved beyond such puppeteering and become an 'advanced' race." *See* Jay Garmon, *Why 'Star Trek's Prime Directive is stupid'*, TECHREPUBLIC.COM, Feb. 12, 2007, **http://blogs.techrepublic.com.com/geekend/?p=533**.

23 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 109–10, 113, 117–18, 187.

don't have to, or to track down the location of their vehicle if it is stolen. Security means more to them than privacy, and if they don't consciously realize they are exchanging one for the other when they sign up with OnStar, it seems to me the best solution is to require OnStar to inform them of this trade-off in simple and unambiguous terms. The law could also require OnStar to provide further information, perhaps including a primer on the search and seizure jurisprudence of Fourth Amendment law. Making OnStar generative, so that private citizens can readily discern incursions by government actors, would not give OnStar customers any more of what they appear to want—a high level of security overtly linked to constant, dedicated supervision. Enhanced generativity might also provide opportunities for private spying or intentional service disruptions by the very villains Zittrain spills so much ink warning against.

Many of his examples of useful online-governance initiatives rely on extensive amounts of volunteer labor. But the important technological innovations related to the Internet were motivated by some form of self-interest. The U.S. Defense Department developed the Internet as a decentralized communications system that would be difficult to disrupt during wartime.[24] Tim Berners-Lee invented the World Wide Web as a way to facilitate communications with other physicists.[25] Pornographers have long used spam, browser hijacking, and search-engine manipulation to reach the eyeballs of potential customers.[26] All may have relied on generativity (though one might question how open and accessible the Defense Department was) but not all are socially beneficial.[27]

Sometimes Internet users may donate their labor involuntarily. Their online activities are harvested and bundled into what Zittrain applauds as the mediated wisdom of the masses. For example, he notes as follows:

---

24 *See* Joseph D. Schleimer, *Protecting Copyrights at the "Backbone" Level of the Internet*, 15 UCLA ENT. L. REV. 139, 149 (2008); *see also* JANET ABBATE, INVENTING THE INTERNET 7–41 (1999).

25 ABBATE, *supra*; *see also* Dick Kaser, *The Guy Who Did the WWW Thing at the Place Where He Did It*, INFO. TODAY, Feb. 2004, at 30.

26 *See, e.g.*, *Pornographers Can Fool You With Hi-Tech*, FILTERGUIDE.COM, **http://www.filterguide.com/pornsfool.htm** (setting forth various ways in which pornographers use technology to fool children) (last visited Oct 21, 2009); PEW INTERNET & AMERICAN LIFE PROJECT, SPAM IS STARTING TO HURT EMAIL (2003), **http://www.pewinternet.org/Press-Releases/2003/Spam-is-starting-to-hurt-email.aspx** (accounting for pornography-related spams' impact on email).

27 *See generally* Ann Bartow, *Pornography, Coercion, and Copyright Law 2.0*, 10 VAND. J. ENT. & TECH. L. 799, 800 (2008) ("Pornography is a dominant industrial force that has driven the evolution of the Internet.").

> The value of aggregating data from individual sources is well known. Yochai Benkler approvingly cites Google Pagerank algorithms over search engines whose results are auctioned, because Google draws on the individual linking decisions of millions of Web sites to calculate how to rank its search results. If more people are inking to a Web site criticizing Barbie dolls than to one selling them, the critical site will, all else equal, appear higher in the rankings when a user searches for "Barbie."[28]

But all else is unlikely to be equal. Mattel can hire reputation-defense companies like ReputationDefender[29] to bury the critical sites about Barbie using search engine-optimization techniques and to surreptitiously edit Wikipedia entries.[30] For-profit entities don't just want to spy on and control their customers with tethers. They also want to manipulate as much of the Internet as possible to their benefit, and this logically includes taking steps to highlight positive information and minimize the visibility of disparagement by third parties.

Additionally, collective actions by the online masses can be oppressive. If more people link to websites glorifying sexual violence against women than to websites where women are treated as if they are fully human, those sites appear higher in the rankings when a user searches for a wide variety of things related to sex. The same is potentially true for racist and homophobic sites and other content that depict discrete groups in derogatory ways. In this way, negative stereotypes can be reinforced and spread virally.[31]

Finally, in the Google PageRank example, the power and input of the masses is being harnessed, for profit, by a large corporation. Google is doubtlessly happy to use generative tools when they are effective. But contrast the Google search

---

28 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3 at 160 (footnote omitted).

29 *See id.* at 230 (asserting that ReputationDefender uses "moral suasion" as its primary technique for manipulating search-engine results). I offer a very different perspective on this. *See* Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383 (2009).

30 Zittrain himself noted something similar, writing, "If the Wikipedia entry on Wal-Mart is one of the first hits in a search for the store, it will be important to Wal-Mart to make sure the entry is fair—or even more than fair, omitting true and relevant facts that nonetheless reflect poorly on the company." *See* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3 at 139.

31 *See* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3 at 147. Zittrain tacitly acknowledges this: "There are plenty of online services whose choices can affect our lives. For example, Google's choices about how to rank and calculate its search results can determine which ideas have prominence and which do not."

engine with Google's Gmail, and it becomes apparent that the same company will keep a service tethered and proprietary when doing so best suits its purposes.[32]

The idiosyncratic online juggernaut that is Wikipedia, to which Zittrain devotes virtually an entire chapter, also illustrates some of the downsides of excessive generativity.[33] Wikipedia is an online encyclopedia that, at least in theory, anyone can edit. Zittrain is clearly enamored of it, writing, "Wikipedia stands at the apex of amateur endeavor: an undertaking done out of sheer interest in or love of a topic, built on collaborative software that enables a breathtakingly comprehensive result that is the sum of individual contributions, and one that is extraordinarily trusting of them."[34] Zittrain provides a lot of information about Wikipedia, and the vast majority of it skews positive. He writes, "Wikipedia has charted a path from crazy idea to stunning worldwide success";[35] and "Wikipedia is the canonical bee that flies despite scientists' skepticism that the aerodynamics add up";[36] and asserts that the manner in which Wikipedia operates "is the essence of law."[37] Perhaps echoing Zittrain's enthusiasm, one researcher determined Wikipedia has been cited in over 400 U.S. court opinions.[38]

Among myriad other facts and anecdotes, Zittrain notes that Wikipedia co-founder Larry Sanger is controversial because possibly he is given too much credit for his limited contributions to Wikipedia.[39] He also notes that another person involved with Wikipedia, former Wikimedia Foundation member Angela

---

32 *See generally* Paul Boutin, *Read My Mail, Please*, SLATE, Apr. 15, 2004, **http://slate.msn.com/id/2098946**; Deane, *Critics Release the Hounds on GMail*, GADGETOPIA, Apr. 10, 2004, **http://gadgetopia.com/post/2254**; Google Watch, **http://www.google-watch.org/gmail.html**; Brian Morrissey, *An Early Look at How Gmail Works*, DMNEWS, Apr. 19, 2004, **http://www.dmnews.com/an-early-look-at-how-gmail-works/article/83946**.

33 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, chapter six.

34 *Id.* at 96.

35 *Id.* at 136.

36 *Id.* at 148.

37 *Id.* at 144.

38 Lee F. Peoples, *The Citation of Wikipedia in Judicial Opinions*, 12 YALE J.L. & TECH. (forthcoming 2009), *available at* **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1272437**.

39 *See* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 143 ("At times—they are constantly in flux—Wikipedia's articles about Wikipedia note that there is controversy over the 'co-founder' label for Sanger."); *see also* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3 at 142, 145.

Beesley Starling, unsuccessfully fought to have her Wikipedia entry deleted.[40] That a man who wants undeserved credit and a woman who wants no attention at all have likely both been thwarted by Wikipedians is something Zittrain seems to view as a positive indicator. Angela Beesley Starling probably feels very differently, especially if her reasons for wanting her Wikipedia entry deleted included pressing personal safety concerns. The "talk" page of her Wikipedia biography quotes her as saying, "I'm sick of this article being trolled. It's full of lies and nonsense."[41] The forced publicity of Wikipedia entries is something all women may encounter under Wikipedia's "system of self-governance that has many indicia of the rule of law without heavy reliance on outside authority or boundary."[42] Research suggests that women, though 51% of the population, comprise a mere 13% of Wikipedia contributors,[43] for reasons that probably have to do with the culture of this entity, which women may experience more negatively than men do.

Certainly notable living feminists have been on the receiving end of a campaign of nasty and untruthful edits to Wikipedia entries they would probably prefer not to have. Many entries on feminism have been written or edited by people who are actively hostile toward feminists, but they prevail because they seem to have a lot of free time and the few feminists who enter the wikifray seem to get driven out or edited into oblivion. To take just one example, the entries about Melissa Farley,[44] Catharine MacKinnon,[45]and Sheila Jeffries[46] have all been

---

40 *Id.* at 143.

41 *See Angela Beesley Starling Talkpage*, WIKIPEDIA,**http://en.wikipedia.org/wiki/Talk:Angela_Beesley_Starling** (last visited Sept. 4, 2009) ("Angela Beesley has tried to have her biography on Wikipedia deleted, saying 'I'm sick of this article being trolled. It's full of lies and nonsense.' The Register and Wikitruth claim that her objections are ironic in light of the generally liberal policy of Wikipedia administrators to the accuracy and notability of biographies in Wikipedia of living people. Seth Finkelstein, who tried to have his own entry from Wikipedia removed, called it 'a pretty stunning vote of no-confidence. Even at least some high-ups can't eat the dog food.'") (footnotes omitted).

42 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3 at 143.

43 *See, e.g.*, Andrew LaVallee, *Only 13% of Wikipedia Contributors Are Women, Study Says*, WALL ST. J., Aug. 31, 2009, **http://blogs.wsj.com/digits/2009/08/31/only-13-of-wikipedia-contributors-are-women-study-says**; Jennifer Van Grove, *Study: Women and Wikipedia Don't Mix*, MASHABLE, Sept. 1, 2009, **http://mashable.com/2009/09/01/women-wikipedia**; Cathy Davidson, *Wikipedia and Women*, HASTAC, Sept. 2, 2009, **http://www.hastac.org/blogs/cathy-davidson/wikipedia-and-women**.

44 *See Melissa Farley*, WIKIPEDIA, **http://en.wikipedia.org/wiki/Melissa_Farley** (last visited July28, 2009).

45 *See Catharine MacKinnon,* WIKIPEDIA, **http://en.wikipedia.org/wiki/Catharine_MacKinnon** (last visited July 28, 2009).

heavily edited[47] by a rabid pornography proponent named Peter G. Werner[48] who sometimes also uses the pseudonym Iamcuriousblue.[49] Each entry is the first result returned after a Google search of their names. He has deleted or attempted to have deleted entries about other feminists.[50] He shows up under one identity or another in virtually every entry in which feminism is mentioned. And he successfully convinced the Wikipedia community to ban a feminist activist who vigorously contested his edits.[51] Any group that is not well represented within the Wikipedia editing community is likely to experience similar marginalization.

Recently, Wikipedia announced that the entries of living people will receive a mandatory layer of intermediation. A new feature called "flagged revisions" will require that an experienced volunteer editor sign off on any changes before they become permanent and publicly accessible.[52] A New York Times report noted that this would "divide Wikipedia's contributors into two classes—experienced, trusted editors, and everyone else—altering Wikipedia's implicit notion that everyone has an equal right to edit entries."[53] This seems to be one realization of what Zittrain broadly desires—control over the ignorant wikimasses by a designated elite. But the project became significantly less collaborative and open when this change was made.

Wikipedia entries are generated by a massive assemblage of volunteers with unknown motivations and agendas. Group behavior is always unpredictable, a fact that Zittrain acknowledges but under-appreciates. One somewhat organized assemblage that calls itself Anonymous launches cyber-attacks that

---

46 *See Sheila Jeffreys,* WIKIPEDIA, **http://en.wikipedia.org/wiki/Sheila_Jeffreys** (last visited July 28, 2009).

47 *See, e.g.*, *Catharine MacKinnon Talkpage*, WIKIPEDIA, **http://en.wikipedia.org/wiki/Talk:Catharine_MacKinnon** (last visited July 28, 2009).

48 *See Peter G Werner Userpage*, WIKIPEDIA, **http://en.wikipedia.org/wiki/User:Peter_G_Werner** (last visited July 28, 2009).

49 *See Iamcuriousblue Userpage*, WIKIPEDIA, **http://en.wikipedia.org/wiki/User:Iamcuriousblue** (last visited July 28, 2009).

50 *See, e.g.*, *Articles for deletion/Cheryl Lindsey Seelhoff,* WIKIPEDIA, **http://en.wikipedia.org/w/index.php?title=Wikipedia:Articles_for_deletion/Cheryl_Lindsey_Seelhoff&oldid=150110815** (last visited Sept. 25, 2009), *see also Nikki Craft Talkpage*, WIKIPEDIA, **http://en.wikipedia.org/wiki/Talk:Nikki_Craft** (last visited Sept. 25, 2009).

51 Telephone interview with Nikki Craft; *see also Nikki Craft Talkpage*, *supra* (containing conversation in which user Iamcuriousblue discredits Nikki Craft's Wikipedia article).

52 Noam Cohen, *Wikipedia to Limit Changes to Articles on People*, N.Y. TIMES, Aug. 25, 2009, at B1.

53 *Id.*

online norms do not seem to have any cognizable role in addressing.[54] As with Wikipedians, Anonymous is hostile to others and outsiders. One blogger noted:

> Interestingly … Anon never seems to take down the big sites. Walmart.com and the Pentagon are safe from his attentions. It's not that Anon is a big fan of Walmart or the government. It's just so much easier to attack the vulnerable. Big business and big government aren't vulnerable on the Internet. They can afford not to be.
>
> Small discussion boards and blogs, particularly ones that advocate unpopular points of view, are often run by individuals who put up their own funds, if they can scrape them together, and who must be their own IT departments. They can't afford the type of security that requires the big bucks. And since they have jobs (unlike Anon, apparently), they have to put their desire to maintain an Internet presence in the balance with supporting themselves and their families. When the crunch comes and time pressures set in, it's not the Internet presence that wins out.
>
> So the actions of these "apolitical" hackers do have a political end: They remove unpopular, radical, fringe viewpoints from

---

54 *See e.g.*, Shaun Davies, *'No Cussing' Teen Faces Net Hate Campaign*, NINEMSN NEWS, Jan. 18, 2009, **http://news.ninemsn.com.au/technology/720115/no-cussing-teen-faces-net-hate-campaign** (stating "McKay Hatch's No Cussing Club, which encourages teens to 'chill on the profanity', claims to have over 20,000 members worldwide. Hatch, a 15-year-old from South Pasadena in California, garnered wide media coverage for his anti-swearing campaign, including an appearance on Dr Phil. But at the beginning of the year, Hatch's email inbox began clogging up with hate mail from an unknown source. Pizza and porn deliveries became commonplace for his family, who eventually called in the FBI after numerous receiving[sic] death threats and obscene phone calls. Anonymous appears to be behind the attacks, with threads on sites such as 4chan.org and 711chan.org identifying their members as the culprits. And the pain may not yet be over for the Hatch family—Anonymous appears to be planning future raids and has threatened to 'wipe this cancer [the No Cussing Club] from the face of the internet'.[sic] In one 4chan thread, a number of users boasted about sending bogus pizza deliveries and even prostitutes to the Hatchs' house, although it was impossible to verify if these claims were genuine. The same thread also contained a credit card number purported to be stolen from Hatch's father, phone numbers, the family's home address and Hatch's instant messenger address."); *see also Behind the Façade of the "Anonymous" Hate Group*, RELIGIOUS FREEDOM WATCH, July 6, 2009, **http://www.religiousfreedomwatch.org/media-newsroom/behind-the-facade-of-the%E2%80%9Canonymous%E2%80%9D-hate-group/**; *see* also *Alex Wuori*, ENCYCLOPAEDIA DRAMATICA, **http://encyclopediadramatica.com/Alex_Wuori** (last visited July 28, 2009).

> the web. Big government doesn't have to eliminate the subversive websites; Anon will do it.[55]

The activities of Anonymous have been characterized as domestic terrorism.[56] And Anonymous certainly takes advantage of generative technologies, just as Wikipedians with reprehensible agendas do. Zittrain asserts that bad actors like Anonymous are driving the demand for increased security,[57] but he doesn't provide any targeted mechanisms for hindering them, or explain why increasing security necessarily compromises productive generativity.

## The Zittrainnet's Netizens: Overlords of Good Faith

As with a James Joyce novel, there are a variety of transactions that the careful reader negotiates with the author. Each section has to be read independently of the others, because while it may cohere internally, it may not combine with other delineated portions to paint a consistent picture of Zittrain's preferred future for the Internet, which will hereafter be called the "Zittrainnet."

Some of the recommendations he makes invite broad democratic participation in Zittrainnet governance, while other times he warns against it and suggests ways to decrease the threats posed "by outsiders—whether by vendors, malware authors, or governments."[58] One wonders how something as disaggregated as the Internet can have outsiders, until recognition dawns about what Zittrain is truly suggesting, at least part of the time, in terms of who should control the Internet to best ensure its evolution into the Zittrainnet: an elite circle of people with computer skills and free time who share his policy perspective.

### Technologists Rule

Zittrain doesn't contemplate "anyone" developing serviceable code. Zittrain's view is that only a select few can take productive advantage of generativity, and within this elite group are bad actors as well as good. He thinks that cyberlaw is the appropriate mechanism to encourage positive uses of generativity while

---

55 VeraCity, *Dominator Tentacles*, **http://vera.wordpress.com/2007/08/24/dominator-tentacles/** (Aug. 24, 2007).

56 VA. FUSION CTR., VA. DEP'T OF STATE POLICE, 2009 VIRGINIA TERRORISM THREAT ASSESSMENT 48 (2009), *available at* **http://www.infowars.com/virginia-fusion-center-releaseshomegrown-terrorism-document/**.

57 *See generally* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at chapter 3. This is one of the central claims of the book.

58 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 173.

thwarting the troublesome ones, cyberlaw being computer-code construction and norm entrepreneurship within Internet communities, as well as more traditionally recognized modes of law formation such as statutes and regulations.[59] As far as who exactly will divine good generativity from bad, and wield the mighty sword of cyberlaw to defend the former and defeat the latter, Zittrain is decidedly vague. In the "Solutions" section of the tome Zittrain lists "two approaches that might save the generative spirit of the Net":

> The first is to reconfigure and strengthen the Net's experimentalist architecture to make it fit better with its now-mainstream home. The second is to create and demonstrate the tools and practices by which relevant people and institutions can help secure the Net themselves instead of waiting for someone else to do it.[60]

By "relevant people and institutions" Zittrain seems to mean technologically skilled, Internet users of good will.[61] But as far as who it is that will "reconfigure and strengthen the Net's experimentalist architecture" or who will "create and demonstrate the tools and practices" on behalf of these relevant people and institutions (shall we call them "generativators?"), Zittrain offers few specifics. He mentions universities generally,[62] and two organizations he is affiliated with specifically, Harvard University's Berkman Center (where he is one of 13 Directors—all male, of course[63]) and the Oxford Internet Institute (where he is a Research Associate[64]), which he describes as "multidisciplinary academic enterprises dedicated to charting the future of the Net and improving it."[65] Those who share his visions for the Zittrainnet are supposed to function as norm entrepreneurs, guiding lights for the undereducated, inadequately skilled online masses to follow, sheep-like.

Less-relevant people are described as "[r]ank-and-file Internet users [who] enjoy its benefits while seeing its operation as a mystery, something they could not

---

59 *Id.* chapter 5.

60 *Id.* at 152.

61 *Id.* at 246.

62 *Id.* at 198, 245.

63 *See People*, Berkman Center for Internet and Society at Harvard University, **http://cyber.law.harvard.edu/people**.

64 *See People*, OXFORD INTERNET INSTITUTE UNIVERSITY OF OXFORD, **http://www.oii.ox.ac.uk/people/?status=current&type=&keywords=zittrain**.

65 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 159.

possibly hope to affect."[66] These ignorant non-generativators frighten Zittrain, because when he fears that, a crisis comes, they will pressure the government to enhance Internet security at the expense of Internet generativity, out of short-sighted, ill-informed perceptions of their own self-interest.[67] He knows better than they do what's best for them.

In a related article he published in *Legal Affairs* to promote the book, Zittrain explains:

> If the Internet does have a September 11 moment, a scared and frustrated public is apt to demand sweeping measures to protect home and business computers—a metaphorical USA Patriot Act for cyberspace. Politicians and vendors will likely hasten to respond to these pressures, and the end result will be a radical change in the technology landscape. The biggest casualty will likely be a fundamental characteristic that has made both the Internet and the PC such powerful phenomena: their "generativity."[68]

Many of the stories Zittrain tells in the book are intended to persuade readers that unless somebody does something, the Internet will do what the book's cover suggests: derail and drive over a cliff. But after ominously warning his audience repeatedly that "Steps Must Be Taken Immediately," the particulars of whom that somebody is and the details of what s/he should be doing are never made explicit.

In addition, the law component of cyberlaw gets surprisingly little attention in the book, given that Zittrain is a law professor. According to Larry Lessig, "This book will redefine the field we call the law of cyberspace."[69] This is

---

66 *Id.* at 245.

67 *Id.*

68 *See* Jonathan Zittrain, *Without a Net*, LEGAL AFFAIRS, Jan./Feb. 2006, at 34, available at **http://www.legalaffairs.org/issues/January-February-2006/feature_zittrain_janfeb06.msp**; *see also* Lawrence Lessig, *Z's Book Is Out*, LESSIG 2.0, May 1, 2008, **http://lessig.org/b.og/just_plain_brilliant/** [hereinafter Lessig, *Z's Book Is Out*]; Lawrence Lessig, *The state of Cyberlaw, 2005*, LESSIG 2.0, Dec. 30, 2005, **http://lessig.org/b.og/read_this/** (stating "Legal Affairs has a fantastic collection of essays about various cyberspace related legal issues by some of my favorite writers about the subject. Zittrain's piece outlines the beginning of his soon to be completed book. It shall be called Z-theory.").

69 *See* Lessig, *Z's Book Is Out*, *supra*. Lessig explains his thoughts regarding the importance of Zittrain's book in his blog:

> This book will redefine the field we call the law of cyberspace. That sounds like a hokey blurb no doubt. But hokeness [sic] does not mean it is not true.

worrisome to anyone still struggling to ascertain the parameters of cyberlaw in the first instance, beyond the macro concerns about top-down versus bottom-up approaches to governance identified by the scholars mentioned above. The role of law in Zittrainnet's rule of law is extremely limited. Laws concerning jurisdiction, privacy, free speech, copyrights, and trademarks often transmogrify into cyberlaw when they are invoked in an Internet context, but they exist and evolve offline too, which prevents their total capture by cyberlaw scholars. Zittrain's redefinition of cyberlaw compresses debates that engage complicated, intersecting bodies of law into a much narrower conversation about the value of generativity, and how best to secure the appropriate level of it. In general Zittrain seems quite pessimistic about whether cyberlaw can achieve anything positive beyond somehow—he never tells us how—fostering generativity. At one point in the book he even describes the enforcement of laws online as something that could result in net social losses, and therefore a mechanism of Internet governance that is inferior to "retention of generative technologies."[70]

Zittrain seems to have a lot more confidence in technologists than in attorneys. He waxes rhapsodic about the wisdom and forethought of the "framers" of the Internet throughout the tome.[71] One of "the primary" ways he proposes to address tetheredness and its associative ills is "a series of conversations, arguments, and experiments whose participants span the spectrum between network engineers and PC software designers, between expert users with time

---

> It is true. The field before this book was us cheerleaders trying to convince a skeptical (academic) world about the importance and value of certain central features of the network. Zittrain gives these features a name—generativity—and then shows us an aspect of this generative net that we cheerleaders would rather you not think much about: the extraordinary explosion of malware and the like that the generative net has also generated.

[70] *See* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 113-114. Zittrain states:

> Technologies that lend themselves to an easy and tightly coupled expression of governmental power simply will be portable from one society to the next. It will make irrelevant the question about how firms like Google and Skype should operate outside their home countries.
>
> This conclusion suggests that although some social gain may result from better enforcement of existing laws in free societies, the gain might be more than offset by better enforcement in societies that are less free—under repressive governments today, or anywhere in the future. If the gains and losses remain coupled, it might make sense to favor retention of generative technologies to put what law professor James Boyle has called the "Libertarian gotcha" to authoritarian regimes: if one wants technological progress and the associated economic benefits, one must be prepared to accept some measure of social liberalization made possible with that technology.

[71] *See* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 7, 27, 31, 33, 34, 69, 99.

to spend tinkering and those who simply want the system to work—but who appreciate the dangers of lockdown" (p. 173). On the Zittrainnet, with the exception of a select few cyberlaw professors, academics in disciplines other than law, particularly computer science, are going to be the true benevolent dictators of cyberlaw, mediating disputes with technological innovations and enforcing their judgments through code.

## The Private Sector

Zittrain quite understandably doubts that for-profit entities will selflessly prioritize the well-being of the Internet over their own commercial gain. So, they are unlikely to consistently adhere to pro-generative business plans unless they can be convinced that doing so will benefit them. One of Zittrain's objectives in writing the book was to educate the reader about the ways that extensive generativity can serve commercial goals. However, while corporate actors may find Zittrain's book of interest, I suspect actual experiences in the marketplace will be what drives their decisions about tethers and generativity.

Zittrain opens his book with what is framed as an apocryphal tale: Apple II computers were revolutionary because they facilitated the development of new and original uses by outsiders; but thirty years later the same company launched an anti-generativity counterrevolution of sorts by releasing its innovative iPhone in a locked format intended to discourage the use of applications that were not developed or approved by Apple.[72]

But how would Zittrain change this? Surely when the company made this decision, it knew even more than Zittrain about the role that generativity played in the success of the Apple II, but still chose a different strategy for the iPhone. Affirmative curtailment of its generativity initially lowered the risk that iPhones would be plagued by viruses or malware, and allowed Apple to control the ways that most consumers use them. Would Zittrain have forced generativity into the mechanics of the iPhone by law? Or, would he strip Apple of its ability to use the law to interfere when others hack the iPhone and make it more customizable? Or, would he instead simply wait for the market to show Apple the error of its degenerative ways? He never specifies. What he says at the end of his iPhone discussion is:

> A lockdown on PCs and a corresponding rise of tethered appliances will eliminate what today we take for granted: a world where mainstream technology can be influenced, even revolutionized, out of left field. Stopping this future depends

---

72 *See generally* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 86–87 (summarizing work by Eric von Hippel on the subject).

> on some wisely developed and implemented locks, along with new technologies and a community ethos that secures the keys to those locks among groups with shared norms and a sense of public purpose, rather than in the hands of a single gatekeeping entity, whether public or private.[73]

It sounds like Zittrain wants to prevent Apple from interfering when consumers modify their iPhones. But how he proposes to achieve this is addressed only generally, much later in the book when he suggests vague, persuasion-based solutions. My inner pragmatist thinks strong consumer protection laws might be a viable option to this and many other problems he articulates in the book, but Zittrain mentions that possibility only glancingly, in the context of maintaining data portability.[74]

In July of 2008, Apple began allowing software developers to sell software for the iPhone, and tens of thousands of applications have subsequently been independently developed for the iPhone,[75] suggesting either successful deployment of a strategic multistep product rollout Apple had planned all along, or a midcourse marketing correction. In either event, after the App Store the iPhone cannot accurately be described as non-generative, at least as I understand the concept,[76] and what Zittrain characterized as a problem seems to have been largely solved without the intervention of cyberlaw. The iPhone is still tethered, of course, possibly giving consumers just enough rope to hang themselves if Apple decides to interfere with the contents or operation of any given phone. But tethering also facilitates positive interactions, such as updates and repairs. It is now, to use a phrase Zittrain uses in a different context, "[a] technology that splits the difference between lockdown and openness."[77]

It is true that Apple could alter the iPhone's balance between generativity and tetheredness without notice or reason. But there is every reason to expect that Apple will try to keep its customers happy, especially given increased competition by devices running Google's Android operating system—with its

---

73 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 5.

74 *Id.* at 177.

75 *See, e.g.*, Jon Fortt, *iPhone apps: For fun and profit?*, FORTUNE TECH DAILY, July 6, 2009, **http://money.cnn.com/2009/07/06/technology/apple_iphone_apps.fortune/index.htm**

76 *See, e.g.*, Adam Thierer *iPhone 2.0 cracked in hours … what was that Zittrain thesis again?*, THE TECHNOLOGY LIBERATION FRONT, July 10, 2008, **http://techliberation.com/2008/07/10/iphone-20-cracked-in-hours-what-was-that-zittrain-thesis-again/**.

77 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 155.

even more open apps marketplace.[78] A recent short review of the book in *The Observer* noted:

> The problem facing books about the internet is that by the time they have hit the shelves, they are already dated. This is clear on the second page of The Future of the Internet, where Jonathan Zittrain writes that the iPhone is purposefully resistant to "applications" (programmes allowing the phone to do clever things apart from make calls).[79]

The problem facing this book is deeper than datedness. Zittrain is wrong in his assumptions about rigidity and fixedness.[80] In the abstract generativity and tetheredness may be opposites, but in reality they can exist within a single appliance. He actually makes this point when he describes computers with dual applications designated "red" and "green," one generative and the other secure.[81] But he does not acknowledge that many technological devices already

---

78 Yi-Wyn Yen & Michal Lev-Ram, *Google's $199 Phone to Compete with the iPhone*, TECHLAND, Sept. 17, 2008, **http://techland.blogs.fortune.cnn.com/2008/09/17/googles-199-phone-to- compete-with-the-iphone/**.

79 Helen Zaltzman, *The Future of the Internet by Jonathan Zittrain*, OBSERVER (London), June 14, 2009, at 26, *available at* **http://www.guardian.co.uk/books/2009/jun/14/future-internet-zittrain-review**.

80 *See* Adam Thierer, *Review of Zittrain's "Future of the Internet"*, THE TECHNOLOGY LIBERATION FRONT, Mar. 23, 2008, **http://techliberation.com/2008/03/23/review-of-zittrains-future-of-the-internet/**. Thierer writes:

> My primary objection to Jonathan's thesis is that (1) he seems to be over-stating things quite a bit; and in doing so, (2) he creates a false choice of possible futures from which we must choose. What I mean by false choice is that Jonathan doesn't seem to believe a hybrid future is possible or desirable. I see no reason why we can't have the best of both worlds—a world full of plenty of tethered appliances, but also plenty of generativity and openness.

*See also* Timothy B. Lee, *Sizing Up "Code" With 20/20 Hindsight*, FREEDOM TO TINKER, May 14, 2009, **http://www.freedom-to-tinker.com/blog/tblee/sizing-code-2020-hindsight**. Lee writes:

> I think Jonathan Zittrain's The Future of the Internet and How to Stop It makes the same kind of mistake Lessig made a decade ago: overestimating regulators' ability to shape the evolution of new technologies and underestimating the robustness of open platforms. The evolution of technology is mostly shaped by engineering and economic constraints. Government policies can sometimes force new technologies underground, but regulators rarely have the kind of fine-grained control they would need to promote "generative" technologies over sterile ones, any more than they could have stopped the emergence of cookies or DPI if they'd made different policy choices a decade ago.

81 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 154-57.

shift between tethered and generative functions, driven by the demands of their users.

Making assumptions about consumer preferences can be hazardous, especially for folks who tend to associate mostly with people who share common interests, common backgrounds, a common race, a common gender. The Zittrainnet's netizens, being human, are likely to engage in all manner of typecasting and generalizing when they redesign their Internet sectors of interest. If the leading netizens echo the demographic pattern of the cyberlaw scholars, white men with elite educations will be making most of the calls.[82] And Internet governance will be exceedingly top-down.

At present companies can dramatically alter the levels of tetheredness and generativity in their products and services for any reason or no reason at all, and Zittrain never explains what sort of regulations or market interventions he thinks are necessary to achieve or preserve the Zittrainnet. He is critical of companies that assist totalitarian governments with surveillance or censorship initiatives,[83] but fails to acknowledge the reason that many technologies that can be readily employed to spy on people are developed: Companies want to be able to shadow and scrutinize their customers themselves. Consumers usually agree to this scrutiny in nonnegotiable EULA terms and conditions. For companies, closely following the acts and omissions of their customers or client base is generative behavior, even though it relies on tethers. Information about consumers can lead to innovations in goods and services as well as in marketing them.

## Governments

Zittrain expresses grave concerns about government intervention on the Internet. He does not seem to believe that government actors can competently safeguard users, or effectively regulate technology. And he fears governments will further harness the Internet to advance surveillance and censorship agendas that are anathema to freedom. Zittrain writes with deep foreboding:

> The rise of tethered appliances significantly reduces the number and variety of people and institutions required to apply the state's power on a mass scale. It removes a practical check on the use of that power. It diminishes a rule's ability to attain

---

82 *See* Anupam Chander, *Whose Republic?*, 69 U. CHI. L. REV. 1479, 1484–85 (2002) (reviewing CASS SUNSTEIN, REPUBLIC.COM (2001)).

83 ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 112–13.

> legitimacy as people choose to participate in its enforcement, or at least not stand in its way.[84]

So it seems strange to learn that his solution to too much tethering is "a latter-day Manhattan Project."[85] The Manhattan Project was, of course, the code name for the U.S. government's secret project to develop a nuclear bomb. It may have been staffed by scientists, many of whom were academics, but it was organized, funded, and strictly controlled by the government.[86] An analogous initiative to formulate the Zittrainnet would hardly be open and accessible to the online public. Moreover, governments generally take some kind of proprietary interest in the outcomes of projects they fund. Even under the Bayh-Dole Act,[87] which allows universities in the United States to patent inventions developed with federal funding, the U.S. government retains march-in rights.[88] Zittrain seems to want the resources that governments can provide without any of the restrictions or obligations governments will, as experience suggests, inevitably impose. It's possible that a well-crafted Zittrainet Project could receive the unconditional support of government actors, but I don't think this is terribly likely to happen.

Surprisingly, one of the success stories for generativity that Zittrain references is the Digital Millennium Copyright Act of 1998.[89] Not only did this require government intervention in the form of traditional law, but it also relied on tethering. Web sites could not take down potentially infringing material without retaining a level of control that enables this.

In addition to generativity, one of the defining principles of the Zittrainnet will be adherence to First Amendment principles. Zittrain's descriptions of online freedom and autonomy suggest a strong belief that all the countries of the world

---

84 *Id.* at 118.

85 *Id.* at 173.

86 U.S. DEP'T OF ENERGY, OFFICE OF HISTORY & HERITAGE RES., *Early Government Support*, *in* THE MANHATTAN PROJECT: AN INTERACTIVE HISTORY, **http://www.cfo.doe.gov/me70/manhattan/1939-1942.htm** (last visited July 30, 2009); *The Manhattan Project (and Before)*, *in* THE NUCLEAR WEAPON ARCHIVE, **http://nuclearweaponarchive.org/Usa/Med/Med.html** (last visited Oct. 4, 2009); U.S. DEP'T OF ENERGY, OFFICE OF HISTORY & HERITAGE RES., *A Tentative Decision to Build the Bomb*, *in* THE MANHATTAN PROJECT: AN INTERACTIVE HISTORY, **http://www.cfo.doe.gov/me70/manhattan/tentative_decision_build.htm** (last visited July 30, 2009).

87 35 U.S.C. §§ 200–212 (2006).

88 *Id.* § 203.

89 *See* Pub. L. No. 105–304, 112 Stat. 2860 (1998). *See also* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 119–20 (stating Zittrain's discussion of the DMCA).

should honor and implement the free-speech values of the First Amendment, whether they want to or not.[90] This raises complicated issues of state sovereignty and international law that Zittrain does not address.

## Conclusion

I've been very hard on *The Future of the Internet* in this review, but I truly did enjoy reading it. The book is very informative, if you can sift through the portions contrived to illustrate an unconvincing macro theory of the Internet. I wish Zittrain had written a book that set out only to describe the history and state of the Internet, rather than one that was formulated to support questionable generalizations and grandiose prescriptions. He could have told many of the same extremely interesting stories, but with more balance and less of a blatant "big think" agenda.

The book is woefully lacking in specifics, in terms of advancing the reforms Zittrain asserts are necessary. Even if I were willing to buy into Zittrain's claim that preserving and enhancing generativity should be the organizing principle of the Internet governance interventions, the mechanics of how this could be pursued holistically are never revealed. And the technicalities by which good generativity could be fostered while bad generativity was simultaneously repressed are similarly unstated. The only extensively developed account of a generative system Zittrain unabashedly admires is Wikipedia, which he admits is undemocratic.[91] It is also a system that facilitates repression of unpopular viewpoints, and this is likely to affect outsider groups most dramatically.

Who will step forward to somehow cultivate the Zittrainnet is a mystery. The future of the Internet, Zittrain asserts, would be much safer in the hands of those who can competently safeguard it. He describes these people in very general terms as being skilled and of good faith. These hands do not belong to people who are affiliated with dot-coms, because they use tethering to constrain generativity when doing so is profitable. Nor do they belong to dot-gov bureaucrats, who are at best uninformed and at worst eager to use the Internet to enforce regimes of totalitarian rule. Readers of the book learn a lot more about who Zittrain thinks should *not* be in control of the Internet than who should be. But there are a number of hints and suggestions scattered throughout its pages that he believes he and his colleagues are capable of directing the Internet's future wisely and beneficently. If they are going to attempt to do this by writing books, perhaps Zittrain's offering makes sense as a

---

90 *Contra* Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS 261 (2002).

91 *See* ZITTRAIN, THE FUTURE OF THE INTERNET, *supra* note 3, at 141 ("And Wikipedia is decidedly not a democracy: consensus is favored over voting and its head counts.").

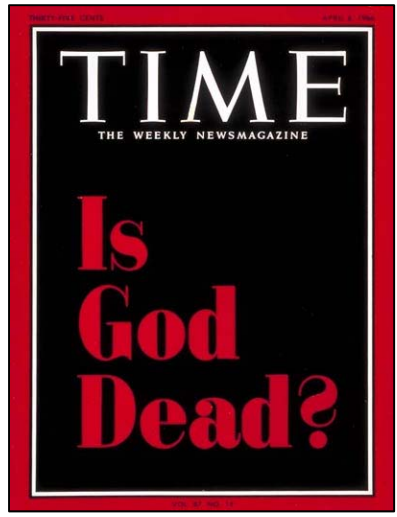
declaration of first principles. Maybe his next book will describe the steps along the path to the Zittrainnet more concretely.

# The Case for Internet Optimism, Part 2: Saving the Net from Its *Supporters*

By Adam Thierer*

*In an earlier essay, I argued that two distinct strands of "Internet pessimism" increasingly dominate Internet policy discussions. The pessimism of "Net skeptics" is rooted in a general skepticism of the supposed benefits of cyberspace, digital technologies, and information abundance. Here, I respond to a very different strand of Internet pessimism—one expressed by fans of the Internet and cyberspace who nonetheless fear that dark days lie ahead unless steps are taken to "save the Net" from a variety of ills, especially the perceived end of "openness."*

## Introduction: Is the Web Really Dying?




"The Death of the Internet" is a hot meme in Internet policy these days. Much as a famous *Time* magazine cover asked "Is God Dead?" in 1966,[1] *Wired* magazine, the magazine for the modern digerati, proclaimed in a recent cover story that "The Web is Dead."[2] A few weeks later, *The Economist* magazine ran a cover story fretting about "The Web's New Walls," wondering "how the threats to the Internet's openness can be averted."[3] The primary concern expressed in both essays:

---

* Adam Thierer is a senior research fellow at the **Mercatus Center at George Mason University** where he works with the **Technology Policy Program**.

1 "Is God Dead?" TIME, April 8, 1966, **www.time.com/time/covers/0,16641,19660408,00.html**

2 Chris Anderson & Michael Wolff, *The Web Is Dead. Long Live the Internet*, WIRED, Aug. 17, 2010, **www.wired.com/magazine/2010/08/ff_webrip/all/1**. Incidentally, there's a long history of pundits declaring just about everything "dead" at some point, from email, RSS, and blogging to eReaders, browser, and even Facebook and Twitter. *See* Harry McCracken, *The Tragic Death of Practically Everything*, TECHNOLOGIZER, Aug. 18, 2010, **http://technologizer.com/2010/08/18/the-tragic-death-of-practically-everything**

3 *The Web's New Walls*, THE ECONOMIST, Sept. 2, 2010, **www.economist.com/research/articlesBySubject/displayStory.cfm?story_id=16943579&subjectID=348963&fsrc=nwl**

The wide-open Internet experience of the past decade is giving way to a new regime of corporate control, closed platforms, and walled gardens.


This fear is given fuller elucidation in recent books by two of the intellectual godfathers of modern cyberlaw: Jonathan Zittrain's *The Future of the Internet—And How to Stop It*,[4] and Tim Wu's *The Master Switch: The Rise and Fall of Information Empires*.[5] These books are best understood as the second and third installments in a trilogy that began with the publication of Lawrence Lessig's seminal 1999 book, *Code and Other Laws of Cyberspace*.[6]

Lessig's book framed much of how we study and discuss cyberlaw and Internet policy. More importantly, *Code* spawned a *bona fide* philosophical movement within those circles as a polemic against both cyber-libertarianism and Internet exceptionalism (closely related movements), as well as a sort of call to arms for a new Net activist movement. The book gave this movement its central operating principle: Code and cyberspace *can* be bent to the will of some amorphous collective or public will, and it often *must* be if we are to avoid any number of impending disasters brought on by nefarious-minded (or just plain incompetent) folks in corporate America scheming to achieve "perfect control" over users.

It's difficult to know what to label this school of thinking about Internet policy, and Prof. Lessig has taken offense at me calling it "cyber-collectivism."[7] But the collectivism of which I speak is a more generic type, not the hard-edged Marxist brand of collectivism of modern times. Instead, it's the belief that markets, property rights, and private decision-making about the future course of the Net must yield to supposedly more enlightened actors and mechanisms. As Declan McCullagh has remarked, Lessig and his students

---

4 JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008).

5 TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2010).

6 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

7 Adam Thierer, *Our Conflict of Cyber-Visions*, CATO UNBOUND, May 14, 2009, **www.cato-unbound.org/2009/05/14/adam-thierer/our-conflict-of-cyber-visions/**

> prefer … what probably could be called technocratic philosopher kings, of the breed that Plato's *The Republic* said would be "best able to guard the laws and institutions of our State—let them be our guardians." These technocrats would be entrusted with making wise decisions on our behalf, because, according to Lessig, "politics is that process by which we collectively decide how we should live."[8]

What is it, exactly, that these cyber-collectivists seek to protect or accomplish? To the extent it can be boiled down to a single term, their rallying cry is: Openness! "Openness" is almost always The Good; anything "closed" (restricted or proprietary) in nature is The Bad. Thus, since they recoil at the "cyber-collectivist" label, we might think of adherents to this philosophy as "Openness Evangelicals," since they evangelize in favor of "openness" and seemingly make all else subservient to it.

For example, in *Future of the Internet*, Zittrain argues that, for a variety of reasons, we run the risk of seeing the glorious days of "generative" devices and the "open" Internet give way to more "tethered appliances" and closed networks. He says:

> Today, the same qualities that led to [the success of the Internet and general-purpose PCs] are causing [them] to falter. As ubiquitous as Internet technologies are today, the pieces are in place for a wholesale shift away from the original chaotic design that has given rise to the modern information revolution. This counterrevolution would push mainstream users away from the generative Internet that fosters innovation and disruption, to an appliancized network that incorporates some of the most powerful features of today's Internet while greatly limiting its innovative capacity—and, for better or worse, heightening its regulability. A seductive and more powerful generation of proprietary networks and information appliances is waiting for round two. If the problems associated with the Internet and PC are not addressed, a set of blunt solutions will likely be applied to solve the problems at the expense of much of what we love about today's information ecosystem.[9]

---

8 Declan McCullagh, *What Larry Didn't Get*, CATO UNBOUND, May 4, 2009, **www.cato-unbound.org/2009/05/04/declan-mccullagh/what-larry-didnt-get**

9 Zittrain, *supra* note 4 at 8.

In other words, Zittrain fears most will flock to tethered appliances in a search for stability or security. That's troubling, he says, because those tethered appliances are less "open" and more likely to be "regulable," either by large corporate intermediaries or government officials. Thus, the "future of the Internet" Zittrain is hoping to "stop" is a world dominated by tethered digital appliances and closed walled gardens because they are too easily controlled by other actors.

My primary beef with these "Openness Evangelicals" is not that openness and generativity aren't fine generic principles but that:

1. They tend to significantly overstate the severity of this problem (the supposed decline of openness or generativity, that is);

2. I'm more willing to allow evolutionary dynamism to run its course within digital markets, even if that means some "closed" devices and platforms remain (or even thrive); and,

3. It's significantly more likely that the "openness" advocated by Openness Evangelicals will devolve into expanded government control of cyberspace and digital systems than that unregulated systems will become subject to "perfect control" by the private sector, as they fear.

More generally, my problem with this movement—and Zittrain's book, in particular—comes down to the dour, depressing "the-Net-is-about-to-die" fear that seems to fuel this worldview. The message seems to be: "Enjoy the good old days of the open Internet while you can, because any minute now it will be crushed and closed-off by corporate marauders!" Lessig started this nervous hand-wringing in *Code* when he ominously predicted that "Left to itself, cyberspace will become a perfect tool of control."[10] Today, his many disciples in academia (including Zittrain and Wu) and a wide variety of regulatory advocacy groups continue to preach this gloomy gospel of impending digital doom and "perfect control" despite plenty of evidence that supports the case for optimism.

For example, Wu warns there are "forces threatening the Internet as we know it"[11] while Zittrain worries about "a handful of gated cloud communities whose proprietors control the availability of new code."[12] At times, this paranoia of

---

10 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) at 5-6.

11 WU, *supra* note 5 at 7.

12 Jonathan Zittrain, *Lost in the Cloud*, NEW YORK TIMES, July 19, 2009, **www.nytimes.com/2009/07/20/opinion/20zittrain.html**.

some in the Openness Evangelical clan borders on outright hysteria. In August 2008, a Public Knowledge analyst likened Apple's management of applications in its iPhone App Store to the tyranny of Orwell's *1984*! [13] In other words, the Big Brother they want us to fear is *Corporate* Big Brother. Someday very soon, we are repeatedly told, the corporate big boys will toss the proverbial "master switch," suffocating Internet innovation and digital freedom, and making us all cyber-slaves within their commercialized walled gardens. The possibility of consumers escaping from these walled gardens or avoiding them altogether is treated as remote—if the notion is entertained at all.

We might think of this fear as "The Great Closing," or the notion that, unless radical interventions are pursued—often through regulation—a Digital Dark Age of Closed Systems will soon unfold, complete with myriad America Online-like walled gardens, "sterile and tethered devices," corporate censorship, and gouging of consumers. Finally, the implicit message in the work of all these hyper-pessimistic critics is that markets must be steered in a more sensible direction by those technocratic philosopher kings (although the details of their blueprint for digital salvation are often scarce).

## Problems with "The Great Closing" Thesis

There are serious problems with the "Great Closing" thesis as set forth in the high-tech threnody of Lessig, Zittrain, Wu, and other Openness Evangelicals, or ""as *The New York Times* has called them, digital "doomsayers."[14]

### No Clear Definitions of Openness or Closedness; Both Are Matters of Degree

"Open" vs. closed isn't as black and white as some Openness Evangelicals make it out to be. For example, Zittrain praises the supposedly more open nature of PCs and the openness to innovation made possible by Microsoft's Windows operating system. How ironic, since so many have blasted Windows as the Great Satan of closed code! Meanwhile, while most others think of Apple as "everyone's favorite example of innovation,"[15] Zittrain makes the

---

13 Alex Curtis, *Benefits of iPhone App Store Tainted by 1984-like Control*, Public Knowledge Blog, Aug. 11, 2008, **www.publicknowledge.org/node/1703** The tech gadget website Gizmodo recently ran a similar Apple-as-Big-Brother essay: Matt Buchanan, *Big Brother Apple and the Death of the Program*, GIZMODO, Oct. 22, 2010, **http://gizmodo.com/5670812/big-brother-apple-and-the-death-of-the-program**.

14 Eric Pfanner, *Proclaimed Dead, Web is Showing Signs of New Life*, NEW YORK TIMES, Oct. 31, 2010, **www.nytimes.com/2010/11/01/technology/01webwalls.html**

15 Amar Bhide, *Don't Expect Much From the R&D Tax Credit*, WALL STREET JOURNAL, Sept. 11, 2010, **http://online.wsj.com/article/SB10001424052748704644404575481534193344088.html**

iPhone and iPad out to be "sterile, tethered" appliances. But the company's App Store has offered millions of innovators the opportunity to produce almost every conceivable type of mobile application the human mind could imagine for those devices.[16] Moreover, those Apple devices don't block completely "open" communications applications or interfaces, such as Web browsers, email and SMS clients, or Twitter. "In the abstract," notes University of South Carolina School of Law professor Ann Bartow, "generativity and tetheredness may be opposites, but in reality they can exist within a single appliance."[17]

While the Apple devices seem to prove that, in reality, almost *all* modern digital devices and networks feature some generative and "non-generative" attributes. "No one has ever created, and no one will ever create, a system that allows any user to create anything he or she wants. Instead, every system designer makes innumerable tradeoffs and imposes countless constraints," note James Grimmelmann and Paul Ohm.[18] "Every generative technology faces … tradeoffs. Good system designers always restrict generativity of some kinds in order to encourage generativity of other kinds. The trick is in striking the balance," they argue.[19] Yet, "Zittrain never fully analyzes *split-generativity* systems, those with generative layers built upon non-generative layers, or vice-versa."[20]

The zero-sum fear that the ascendancy of mobile apps means less "generativity" or the "death of the Web" is another myth. Nick Bilton of *The New York Times* notes:

> Most of these apps and Web sites are so intertwined that it's difficult to know the difference. With the exception of downloadable games, most Web apps for news and services require pieces of the Web and Internet to function properly. So as more devices become connected to the Internet, even if they're built to access beautiful walled gardens, like mobile

---

16 Apple, *Apple's App Store Downloads Top Three Billion*, Jan. 5, 2010, **www.apple.com/pr/library/2010/01/05appstore.html**

17 Ann Bartow, *A Portrait of the Internet as a Young Man*, 108 MICHIGAN LAW REVIEW 6, at 1102-03, **www.michiganlawreview.org/assets/pdfs/108/6/bartow.pdf**

18 James Grimmelmann & Paul Ohm, *Dr. Generative or: How I Learned to Stop Worrying and Love the iPhone*, MARYLAND LAW REVIEW (2010) at 940-41.

19 *Id.* at 941.

20 *Id.* at 944. (emphasis in original).

> apps or TV-specific interfaces, they will continue to access the Web too, enabling each platform to grow concurrently.[21]

Ironically, it was Chris Anderson, editor of *Wired* and author of the apocalyptic "Web is Dead" cover story, who best explained why fears of "The Great Closing" are largely overblown:

> Ecommerce continues to thrive on the Web, and no company is going to shut its Web site as an information resource. More important, the great virtue of today's Web is that so much of it is noncommercial. The wide-open Web of peer production, the so-called generative Web where everyone is free to create what they want, continues to thrive, driven by the nonmonetary incentives of expression, attention, reputation, and the like.[22]

And Jeff Bertolucci of *PC World* makes it clear generative computing is alive and well:

> The next big computing platform won't be a version of Apple's Mac OS, Google's Android, or Microsoft's Windows. It's already here—and it's the Web. And the drive to offer the most compelling window to the Web possible, via the browser, is intense. The browser is spreading beyond the PC and smartphone to new types of gadgetry, including TV set-top boxes and printers. This is a trend that will accelerate in the coming years.[23]

## The Evils of Closed Systems or Digital "Appliances" Are Greatly Over-Stated

Openness Evangelicals often fail to appreciate how there obviously must have been a need / demand for some "closed" or "sterile" devices or else the market wouldn't have supplied them. Why *shouldn't* people who want a simpler or more secure digital experience be offered such options? Wu worries that devices like the iPad "are computers that have been reduced to a strictly limited set of functions that they are designed to perform extremely well."[24] Needless to say,

---

21 Nick Bilton, *Is the Web Dying? It Doesn't Look That Way*, NEW YORK TIMES BITS BLOG, Aug. 17, 2010, **http://bits.blogs.nytimes.com/2010/08/17/the-growth-of-the-dying-web**

22 Anderson & Wolff, *supra* note 2.

23 Jeff Bertolucci, *Your Browser in Five Years,* PC WORLD, June 16, 2010, **www.pcworld.com/article/199071/your_browser_in_five_years.html**

24 Wu, *supra* note 5 at 292.

it will be hard for many consumers to sympathize with Wu's complaint that products work too well!

However, as noted throughout this essay, it's also not quite true that those devices are as closed or crippled as their critics suggest. As Grimmelmann and Ohm aptly note, "restricting generativity in one place (for example, by building computers with fixed circuit boards rather than a tangle of reconfigurable wires) can massively enhance generativity overall (by making computers cheap and usable enough that everyone can tinker with their software)."[25] For example, in November 2010, Damon Albarn, lead singer of the popular band "Gorillaz," announced that the group's next album would be recorded entirely on an iPad.[26]

Regardless, just how far would these critics go to keep devices or platform perfectly "generative" or "open" (assuming we can even agree on how to define these concepts)? Do the Openness Evangelicals really think consumers would be better served if they were forced to fend for themselves with devices that arrived totally unconfigured? Should the iPhone or iPad, for example, be shipped to market with no apps loaded on the main screen, forcing everyone to go find them on their own? Should TiVos have no interactive menus out-of-the-box, forcing consumers to go online and find some "homebrew" code that someone whipped up to give users an open source programming guide?

Some of us are able to do so, of course, and those of us who are tech geeks sometimes find it easy to look down our noses at those who want their hand held through cyberspace, or who favor more simplistic devices. But there's nothing wrong with those individuals who seek simplicity, stability, or security in their digital devices and online experiences—even if they find those solutions in the form of "tethered appliances" or "walled gardens." Not everyone wants to tinker or to experience cyberspace as geeks do. Not everyone wants to program their mobile phones, hack their consoles, or write their own code. Most people live perfectly happy lives without ever doing any of these things! Nonetheless, many of those "mere mortals" *will* want to use many of the same toys that the tech geeks use, or they may just want to take more cautious steps into the occasionally cold pool called cyberspace—one tippy toe at a time. Why shouldn't those users be accommodated with "lesser" devices or a "curated" Web experience? Kevin Kelly argues that there's another way of looking at these trends. Digital tools are becoming more specialized, he argues, and "with the advent of rapid fabrication … specialization will leap ahead so that any tool can be customized to an individual's personal needs or desires."[27] Viewed in

---

25 Grimmelmann & Ohm, *supra* note 18, at 923.

26 *Damon Albarn Records New Gorillaz Album on an iPad*, NME NEWS, November 12, 2010, **http://www.nme.com/news/gorillaz/53816**

27 Kevin Kelly, *What Technology Wants* (2010) at 295-6.

this light, the Openness Evangelicals would hold back greater technological specialization in the name of preserving market norms or structures they prefer.

The best argument against digital appliancization is that the desire for more stable and secure systems will lead to a more "regulable" world—*i.e.*, one that can be more easily controlled by both corporations and government. As Zittrain puts it:

> Whether software developer or user, volunteering control over one's digital environment to a Manager means that the manager can change one's experience at any time—or worse, be compelled to by outside pressures. … The famously ungovernable Internet suddenly becomes much more governable, an outcome most libertarian types would be concerned about.[28]

No doubt, concerns about privacy, child safety, defamation, cybersecurity, identity theft and so on, will continue to lead to calls for more intervention. At the corporate level, however, some of that potential intervention makes a great deal of sense. For example, if ISPs are in a position to help do something to help alleviate some of these problems—especially spam and viruses—what's wrong with that? Again, there's a happy balance here that critics like Zittrain and Wu fail to appreciate. Bruce Owen, an economist and the author of *The Internet Challenge to Television*, discussed it in his response to Zittrain's recent book:

> Why does Zittrain think that overreaction is likely, and that its costs will be unusually large? Neither prediction is self-evident. Faced with the risk of infection or mishap, many users already restrain their own taste for PC-mediated adventure, or install protective software with similar effect. For the most risk-averse PC users, it may be reasonable to welcome "tethered" PCs whose suppliers compete to offer the most popular combinations of freedom and safety. Such risk-averse users are reacting, in part, to negative externalities from the poor hygiene of other users, but such users in turn create positive externalities by limiting the population of PCs vulnerable to contagion or hijacking. As far as one can tell, this can as easily produce balance or under-reaction as overreaction—it is an empirical question. But, as long as flexibility has value to users,

---

[28] Jonathan Zittrain, *Has the Future of the Internet Happened*? Sept. 7, 2010, CONCURRING OPINIONS blog, **www.concurringopinions.com/archives/2010/09/has-the-future-of-the-internet-come-about.html**

> suppliers of hardware and interconnection services will have incentives to offer it, in measured ways, or as options.[29]

Indeed, we can find happy middle-ground solutions that balance openness and stability—and platform operators must be free to discover where that happy medium is through an ongoing process of trial and error, for only through such discovery can the right balance be struck in a constantly changing landscape. A world full of hybrid solutions would offer more consumers more choices that better fit their specific needs.

Finally, to the extent something more must be done to counter the supposed regulability of cyberspace, the solution should not be new limitations on innovation. Instead of imposing restrictions on code or coders to limit regulability, we should instead place more constraints on our government(s). Consider privacy and data collection concerns. While, as a general principle, it is probably wise for companies to minimize the amount of data they collect about consumers to avoid privacy concerns about data breaches, there are also benefits to the collection of that data. So rather than legislating the "right" data retention rules, we should hold companies to the promises they make about data security and breaches, and tightly limit the powers of government to access private information through intermediaries in the first place.

Most obviously, we could begin by tightening up the Electronic Communications Privacy Act (ECPA) and other laws that limit government data access.[30] More subtly, we must continue to defend Section 230 of the Communications Decency Act, which shields intermediaries from liability for information posted or published by users of their systems, because (among many things) such liability would make online intermediaries more susceptible to the kind of back-room coercion that concerns Zittrain, Lessig and others. If we're going to be legislating the Internet, we need more laws like that, not those of the "middleman deputization" model or those that would regulate code to achieve this goal.

## Companies Have Strong Incentives to Strike the Right Openness/Closedness Balance

Various social and economic influences help ensure the scales won't be tipped completely in the closed or non-generative direction. The Web is built on

---

29 Bruce Owen, *As Long as Flexibility Has Value to Users, Suppliers Will Have Incentives to Offer It*, BOSTON REVIEW, March/April 2008, **www.bostonreview.net/BR33.2/owen.php**

30 A broad coalition has proposed such reforms. See **www.digitaldueprocess.org**.

powerful feedback mechanisms and possesses an extraordinary level of transparency in terms of its operations.

Moreover, the breaking news cycle for tech developments can be measured not in days, but in minutes or even seconds. Every boneheaded move meets immediate and intense scrutiny by bloggers, tech press, pundits, gadget sites, *etc.* Never has the white-hot spotlight of public attention been so intense in helping to shine a light on corporate missteps and forcing their correction. We saw this dynamic at work with the Facebook Beacon incident,[31] Google' Buzz debacle,[32] Amazon *1984* incident,[33] Apple's Flash restrictions,[34] the Sony rootkit episode,[35] and other examples.

## Things Are Getting More Open All the Time Anyway

Most corporate attempts to bottle up information or close off their platforms end badly. The walled gardens of the past failed miserably. In critiquing Zittrain's book, Ann Bartow has noted that "if Zittrain is correct that CompuServe and America Online (AOL) exemplify the evils of tethering, it's pretty clear the market punished those entities pretty harshly without Internet governance-style interventions."[36] Indeed, let's not forget that AOL was the big, bad corporate boogeyman of Lessig's *Code* and yet, just a decade later, it has been relegated to an also-ran in the Internet ecosystem.

---

31 *See* Nancy Gohring, *Facebook Faces Class-Action Suit Over Beacon*, NETWORKWORLD.COM, Aug. 13, 2008, **http://www.networkworld.com/news/2008/081308-facebook-faces-class-action-suit-over.html**.

32 *See* Ryan Paul, *EPIC Fail: Google Faces FTC Complaint Over Buzz Privacy*, ARS TECHNICA, Feb. 17, 2010, **http://arstechnica.com/security/news/2010/02/epic-fail-google-faces-complaint-over-buzz-privacy-issues.ars**.

33 *See* John Timmer, *Amazon Settles 1984 Suit, Sets Limits on Kindle Deletions*, ARS TECHNICA, Oct. 2, 2009, **http://arstechnica.com/web/news/2009/10/amazon-stipulates-terms-of-book-deletion-via-1984-settlement.ars**.

34 *See* Rob Pegoraro, *Apple Ipad's Rejection of Adobe Flash Could Signal the Player's Death Knell*, THE WASHINGTON POST, Feb. 7, 2010, **http://www.washingtonpost.com/wp-dyn/content/article/2010/02/05/AR2010020501089.html**.

35 *See* Wikipedia, *Sony BMG CD Copy Protection Scandal,* **http://en.wikipedia.org/wiki/Sony_BMG_CD_copy_protection_scandal** (last accessed Dec. 9, 2010).

36 Bartow, *supra* note 17 at 1088, **www.michiganlawreview.org/assets/pdfs/108/6/bartow.pdf**

**The America Online Case Study:**
**Remembering Yesterday's Face of "Closed" Evil**

When it comes to "closed" systems, evil has a face, but it seems the face is always changing. When Lessig penned *Code* a decade ago, it was American Online (AOL) that was set to become the corporate enslaver of cyberspace. For a time, it was easy to see why Lessig and others might have been worried. Twenty five million subscribers were willing to pay $20 per month to get a guided tour of AOL's walled garden version of the Internet. Then AOL and Time Warner announced a historic mega-merger that had some predicting the rise of "new totalitarianisms"[37] and corporate "Big Brother."[38]

But the deal quickly went off the rails.[39] By April 2002, just two years after the deal was struck, AOL-Time Warner had already reported a staggering $54 billion loss.[40] By January 2003, losses had grown to $99 billion.[41] By September 2003, Time Warner decided to drop AOL from its name altogether and the deal continued to slowly unravel from there.[42] In a 2006 interview with the *Wall Street Journal*, Time Warner President Jeffrey Bewkes famously declared the death of "synergy" and went so far as to call synergy "bullsh*t"![43] In early 2008, Time Warner decided to shed AOL's dial-up service[44] and in 2009 spun off AOL entirely.[45] Further deconsolidation followed for Time Warner, which

---

37 Norman Soloman, *AOL Time Warner: Calling The Faithful To Their Knees*, Jan. 2000, **www.fair.org/media-beat/000113.html**

38 Robert Scheer, *Confessions of an E-Columnist*, Jan. 14, 2000, ONLINE JOURNALISM REVIEW, **www.ojr.org/ojr/workplace/1017966109.php**

39 Adam Thierer, *A Brief History of Media Merger Hysteria: From AOL-Time Warner to Comcast-NBC*, Progress & Freedom Foundation, PROGRESS ON POINT 16.25, Dec. 2, 2009, **www.pff.org/issues-pubs/pops/2009/pop16.25-comcast-NBC-merger-madness.pdf**

40 Frank Pellegrini, *What AOL Time Warner's $54 Billion Loss Means*, April 25, 2002, TIME ONLINE, **www.time.com/time/business/article/0,8599,233436,00.html**

41 Jim Hu, *AOL Loses Ted Turner and $99 billion,* CNET NEWS.COM, Jan. 30, 2004, **http://news.cnet.com/AOL-loses-Ted-Turner-and-99-billion/2100-1023_3-982648.html**

42 *Id.*

43 Matthew Karnitschnig, *After Years of Pushing Synergy, Time Warner Inc. Says Enough*, WALL STREET JOURNAL, June 2, 2006, **http://online.wsj.com/article/SB114921801650969574.html**

44 Geraldine Fabrikant, Time Warner Plans to Split Off AOL's Dial-Up Service, NEW YORK TIMES, Feb. 7, 2008, **www.nytimes.com/2008/02/07/business/07warner.html?_r=1&adxnnl=1&oref=slogin&adxnnlx=1209654030-ZpEGB/n3jS5TGHX63DONHg**

45 Press Release, Time Warner, Time Warner Inc. Completes Spin-off of AOL Inc. (Dec. 10, 2009), **http://www.timewarner.com/corp/newsroom/pr/0,20812,1946835,00.html**.

spun off its cable TV unit and various other properties. Looking back at the deal, Fortune magazine senior editor at large Allan Sloan called it the "turkey of the decade."[46]

In the larger scheme of things, AOL's story has already become an afterthought in our chaotic cyber-history. But we shouldn't let those old critics forget about their lugubrious lamentations. To recap: the big, bad corporate villain of Lessig's *Code* attempted to construct the largest walled garden ever, and partner with a titan of the media sector in doing so—*and this dastardly plot failed miserably.*

The hysteria about AOL's looming monopolization of instant messaging—and with it, the rest of the Web—seems particularly silly: Today, anyone can download a free chat client like Digsby or Adium to manage multiple IM services from AOL, Yahoo!, Google, Facebook and just about anyone else, all within a single interface, essentially making it irrelevant which chat service your friends use.

From this case study one would think the Openness Evangelicals would have gained a newfound appreciation for the evolutionary and dynamic nature of digital markets and come to understand that, in markets built upon code, the pace and nature of change is unrelenting and utterly unpredictable. Indeed, *contra* Lessig's lament in *Code* that "Left to itself, cyberspace will become a perfect tool of control," cyberspace has proven far more difficult to "control" or regulate than any of us ever imagined. The volume and pace of technological innovation we have witnessed over the past decade has been nothing short of stunning.

Critics like Zittrain and Wu, however, wants to keep beating the cyber-sourpuss drum. So, the face of corporate evil had to change. Today, Steve Jobs has become the supposed apotheosis of all this closed-system evil instead of AOL. Jobs serves as a prime villain in the books of Zittrain and Wu and in many of the essays they and other Openness Evangelicals pen. It's worth noting, however, that their enemies list is growing longer and now reads like a "Who's Who" of high-tech corporate America. According to Zittrain and Wu's books, 'we need to worry about just about every major player in the high-tech ecosystem—telcos, cable companies, wireless operators, entertainment providers, Facebook, and others.

Even Google—Silicon Valley's supposed savior of Internet openness—is not spared their scorn. "Google is the Internet's switch," Wu argues. "In fact, it's

---

46 Allan Sloan, *'Cash for…' and the Year's Other Clunkers*, WASHINGTON POST, Nov. 17, 2009, **www.washingtonpost.com/wp-dyn/content/article/2009/11/16/AR2009111603775.html**

the world's most popular Internet switch, and as such, it might even be described as the current custodian of the Master Switch." More ominously, he warns, "it is the switch that transforms mere communications into networking—that ultimately decides who reaches what or whom."[47]

It seems, then, that the face of "closed" evil is constantly morphing. Shouldn't that tell us something about how dynamic these markets are?

There are few reasons to believe that today's efforts to build such walled gardens would end much differently. Indeed, increasingly when companies or coders erect walls of any sort, holes form quickly. For example, it usually doesn't take long for a determined group of hackers to find ways around copy/security protections and "root" or "jailbreak" phones and other devices.[48] Once hacked, users are usually then able to configure their devices or applications however they wish, effectively thumbing their noses at the developers. This process tends to unfold in a matter of just days, even hours, after the release of a new device or operating system.

**Number of Days Before New Devices Were "Rooted" or "Jailbroken"**[49]

| | |
|---|---|
| original iPhone | 10 days |
| original iPod Touch | 35 days |
| iPhone 3G | 8 days |
| iPhone 3GS | 1 day |
| iPhone 4 | 38 days |
| iPad | 1 day |
| T-Mobile G1 (first Android phone) | 13 days |
| Palm Pre | 8 days |

Of course, not every user will make the effort—or take the risk[50]—to hack their devices in this fashion, even once instructions are widely available for doing so.

---

47 Wu, *supra* note 5 at 280.

48 "In living proof that as long as there's a thriving geek fan culture for a device, it will never be long for the new version to be jailbroken: behold iOS 4.1. Most people are perfectly willing to let their devices do the talking for them, accept what's given, and just run sanctioned software. But there are those intrepid few—who actually make up a fairly notable portion of the market—who want more out of their devices and find ways around the handicaps built into them by the manufacturers." Kit Dotson, *New iOS for Apple TV Firmware Released, Promptly Decrypted*, SiliconAngle, Sept. 28, 2010, **http://siliconangle.com/blog/2010/09/28/new-ios-for-apple-tv-firmware-released-promptly-decrypted**

49 Original research conducted by author and Adam Marcus based on news reports.

Nonetheless, even if copyright law might sometimes seek to restrict it, the hacking option still exists for those who wish to exercise it. Moreover, because many manufacturers know their devices are likely to be hacked, they are increasingly willing to make them more "open" right out of the gates or offer more functionality/flexibility to make users happy.

## Innovation Continues to Unfold Rapidly *in Both Directions* along the "Open" vs. "Closed" Continuum

As noted above, part of Zittrain and Wu's lament seems to be that the devices that the *hoi polloi* choose might crowd out those favored by tinker-happy tech geeks (of which I count myself a proud member). But we geeks need not fear such foreclosure. Just because there are some "closed" systems or devices on the market, it doesn't mean innovation has been foreclosed among more "open" systems or platforms. A hybrid future is both possible and desirable. Again, we can have the best of both worlds—a world full of plenty of closed systems or even "tethered appliances," but also plenty of generativity and openness. As Web 2.0 pioneer Tim O'Reilly notes:

> I'm not terribly taken in by the rhetoric that says that because content silos are going up, and we're seeing more paid content, the open web is over. Individuals, small companies, entrepreneurs, artists, all have enormous ability to share and distribute their work and find an audience. I don't see that becoming less in today's environment.[51]

Consider the battle between the Apple iPhone and Google Android mobile phone operating systems. Zittrain says Android is "a sort of canary in the coal mine"[52] for open platforms, but ignores the frantic pace of its growth, now accounting for one-quarter of mobile Web traffic just three years after its inception[53] and stealing away Apple's marketshare in the process.[54] Beyond

---

50 Rooting or jailbreaking a smartphone creates the risk of "bricking" the device—rendering it completely inoperable (and thus no more useful than a brick). Additionally, hacking devices in this fashion typically voids any manufacturer warranty.

51 *The Web is Dead? A Debate*, WIRED, Aug. 17, 2010, **www.wired.com/magazine/2010/08/ff_webrip_debate/all/1**

52 Jonathan Zittrain, *Has the Future of the Internet Happened?* Sept. 7, 2010, CONCURRING OPINIONS blog, **www.concurringopinions.com/archives/2010/09/has-the-future-of-the-internet-come-about.html**

53 Sean Hollister, *Android Accounts for One-Quarter of Mobile Web Traffic, Says Quantcast*, ENGADGET, Sept. 4, 2010, **www.engadget.com/2010/09/04/android-accounts-for-one-quarter-of-mobile-web-traffic-says-qua**; *Android Most Popular Operating System in U.S.*

downplaying Android's success as a marketplace triumph for openness (and proof of the non-governmental forces that work to force a balance between openness and closedness), Zittrain also reverts to the "kill switch" boogeyman: He warns us that any day now Google could change its mind, close the Android platform, and "kill an app, or the entire phone" remotely.[55] But where's the business sense in that? What's the incentive for Google to pursue such a course of action? Would Google be able to produce all those millions of apps currently produced by independent developers? That seems both unlikely and unpopular. Meanwhile, how many times has supposedly control-minded Apple actually thrown the dreaded "kill switch" on apps? There are tens of millions of apps in Apple's App Store and hundreds of billions of downloads. If Steve Jobs is supposed to be the great villain of independent innovation, he seems to be doing a pretty bad job at it! "The App Store is, by some estimates, now a multi-billion-dollar-a-year business," note Grimmelmann and Ohm.[56] "The iPhone is a hotbed of creative tinkering; people are doing amazing things with it."[57]

In fact, Wu admits Apple's App Store offers a "seemingly unlimited variety of functions" and that "Apple does allow outsiders to develop applications on its platform" since "the defeat of the Macintosh by Windows taught Jobs that a platform completely closed to outside developers is suicide."[58] That should be the end of the story. Yet Wu's fear of that big proverbial "kill switch" overrides all: Any day now, that switch will be thrown and Lessig's pessimistic predictions of "perfect control" will finally come to pass, he implies. As Wu says, "all innovation and functionality are ultimately subject to Apple's veto."[59] And consider the lament of Tom Conlon of *Popular Science*: "Once we replace the personal computer with a closed-platform device such as the iPad, we replace

---

*Among Recent Smartphone Buyers*, NIELSEN WIRE, Oct. 5, 2010, **http://blog.nielsen.com/nielsenwire/online_mobile/android-most-popular-operating-system-in-u-s-among-recent-smartphone-buyers**

54 Tricia Duryee, *Apple Continued To Lose U.S. Marketshare Despite Spike From iPhone 4 Sales*, MOCONEWS.NET, Sept. 15, 2010, **http://moconews.net/article/419-apple-continued-to-lose-u.s.-marketshare-despite-spike-from-iphone-4-sa**; Miguel Helft, The iPhone Has a Real Fight on Its Hands, NEW YORK TIMES BITS, Oct. 5, 2010, **http://bits.blogs.nytimes.com/2010/10/05/the-iphone-has-a-real-fight-on-its-hands/**

55 Jonathan Zittrain, *Has the Future of the Internet Happened?* Sept. 7, 2010, CONCURRING OPINIONS blog, **www.concurringopinions.com/archives/2010/09/has-the-future-of-the-internet-come-about.html**

56 Grimmelmann & Ohm, *supra* note 18 at 923.

57 *Id.*

58 Wu, *supra* note 5 at 292.

59 *Id.*

freedom, choice, and the free market with oppression, censorship, and monopoly."[60] But Apple is hardly the only game in town, and each time Apple creates a new product category (iPod, iPhone, iPad, *etc.*), other companies are quick to follow with their own, usually more open systems, often running Google's Android operating system.

Neither Wu nor Zittrain, however, spend much time investigating how often their proverbial kill switch is actually thrown—by Apple or anyone else. There have been a handful of examples, but those are hardly the rule. The *vast* majority of all applications are immediately accepted and offered on the platform. Moreover, if they *were* blocked, they could quickly be found on other platforms. Again, there are plenty of alternatives to Apple products if you don't like their (somewhat) more restrictive policies regarding application development.

Bottom line: Today's supposed "walled gardens" are less "walled" than ever before, and "closed" systems aren't really so closed.

## The Internet Was Never Quite So Open or Generative

At times, Zittrain and others seem to have created an Internet imago; an idealized conception of a supposed better time when cyberspace was more open and vibrant. But let's face it, the "good ol' days" that many Openness Evangelicals seem to be longing for weren't really so glorious. Were you online back in 1994? Did you enjoy Trumpet Winsock and noisy 14.4 baud modems? Did you like loading up multiple 5¼-inch floppy disks just to boot your machine? Needless to say, most of us don't miss those days.

Here's the other forgotten factor about the Net's early history: Until the Net was commercialized, it was an extremely closed system. As Geert Lovink reminds us:

> [In] [t]he first decades[,] the Internet was a closed world, only accessible to (Western) academics and the U.S. military. In order to access the Internet one had to be an academic computer scientist or a physicist. Until the early nineties it was not possible for ordinary citizens, artists, business[es] or activists, in the USA or elsewhere, to obtain an email address

---

60 Tom Conlon, *The iPad's Closed System: Sometimes I Hate Being Right*, POPULAR SCIENCE, Jan. 29, 2010, **www.popsci.com/gadgets/article/2010-01/ipad%E2%80%99s-closed-system-sometimes-i-hate-being-right**

> and make use of the rudimentary UNIX-based applications. …
> It was a network of networks—but still a closed one.[61]

Ironically, it was only because Lessig and Zittrain's much-dreaded AOL and CompuServe came along that many folks were even able to experience and enjoy this strange new world called the Internet. "The fact that millions of Americans for the first time experienced the Internet through services like AOL (and continue to do so) is a reality that Zittrain simply overlooks," notes Lovink.[62] Could it be that those glorious "good ol' days" Zittrain longs for were really due to the way closed "walled gardens" like AOL and CompuServe held our hands to some extent and gave many new Netizens a guided tour of cyberspace?

Regardless, we need not revisit or reconsider that history. That's ancient history now because the walls around those gardens came crumbling down.

## Summary

When you peel away all the techno-talk and hand-wringing, what Zittrain and other Openness Evangelicals object to is the fact that some people are making choices that they don't approve of. To be generous, perhaps it's because they believe that the "mere mortals" don't fully understand the supposed dangers of the choices they are making. But my contention here has been that things just aren't as bad as they make them out to be. More pointedly, who are these critics to say those choices are irrational?

Again, so what if some mere mortals choose more "closed" devices or platforms because they require less tinkering and "just work?" It isn't the end of the world. Those devices or platforms aren't really as closed as they suggests—in fact, they are far more open in some ways that the earlier technologies and platforms Zittrain, *et.al.* glorify. And it simply doesn't follow that just because *some* consumers choose to use "appliances" that it's the end of the generative devices that others so cherish. "General-purpose computers are so useful that we're not likely to abandon them," notes Princeton University computer science professor Ed Felten.[63] For example, a October 2010 NPD Group survey

---

61 Geert Lovink, *Zittrain's Foundational Myth of the Open Internet*, NET CRITIQUE BY GEERT LOVINK, Oct. 12, 2008, **http://networkcultures.org/wpmu/geert/2008/10/12/zittrains-foundational-myth-of-the-open-internet/**

62 *Id.*

63 Ed Felten, *iPad to Test Zittrain's "Future of the Internet" Thesis*, FREEDOM TO TINKER blog, Feb. 4, 2010, **www.freedom-to-tinker.com/blog/felten/ipad-test-zittrains-future-internet-thesis**

revealed that "contrary to popular belief, the iPad isn't causing cannibalization in the PC market because iPad owners don't exhibit the same buying and ownership patterns as the typical consumer electronics customer."[64] According to NPD, only 13% of iPad owners surveyed bought an iPad instead of a PC, while 24% replaced a planned e-reader purchase with an iPad. Thus, to the extent the iPad was replacing anything, it would be other "non-generative" devices like e-readers.

In a similar vein, James Watters, Senior Manager of Cloud Solutions Development at VMware, argues:

> Innovation will be alive and well because the fundamental technologies at the core of cloud computing are designed for massive, vibrant, explosive, awesome, and amazing application innovation. There will always be a big place in the market for companies who achieve design simplicity by limiting what can be done on their platforms—Apple and Facebook may march to massive market share by this principle—but as long as the technologies underpinning the network are open, programmable, extensible, modular, and dynamic as they are and will be, innovation is in good hands.[65]

Thus, we *can* have the best of both worlds—a world full of plenty of "tethered" appliances, but also plenty of generativity and openness. We need not make a choice between the two, and we certainly shouldn't be demanding someone else make it for us.

## Against the Stasis Mentality & Static Snapshots

There are some important practical questions that the Openness Evangelicals often fail to acknowledge in their work. Beyond the thorny question of how to define "openness" and "generativity," what metric should be used when existing yardsticks become obsolete so regularly?

This points to two major failings in the work of all the cyber-collectivists—Lessig in *Code*, Zittrain in *Future of the Internet*, and Wu in *The Master Switch*:

---

64 *Nearly 90 Percent of Initial iPad Sales are Incremental and not Cannibalizing the PC Market, According to NPD,* NPD Group PRESS RELEASE, October 1, 2010, **www.npd.com/press/releases/press_101001.html**

65 James Watters, *NYT Kicks Off Cloud Paranoia Series*, SILICONANGLE blog, July 21, 2009, **http://siliconangle.com/blog/2009/07/21/nyt-kicks-off-cloud-paranoia-editorial-series**

1. They have a tendency to adopt a static, snapshot view of markets and innovation; and,

2. They often express an overly nostalgic view of the past (without making it clear when the "good 'old days" began and ended) while adopting an excessively pessimist view of the present and the chances for progress in the future.

This is what Virginia Postrel was referring to in *The Future and Its Enemies* when she criticized the stasis mentality because "It overvalues the tastes of an articulate elite, compares the real world of trade-offs to fantasies of utopia, omits important details and connections, and confuses temporary growing pains with permanent catastrophes."[66] And it is what economist Israel Kirzner was speaking of when warned of "the shortsightedness of those who, not recognizing the open-ended character of entrepreneurial discovery, repeatedly fall into the trap of forecasting the future against the background of *today's* expectations rather than against the unknowable background of tomorrow's discoveries."[67]

Indeed, there seems to be a complete lack of appreciation among the Openness Evangelicals for just how rapid and unpredictable the pace of change in the digital realm has been and will likely continue to be. The relentlessness and intensity of technological disruption in the digital economy is truly unprecedented but often under-appreciated. We've had multiple mini-industrial revolutions within the digital ecosystem over the past 15 years. Again, this is "evolutionary dynamism" at work. (Actually, it's more like *revolutionary* dynamism!) Nothing—*absolutely nothing*—that was sitting on our desks in 1995 is still there today (in terms of digital hardware and software). It's unlikely that much of what was on our desk in *2005* is still there either—with the possible exception of some crusty desktop computers running Windows XP. Thus, at a minimum, analysts of innovation in this space "should … extend the time horizon for our assessment of the generative ecosystem"[68] to ensure they are not guilty of the static snapshot problem.

Speaking of Windows, it perfectly illustrates the complexity of defining generative systems. Compare the half-life of Windows PC operating systems—which Zittrain indirectly glorifies in his book as generativity nirvana—to the half-life of Android operating systems. Both Apple and Android-based devices

---

66 VIRGINIA POSTREL, THE FUTURE AND ITS ENEMIES (1998), at xvii-xviii.

67 ISRAEL KIRZNER, DISCOVERY AND THE CAPITALIST PROCESS (University of Chicago Press, 1985), at xi.

68 Grimmelmann & Ohm, *supra* note 18 at 947.

have seen multiple OS upgrades since release. Some application developers actually complain about this frantic pace of mobile OS "revolutions," especially with the Android OS, since they must deal with multiple devices and OS versions instead of just one Apple iPhone. They'd rather see more OS consistency among the Android devices for which they're developing to facilitate quicker and more stable rollouts. They also have to consider whether and how to develop the same app for several other competing platforms.

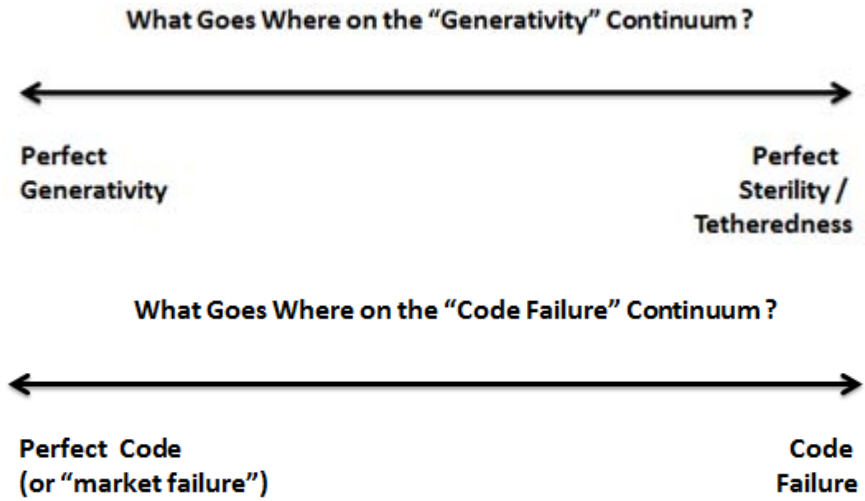
Meanwhile, Windows has offered a more "stable" developing platform for developers because Microsoft rolls out OS upgrades at a much slower pace. Should we should consider an OS with a slower upgrade trajectory more "generative" than an OS that experiences constant upgrades if, in practice, the former allows for more "open" (and potentially rapid) independent innovation by third parties? Of course, there other factors that play into the "generativity" equation,[69] but it would be no small irony to place the Windows PC model on the higher pedestal of generativity than the more rapidly-evolving mobile OS ecosystem.

## Conclusion: Toward Evolutionary Dynamism & Technological Agnosticism

Whether we are debating where various devices sit on a generativity continuum (of "open" versus "closed" systems), or what fits where on a "code failure" continuum (of "perfect code" versus "market failure"), the key point is that *the continuum itself is constantly evolving* and that this evolution is taking place at a much faster clip in this arena than it does in other markets. Coders don't sit still. People innovate around "failure." Indeed, "market failure" is really just the glass-is-half-empty view of a golden opportunity for innovation. Markets evolve. New ideas, innovations, and companies are born. Things generally change for the better—and do so rapidly.

---

[69] "[G]enerativity is essential but can never be absolute. No technological system is perfectly generative at all levels, for all users, forever. Tradeoffs are inevitable." Grimmelmann and Ohm, *supra* note 18 at 923.




In light of the radical revolutions constantly unfolding in this space and upending existing models, it's vitally important we avoid "defining down" market failure. This is not based on a blind faith in free markets, but rather a profound appreciation for the fact that *in markets built upon code, the pace and nature of change is unrelenting and utterly unpredictable*. *Contra* Lessig's lament in *Code* that "Left to itself, cyberspace will become a perfect tool of control"—cyberspace has proven far more difficult to "control" or regulate than any of us ever imagined. Again, the volume and pace of technological innovation we have witnessed over the past decade has been nothing short of stunning.

We need to give evolutionary dynamism a chance. Sometimes it's during what appears to be a given sector's darkest hour that the most exciting things are happening within it—as the AOL case study illustrates. It's easy to forget all the anxiety surrounding AOL and its "market power" circa 1999-2002, when scholars like Lessig predicted that the company's walled garden approach would eventually spread and become the norm for cyberspace. As made clear in the breakout above, however, the exact opposite proved to be the case. The critics said the sky would fall, but it most certainly did not.

Similarly, in the late 1990s, many critics—including governments both here and in the EU—claimed that Microsoft dominated the browser market. Dour predictions of perpetual Internet Explorer lock-in followed. For a short time, there was some truth to this. But innovators weren't just sitting still; exciting things were happening. In particular, the seeds were being planted for the rise of Firefox and Chrome as robust challengers to IE's dominance—not to mention mobile browsers. Of course, it's true that roughly half of all websurfers

still use a version of IE today. But IE's share of the market is falling rapidly[70] as viable, impressive alternatives now exist and innovation among these competitors is more vibrant than ever.[71] That's all that counts. The world changed, and for the better, despite all the doomsday predictions we heard less than a decade ago about Microsoft's potential dominance of cyberspace. Moreover, all the innovation taking place at the browser layer today certainly undercuts the gloomy "death of the Net" thesis set forth by Zittrain and others. Thus, as O'Reilly argues, this case study again shows us the power of open systems and evolutionary dynamism:

> Just as Microsoft appeared to have everything locked down in the PC industry, the open Internet restarted the game, away from what everyone thought was the main action. I guarantee that if anyone gets a lock on the mobile Internet, the same thing will happen. We'll be surprised by the innovation that starts happening somewhere else, out on the free edges. And that free edge will eventually become the new center, because open is where innovation happens. […] it's far too early to call the open web dead, just because some big media companies are excited about the app ecosystem. I predict that those same big media companies are going to get their clocks cleaned by small innovators, just as they did on the web.[72]

In sum, history counsels patience and humility in the face of radical uncertainty and unprecedented change. More generally, it counsels what we might call "technological agnosticism." We should avoid declaring "openness" a sacrosanct principle and making everything else subservient to it without regard to cost or consumer desires. As Anderson notes, "there are many Web triumphalists who still believe that there is only One True Way, and will fight to the death to preserve the open, searchable common platform that the Web represented for most of its first two decades (before Apple and Facebook, to name two, decided that there were Other Ways)."[73] The better position is one based on a general agnosticism regarding the nature of technological platforms and change. In this view, the spontaneous evolution of markets has value in its

---

70 Tim Stevens, *Internet Explorer Falls Below 50 Percent Global Marketshare, Chrome Usage Triples*, ENGADGET, Oct. 5, 2010, **www.engadget.com/2010/10/05/internet-explorer-falls-below-50-percent-global-marketshare-chr**

71 Nick Wingfield & Don Clark, *Browsers Get a Face-Lift*, WALL STREET JOURNAL, Sept. 15, 2010, **http://online.wsj.com/article/SB10001424052748704285104575492102514582856.html**

72 *The Web is Dead? A Debate*, WIRED, Aug. 17, 2010, **www.wired.com/magazine/2010/08/ff_webrip_debate/all/1**

73 *Id.*

own right, and continued experimentation with new models—be they "open" or "closed," "generative" or "tethered"—should be permitted.

Importantly, one need not believe that the markets in code are "perfectly competitive" to accept that they are "competitive *enough*" compared to the alternatives—especially those re-shaped by regulation. "Code failures" are ultimately better addressed by voluntary, spontaneous, bottom-up, marketplace responses than by coerced, top-down, governmental solutions. Moreover, the decisive advantage of the market-driven, evolutionary approach to correcting code failure comes down to the rapidity and nimbleness of those responses.

Let's give those other forces—alternative platforms, new innovators, social norms, public pressure, *etc.*—a chance to work some magic. Evolution happens, if you let it.

# CHAPTER 3

## IS INTERNET EXCEPTIONALISM DEAD?

# The Third Wave of Internet Exceptionalism

By Eric Goldman*

From the beginning, the Internet has been viewed as something special and "unique." For example, in 1996, a judge called the Internet "a unique and wholly new medium of worldwide human communication."[1]

The Internet's perceived novelty has prompted regulators to engage in "Internet exceptionalism": crafting Internet-specific laws that diverge from regulatory precedents in other media. Internet exceptionalism has come in three distinct waves:

## The First Wave: Internet Utopianism

In the mid-1990s, some people fantasized about an Internet "utopia" that would overcome the problems inherent in other media. Some regulators, fearing disruption of this possible utopia, sought to treat the Internet more favorably than other media.

47 U.S.C. § 230 ("Section 230"—a law still on the books) is a flagship example of mid-1990s efforts to preserve Internet utopianism. The statute categorically immunizes online providers from liability for publishing most types of third party content. It was enacted (in part) "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[2] The statute is clearly exceptionalist because it treats online providers more favorably than offline publishers—even when they publish identical content.

## The Second Wave: Internet Paranoia

Later in the 1990s, the regulatory pendulum swung in the other direction. Regulators still embraced Internet exceptionalism, but instead of favoring the Internet, regulators treated the Internet more harshly than analogous offline activity.

For example, in 2005, a Texas website called Live-shot.com announced that it would offer "Internet hunting." The website allowed paying customers to

* Associate Professor and Director, High Tech Law Institute, Santa Clara University School of Law. Email: **egoldman@gmail.com**. Website: **http://www.ericgoldman.org**.

1 American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996).

2 47 U.S.C. § 230(b)(2).

control, via the Internet, a gun on its game farm. An employee manually monitored the gun and could override the customer's instructions. The website wanted to give people who could not otherwise hunt, such as paraplegics, the opportunity to enjoy the hunting experience.[3]

The regulatory reaction to Internet hunting was swift and severe. Over three-dozen states banned Internet hunting.[4] California also banned Internet fishing for good measure.[5] However, regulators never explained how Internet hunting is more objectionable than physical space hunting.

For example, California Sen. Debra Bowen criticized Internet hunting because it "isn't hunting; it's an inhumane, over the top, pay-per-view video game using live animals for target practice … . Shooting live animals over the Internet takes absolutely zero hunting skills, and it ought to be offensive to every legitimate hunter."[6]

Sen. Bowen's remarks reflect numerous unexpressed assumptions about the nature of "hunting" and what constitutes fair play. In the end, however, hunting may just be "hunting," in which case the response to Internet hunting may just be a typical example of adverse Internet exceptionalism.[7]

## The Third Wave: Exceptionalism Proliferation

The past few years have brought a new regulatory trend. Regulators are still engaged in Internet exceptionalism, but each new advance in Internet technology has prompted exceptionalist regulations towards that technology.

For example, the emergence of blogs and virtual worlds has helped initiate a push towards blog-specific and virtual world-specific regulation. In effect, Internet exceptionalism has splintered into pockets of smaller exceptionalist efforts.

---

3 Sylvia Moreno, *Mouse Click Brings Home Thrill of the Hunt*, WASH. POST, May 8, 2005.

4 *Internet Hunting Bans*, The Humane Society of the United States, **http://www.hsus.org/web-files/PDF/internethunting_map.pdf** (last visited Aug. 23, 2010).

5 Zachary M. Seward, *Internet Hunting Has Got to Stop – If It Ever Starts*, WALL ST. J., Aug. 10, 2007.

6 Michael Gardner, *Web 'Hunts' in Cross Hairs of Lawmakers*, S.D. UNION-TRIBUNE, Apr. 6, 2005.

7 Eric Goldman, *A Web Site for Hunting Poses Questions About Killing*, S.J. MERCURY NEWS, July 25, 2005.

Regulatory responses to social networking sites like Facebook and MySpace are a prime example of Internet exceptionalism splintering. Rather than regulating these sites like other websites, regulators have sought social networking site-specific laws, such as requirements to verify users' age,[8] combat sexual predators[9] and suppress content that promotes violence.[10] The result is that the regulation of social networking sites differs not only from offline enterprises but from other websites as well.

## Implications

Internet exceptionalism—either favoring or disfavoring the Internet—is not inherently bad. In some cases, the Internet truly is unique, special or different and should be regulated accordingly. Unfortunately, more typically, anti-Internet exceptionalism cannot be analytically justified and instead reflects regulatory panic.

In these cases, anti-Internet regulatory exceptionalism can be harmful, especially to Internet entrepreneurs and their investors. It can distort the marketplace between Web enterprises and their offline competition by hindering the Web business' ability to compete. In extreme cases, such as Internet hunting, unjustified regulatory intervention may put companies out of business.

Accordingly, before enacting any exceptionalist Internet regulation (and especially any anti-Internet regulation), regulators should articulate how the Internet is unique, special or different and explain why these differences justify exceptionalism. Unfortunately, emotional overreactions to perceived Internet threats or harms typically trump such a rational regulatory process. Knowing this tendency, perhaps we can better resist that temptation.

---

8 Nick Alexander, *Attorneys General Announce Agreement With MySpace Regarding Social Networking Safety*, NAA GAZETTE, Jan. 18, 2008, **http://www.naag.org/attorneys_general_announce_agreement_with_myspace_regarding_social_networking_safety.php**; Brad Stone, *Facebook Settles with New York*, N.Y. TIMES BITS BLOG, Oct. 16 2007, **http://bits.blogs.nytimes.com/2007/10/16/facebook-settles-with-new-york/**.

9 KIDS Act of 2007 (H.R. 719/S. 431) (requiring sexual predators to register their email addresses and other screen names and enabling social networking sites to access those electronic identifiers so that the sexual predators can be blocked from registering with the social networking sites).

10 H. Res. 224 (2007) (resolution requesting that social networking sites proactively remove "enemy propaganda from their sites," such as videos made by terrorists).

# A Declaration of the Dependence of Cyberspace

By Hon. Alex Kozinski* & Josh Goldfoot**

> *Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.*[1]

That was the opening of "A Declaration of the Independence of Cyberspace." The would-be Cyber-Jefferson who wrote it was John Perry Barlow, a co-founder of the Electronic Frontier Foundation, a noted libertarian and a Grateful Dead lyricist. He delivered the Declaration on February 8, 1996, the same day that President Clinton signed into law the Communications Decency Act. That Act was chiefly an early effort to regulate Internet pornography. Many had concerns about that law, and, indeed, the Supreme Court would eventually declare most of it unconstitutional.[2]

Barlow's argument invoked what he believed was a more decisive criticism than anything the Supreme Court could come up with. Barlow saw the Internet as literally untouchable by our laws. Extolling the power of anonymity, he taunted that "our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion." Unlike the Declaration of Independence, this was not a declaration that cyberspace was newly independent; it was an observation that cyberspace had always been independent, and will always remain independent, because its denizens were beyond the law's reach.

Needless to say, the weary giants of flesh and steel did not take kindly to the Declaration. They fought back hard and won numerous battles: witness the fall of Napster, Grokster, Aimster and innumerable other file-sharing and child-pornography-trading sites and services. Ironically, the Department of

---

* Chief Judge, United States Court of Appeals for the Ninth Circuit.

** B.A., Yale University; J.D., University of Virginia School of Law; Trial Attorney, Department of Justice, Criminal Division, Computer Crime & Intellectual Property Section. This essay was originally published in 32 COLUMBIA JOURNAL OF LAW & THE ARTS, no. 4, 2009 at 365. The views expressed in this essay are the views of the authors and do not necessarily represent the views of the U.S. Department of Justice or the United States.

1 John Perry Barlow, A Declaration of the Independence of Cyberspace (Feb. 8, 1996), **http://homes.eff.org/~barlow/Declaration-Final.html**.

2 Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

Homeland Security now has a "National Strategy to Secure Cyberspace."[3] Even the cyber-libertarians have shifted their focus: The Electronic Frontier Foundation, which Barlow co-founded, now accepts that there may be a place for so-called "network neutrality" regulation, even though it regulates how subscribers access the Internet and how content reaches them.[4]

In other ways, the Declaration has proved prescient. As far back as 1996, Barlow had identified that the Internet poses a significant problem for governments. Then, as now, people used the Internet to break the law. The Internet gives those people two powerful tools that help them escape the law's efforts to find and punish them. First, the Internet makes anonymity easy. Today any 11-year-old can obtain a free e-mail account, free website and free video hosting. The companies that provide these things ask for your name, but they make no effort to verify your answer; as a result, only Boy Scouts tell them the truth. You can be tracked through your Internet protocol (IP) address, but it is not too tough to use proxies or some neighbor's open Wi-Fi connection to get around that problem. Thus, if your online conduct ever hurts someone, it will be difficult for the victim to ever find out who you are and sue you.

Second, the Internet makes long-distance international communication cheap. This allows the world's miscreants, con-artists and thieves easy access to our gullible citizens. When people find out they've been had, they often find that they have no practical recourse because of the extraordinary difficulties involved in pursuing someone overseas. The Internet's global nature makes it easy for people to hide from our courts.

These two advantages of Internet law-breakers pose a serious and recurring problem. That problem has been particularly painful for intellectual property rights holders. It is common knowledge that instead of buying music or movies, you can use the Internet to download perfect copies for free from individuals known only by their IP addresses. In some cases, wrongdoers have become so bold that they demand payment in exchange for the opportunity to download infringing material.

The situation seemed unsolvable to Barlow and others in 1996. Armed with anonymity and invulnerability, Internet actors could ignore efforts to apply law to the Internet. Barlow concluded that the Internet's nature posed an insurmountable barrier to any effort at legal enforcement. Some scholars even

---

3 The National Strategy to Secure Cyberspace, Feb. 2003, **http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf**.

4 *See* **https://www.eff.org/files/filenode/nn/EFFNNcomments.pdf**.

began work on theorizing how the diverse denizens of cyberspace might join together and go about creating their own indigenous legal system.[5]

But over time, a solution to Barlow's problem appeared. Let us entertain, for a moment, the conceit that there is a "cyberspace," populated by people who communicate online. The denizens of cyberspace exist simultaneously in cyberspace and in the real flesh-and-steel world. Their cyberspace selves can be completely anonymous; their real-life selves are easier to identify. Their cyberspace selves have no physical presence; their real-life selves both exist and have base material desires for PlayStations, Porsche Boxsters and *Battlestar Galactica* memorabilia. Their physical selves can be found in the real world and made to pay in real dollars or serve real time behind real bars for the damage their cyber-selves cause.

The dilemma that online law-breakers face is that their cyberspace crimes have real-life motives and fulfill real-life needs. Therefore, they need some way to translate their online misdeeds into offline benefits. The teenager downloads a MP3 so that he can listen to it. The con-artist asks for money to be wired to him so that he can withdraw it and buy things with it. The fringe activist who e-mails a death threat to a judge does so in the hopes that the judge will change his behavior in the real world.

These Internet actors usually rely on real-world institutions to get what they want. They use Internet Service Providers (ISPs) and hosting companies to communicate, and they use banks and credit card companies to turn online gains into cash. Without these institutions, they either could not accomplish their online harms, or they would not be able to benefit from them in the real world. Unlike anonymous cyberspace miscreants, however, these institutions have street addresses and real, physical assets that can satisfy judgments in the United States. By placing pressure on those institutions to cut off service to customers who break the law, we can indirectly place pressure on Internet wrong-doers. Through this pressure, we have a powerful tool to promote online compliance with the law.

In some cases, for some offenses, we have the legal tools to do this already. For intellectual property cases, the tool for holding those institutions liable is secondary liability: contributory and vicarious infringement. The Ninth Circuit has led the way in developing the law in this area. In *Perfect 10 v. Google*, the court noted the cases that had applied contributory infringement to Internet actors, and summarized their holdings as saying that "a computer system operator can be held contributorily liable if it has actual knowledge that specific infringing material is available using its system … and can take simple measures

---

5 *See, e.g.*, David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, JOURNAL OF ONLINE LAW, Article 3, (1995), *available at* **http://ssrn.com/abstract=943456**.

to prevent further damage to copyrighted works … yet continues to provide access to infringing works."[6] In other words, if people are using your stuff to infringe copyrights, and you know about it, and you can easily stop them, but you do not, then you are on the hook.

The motive behind secondary liability is simple. Everyone agrees that the direct infringers ideally should be the ones to pay. But there might be too many of them to sue; or, they might be anonymous; or, they might be in Nigeria. This can make them apparently invulnerable to lawsuits. That invulnerability has a cause: someone is providing the tools to infringe and looking the other way. The doctrine of secondary liability says that such behavior is unacceptable. Those who provide powerful tools that can be used for good or evil have some responsibility to make sure that those tools are used responsibly.

Put more directly: with some changes to the law, the institutions that enable the anonymity and invulnerability of cyberspace denizens can be held accountable for what their anonymous and invulnerable customers do. The anonymity of cyberspace is as much a creation of men as it is a creation of computers. It is the result of policy choices. We have accepted, without serious examination, that it is perfectly fine for a business to grant free Web space and e-mail to any schmuck who comes off the street with an IP address, and then either keep no record of that grant or discard the record quickly. Businesses that do this are lending their powerful and potentially harmful capabilities and demanding little accountability in return. That arrangement has obvious benefits but also obvious costs. The victims of online torts and crimes bear these costs, and those victims are, overwhelmingly, third parties. They include big movie studios, middle-aged Internet newbies and, unfortunately in some cases, young children.

If the legal rules change, and companies are held liable more often for what their users do, then the cost of anonymity would shift away from victims and toward the providers. In this world, providers will be more careful about identifying users. Perhaps online assertions of identity will be backed up with offline proof; providers will be more careful about providing potential scam artists in distant jurisdictions with the tools to practice their craft. All this would be expensive for service providers, but not as expensive as it is for injured parties today.

Secondary liability should not reach every company that plays any hand in assisting the online wrong-doer, of course. Before secondary liability attaches, the plaintiff must show that the defendant provided a crucial service, knew of the illegal activity, and had a right and a cost-justified ability to control the

---

6 Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007) (quotations, citations and italics omitted).

infringer's actions. This rule will in almost every case exclude electrical utilities, landlords, and others whose contributions to illegal activity are minuscule.

While we have come a long way from Barlow's Declaration of the Independence of Cyberspace, the central idea behind it—that the Internet is a special place, separate somehow from the brick and mortar world, and thus subject to special rules and regulations, or no rules and regulations—lingers. The name itself has a powerful influence: we don't speak of "telephone-space" or "radio-space" or "TV-space"—though we do have Television City in Hollywood. Prior technological advances that aided in connecting people were generally recognized as tools to aid life in the real world; no one claimed that they made up a separate dimension that is somehow different and separate from the real word. Every time we use the term "cyberspace" or the now-outmoded "Information Superhighway," we buy into the idea that the world-wide network of computers that people use for electronic commerce and communication is a separate, organic entity that is entitled to special treatment.

This idea of cyberspace as a separate place subject to a different set of rules—one where courts ought to tread lightly lest they disturb the natural order of things and thereby cause great harm—still arises in many court cases.[7]

The first of these is *Perfect 10 v. Visa*—a case where one of the authors of this piece was in the dissent.[8] The facts are simple: plaintiff produces and owns pictures of scantily-clad young women, which it sells online. It alleged that unknown parties had copied the pictures and were selling them online, at a lower price, using servers in remote locations where the legal system was not hospitable to copyright and trademark lawsuits, and, moreover, they could fold up their tents and open up business elsewhere if anyone really tried to pursue them. So the plaintiff didn't try to sue the primary infringers; instead, it went after the credit card companies that were processing the payments for what they claimed were pirated photographs.

---

7 Some disclaimers: One of the authors of this piece (Chief Judge Kozinski) sat on the panel that decided some of the cases given as examples here. He wants to make it clear that he won't re-argue the cases here. Both involved split decisions, and his views as to how those cases should have come out is set out in his opinions in those cases. His colleagues on the other side are not present to argue their positions and, in any event, it's unseemly to continue a judicial debate after the case is over. Furthermore, despite his disagreement with his colleagues, he respects and appreciates their views. The judges that came out the other way are some of the dearest of his colleagues, and some of the finest judges anywhere. The disagreement is troubling, because they bring a wealth of intelligence, diligence, talent, experience and objectivity to the problem, and he can't quite figure out why they see things so differently.

8 Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788 (9th Cir. 2007).

This was by far not the first case that applied the doctrine of secondary infringement to electronic commerce. The cases go back at least to the 1995 case of *Religious Technology Center v. Netcom*,[9] a case involving the liability of an ISP for damage caused when it posted copyrighted Scientology documents to USENET, at the direction of one of its users. And, of course, the Napster, Aimster and Grokster cases all dealt with the secondary liability of those who assist others in infringement.[10] *Perfect 10*, though, presented a novel question: how do you apply the doctrine of secondary infringement to people who help the transaction along, but never have any physical contact with the protected work?

Two excellent and conscientious Ninth Circuit jurists, Judges Milan Smith and Stephen Reinhardt, said there was no liability, whereas the dissenting judge concluded that there was. Visa, the dissent argued, was no different from any other company that provided a service to infringers, knew what it was doing, and had the ability to withdraw its service and stop the infringement, but did nothing.

This debate fits within a larger context. In the majority's rejection of contributory liability, it cited a public policy decision that found that the Internet's development should be promoted by keeping it free of legal regulation. Relatedly, the majority distinguished some precedent by saying that its "tests were developed for a brick-and-mortar world" and hence "do not lend themselves well to application in an electronic commerce context."[11]

This argument channels Barlow's declaration that users of the Internet are entitled to special treatment (or, as he would have it, entitled to no treatment). The chief justification for this argument is that the Internet is so new, exotic and complicated that the imposition of legal rules will chill, stifle, discourage or otherwise squelch the budding geniuses who might otherwise create the next Google, Pets.com, or HamsterDance.com. For example, the Electronic Frontier Foundation argued to the Supreme Court during the Grokster case that if the Ninth Circuit's opinion were reversed, the effect would "threaten innovation by subjecting product design to expensive and indeterminate judicial

---

9 Religious Tech. Ctr. v. Netcom, 907 F.Supp. 1361 (N.D. Cal. 1995).

10 *See* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002); In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003); Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

11 *Perfect 10*, 494 F.3d at 798, n.9.

second-guessing."[12] The Ninth Circuit was reversed, and if that decision slowed the pace of product design, no one seems to have noticed.

This argument became particularly central in a second case, *Fair Housing Council of San Fernando Valley v. Roommates.com*.[13] The case involved a claim that the commercial website Roommates.com violated state and federal fair housing laws by helping to pair up roommates according to their personal preferences, the exercise of which is allegedly prohibited by law. Again, one of the authors of this piece was a judge on that case, and was in the majority at both the panel and the *en banc* level—despite the efforts of some conscientious and brilliant dissenting judges, of whose intellectual rigor and commitment to the rule of law no one can doubt.

The majority mostly held that Roommates.com could be held liable, if the plaintiff's allegations were proven true. The court held essentially that an online business had to be held to the same substantive law as businesses in the brick-and-mortar world. The dissenters saw things quite differently; to them, the majority placed in jeopardy the survival of the Internet. Here is a taste of the dissent:

> On a daily basis, we rely on the tools of cyberspace to help us make, maintain, and rekindle friendships; find places to live, work, eat, and travel; exchange views on topics ranging from terrorism to patriotism; and enlighten ourselves on subjects from "aardvarks to Zoroastrianism." … The majority's unprecedented expansion of liability for Internet service providers threatens to chill the robust development of the Internet that Congress envisioned … . We should be looking at the housing issue through the lens of the Internet, not from the perspective of traditional publisher liability.[14]

And finally, the unkindest cut of all: "The majority's decision, which sets us apart from five circuits, … violates the spirit and serendipity of the Internet."[15]

The argument that a legal holding will bring the Internet to a standstill makes most judges listen closely. Just think of the panic that was created when the

---

12 *See* Brief for Respondents, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., No. 04-480 (9th Cir. Mar. 1, 2005), available at 2005 WL 508120 and at **http://w2.eff.org/IP/P2P/MGM_v_Grokster/20050301_respondents_brief.pdf**.

13 Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157 (9th Cir. 2008).

14 *Id.* at 1176-77 (footnote omitted).

15 *Id.* at 1177.

Blackberry server went down for a few hours. No one in a black robe wants to be responsible for anything like that, and when intelligent, hard-working, thoughtful colleagues argue that this will be the effect of one of your rulings, you have to think long and hard about whether you want to go that way. It tests the courage of your convictions.

Closely related is the argument that, even if you don't bring down the existing structure, the threat of liability will stifle innovation, so that the progress we have seen in recent years—and the gains in productivity and personal satisfaction—will stop because the legal structure has made innovation too risky or expensive. The innovation argument is partly right but mostly wrong. Certainly, some innovators will shy away from legally murky areas. It's hard to think of a worse recipe for creativity than having a lawyer attend every engineering meeting. But promoting innovation alone cannot be a sufficient justification for exempting innovators from the law. An unfortunate result of our complex legal system is that almost everyone is confused about what the law means, and everyone engaged in a business of any complexity at some point has to consult a lawyer. If the need to obey the law stifles innovation, that stifling is just another cost of having a society ruled by law. In this sense, the Internet is no different than the pharmaceutical industry or the auto industry: They face formidable legal regulation, yet they continue to innovate.

There is an even more fundamental reason why it would be unwise to exempt the innovators who create the technology that will shape the course of our lives: Granting them that exemption will yield a generation of technology that facilitates the behavior that our society has decided to prohibit. If the Internet is still being developed, then we should do what we can to guide its development in a direction that promotes compliance with the law.

For example, what use is "innovation" in creating a job hunting site if the innovators produce a site that invites employers to automatically reject any applicant from a particular race? Perhaps the job site is a bold new innovation that makes hiring far easier and more efficient than it has ever been. But if this site is used widely, it will facilitate racial discrimination in hiring—conduct that society has already decided it must prohibit. Similarly, is a file-sharing service such as Grokster worth the harm it causes by offering no built-in tools for identifying participants or establishing they have the right to "share" the files they copy? Far from exempting this growing industry from the law, we should vigorously enforce the law as the industry grows, so that when it is mature, its services won't guide behavior toward conduct that society has decided to discourage. As difficult as it might be for innovators today, it is easier than the alternatives: forcing them to rebuild everything ten years down the road, or grudgingly accepting that we have surrendered key aspects of our ability to govern our society through law.

It is Barlow who is generally credited with taking the word "cyberspace" from the science fiction of William Gibson and applying it to the Internet.[16] In doing so, he launched the conceit that such a "space" exists at all. This was wholly unjustified. It is a mistake to fall into Barlow's trap of believing that the set of human interactions that is conducted online can be neatly grouped together into a discrete "cyberspace" that operates under its own rules. Technological innovations give us new capabilities, but they don't change the fundamental ways that humans deal with each other. The introduction of telephones and cars did create new legal questions. Those questions all revolved around what the acceptable uses of the new technologies were. How closely can you follow the car in front of you on the highway? Can you repeatedly dial someone's phone to annoy them? Can you tap into a phone conversation or put a tape recorder in a phone booth? Over time, courts and legislatures answered these questions with new legal rules. They had to; the essence of the controversy arose from the new technological abilities. But no one thought that telephones and cars changed the legal rules surrounding what was said on a telephone or where a car traveled. Can an oral contract be formed with a telephone call? Of course; it is still two people speaking. Is it trespassing to drive across my neighbor's front yard? Of course; you are on his land.

Like cars and telephones, the Internet prompts new questions about the acceptable uses of the new technology. Is port-scanning a form of hacking? When does title to a domain name legally transfer? While analogies to settled legal rules are helpful in answering these questions, they are not conclusive. Answers to these questions will look like new legal rules.

But when the Internet is involved in a controversy only because the parties happened to use it to communicate, new legal rules will rarely be necessary. When the substance of the offense is that something was communicated, then the harm occurs regardless of the tools used to communicate. If an attorney betrays a client's confidence, the duty to the client is breached regardless of whether the attorney used a telephone, a newspaper, a radio station, or the Internet. The choice of communication medium might affect the magnitude of the harm, but if it is illegal for A to communicate X to B without C's permission, there is no reason to fashion new rules of liability that depend on the mode of communication used.

There are some ways that the Internet might require courts to re-think legal rules. The Internet makes long-distance communication cheaper than it was before. To the extent that existing legal rules were premised on the assumption that communications were expensive, the Internet might require a reappraisal. Courts are already reevaluating, for example, what it means to do business

---

16 *See* John Perry Barlow, *Crime and Puzzlement: In Advance of the Law on the Electronic Frontier*, WHOLE EARTH REV., Sept. 22, 1990, at 44, 45.

within a state, for purposes of the long-arm statute, when the defendant's "business establishment" is a server located in Uzbekistan.

Yet the vast majority of Internet cases that have reached the courts have not required new legal rules to solve them. It has been fifteen years since America Online unleashed its hordes of home computing modem-owners on e-mail and the Internet and fifteen years since the release of the Mosaic Web browser. After all that time, we have today relatively few legal rules that apply only to the Internet. Using the Internet, people buy stocks, advertise used goods and apply for jobs. All those transactions are governed by the exact same laws as would govern them if they were done offline.

Those who claim the Internet requires special rules to deal with these ordinary controversies have trouble explaining this history. Despite this dearth of Internet-specific law, the Internet is doing wonderfully. It has survived speculative booms and busts, made millionaires out of many and, unfortunately, rude bloggers out of more than a few. The lack of a special Internet civil code has not hurt its development.

The Internet, it turns out, was never so independent or sovereign as early idealists believed. It was an astounding social and technological achievement, and it continues to change our lives. But it has not proven to be invulnerable to legal regulation—at least, not unless we choose to make it invulnerable. As intriguing as Barlow's Declaration of Independence was, the original 1776 Declaration is more profound in its understanding of the purpose and abilities of government: men have rights of "Life, Liberty and the pursuit of Happiness," and "to secure these rights, Governments are instituted among Men." The government that we have instituted retains its purpose of securing those rights, and it accomplishes that purpose through the law. We have seen that our government has many tools at its disposal through which it can bring law to the Internet's far reaches. The Internet might pose obstacles toward that job, but those obstacles can be overcome. The question is whether we will do it.

# Is Internet Exceptionalism Dead?

By Tim Wu*

In 1831, Alexis de Tocqueville released *Democracy in America,* the founding text of "American exceptionalism." After long study in the field, America, he had concluded, was just different than other nations. In an often-quoted passage, de Tocqueville wrote:

> The position of the Americans is therefore quite exceptional, and it may be believed that no democratic people will ever be placed in a similar one. Their strictly Puritanical origin—their exclusively commercial habits—even the country they inhabit, which seems to divert their minds from the pursuit of science, literature, and the arts—the proximity of Europe, which allows them to neglect these pursuits without relapsing into barbarism—a thousand special causes, of which I have only been able to point out the most important—have singularly concurred to fix the mind of the American upon purely practical objects. His passions, his wants, his education, and everything about him seem to unite in drawing the native of the United States earthward; his religion alone bids him turn, from time to time, a transient and distracted glance to heaven.[1]

Is there such a thing as Internet exceptionalism? If so, just what is the Internet an exception to? It may appear technical, but this is actually one of the big questions of our generation, for the Internet has shaped the United States and the world over the last twenty years in ways people still struggle to understand. From its beginnings the Internet has always been different from the networks that preceded it—the telephone, radio and television, and cable. But is it different in a lasting way?

The question is not merely academic. The greatest Internet firms can be succinctly defined as those that have best understood what makes the Internet different. Those that have failed to understand the "Network of Networks"—say, AOL, perished, while those that have, like Google and Amazon, have flourished. Hence the question of Internet exceptionalism is often a multi-billion dollar question. The state of the Internet has an obvious effect on national and international culture. It is also of considerable political relevance,

---

* Professor, Columbia Law School; Fellow, New America Foundation

1 ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 519 (Henry Reeve trans., D. Appleton and Company 1904) (1831).

both for enforcement of the laws, and the rise of candidates and social movements.

What makes the question so interesting is that the Internet is both obviously exceptional and unexceptional at the same time. It depends on *what* you might think it is an exception to. It is clear that the Internet was a dramatic revolution and an exception to the ordinary ways of designing communications systems. But whether it enjoys a special immunity to the longer and deeper forces that shape human history is, shall we say, yet to be seen.

* * *

In the early 2000s, Jack Goldsmith and I wrote *Who Controls the Internet?*[2] The book is an explicitly anti-exceptionalist work. It addressed one particular way that the Internet might be an exception, namely, the susceptibility, as it were, of the Internet to regulation by the laws of nations. From the mid-1990s onward it was widely thought that the Internet would prove impossible to control or regulate. Some legal scholars, in interesting and provocative work, argued that in some ways the Network might be considered to have its own sovereignty, like a nation-state.[3] That was the boldest claim, but the general idea that the Internet was difficult or impossible to regulate was, at the time, a political, journalistic and academic commonplace, taken for granted. For example, reflecting his times, in 1998 President Clinton gave a speech about China's efforts to control the Internet. "Now, there's no question China has been trying to crack down on the Internet—good luck" he said. "That's sort of like trying to nail Jello to the wall."[4]

That was the conventional wisdom. In our book we suggested that despite the wonders of the Network it did not present an existential challenge to national legal systems, reliant, as they are, on threats of physical force.[5] We predicted that nations would, and to some degree already had, reassert their power over the Network, at least, for matters they cared about. They would assert their power not over the Network in an abstract sense, but the actual, physical humans and machinery who lie underneath it. Many of the book's chapters ended with people in jail; unsurprisingly, China provided the strongest example of what a State will do to try to control information within its borders.

---

2 TIM WU & JACK GOLDSMITH, WHO CONTROLS THE INTERNET (2006).

3 David Post & David Johnson, *Law and Borders–The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

4 R. MICHAEL ALVAREZ & THAD E. HALL, POINT, CLICK AND VOTE: THE FUTURE OF INTERNET VOTING 3 (2004).

5 JOHN AUSTIN, THE PROVINCE OF JURISPRUDENCE DETERMINED (Wilfrid E. Rumble, ed., Cambridge Univ. Press 1995) (1832).

Drama aside, in a deeper way, we were interested in what you might call the persistence of physicality. Despite its virtual qualities, behind the concept of a global network were living human beings, blood and flesh. The human body's susceptibility to pain and imprisonment is a large part of what the nation-state bases its rule on, and that had not changed. We predicted that the nation's threat of physical force, otherwise known as laws, would therefore shape the Network as much as its founding ambitions.

Here is how we put the point in the introduction to our book, written in about 2005 or so:

> Our age is obsessed with the search for the newest "new thing." Our story, by contrast, is about old things—ancient principles of law and politics within nations, cooperation and clashes between nations, and the enduring relevance of territory, and physical coercion. It is a story where Thomas Hobbes is as important as Bill Gates. Like it or not, these old things are as important to the Net's development, if not more so, than any technological or intellectual breakthrough.
>
> In these pages we present a strong resistance to Internet exceptionalism, or any arguments that new technologies can only be understood using novel intellectual frameworks. Like other revolutionary communication technologies, the Internet has changed the way we live, and fostering undreamt of new forms of social organization and interaction. But also like other revolutionary communication technologies, the Internet has not changed the fundamental roles played by territorial government.
>
> We are optimists who love the internet and believe that it can and has made the world a better place. But we are realistic about the role of government and power in that future, and realists about the prospects for the future.

I regret to say that it has been the Chinese government that has done the most to prove our basic thesis correct. The Jello was, somehow, nailed to the wall. Despite nearly a decade of Westerners (most particularly Western newspaper columnists) assuming or hoping that the Net would bring down the Chinese state, it didn't happen; indeed it never even came close. And so, five years later the basic ideas in our book seem hard to contest. Consequently, this one particular species of Internet exceptionalism—the idea that the network has its own sovereignty in a sense, or is an exception to law—has weakened and may be dead.

In the summer of 2010, in fact, as if to hammer to point home, the Chinese government released a new White Paper on "Internet Policy." It made its centerpiece the phrase coined by the Internet exceptionalists of the 1990s: "Internet Sovereignty." However, that phrase did not mean what it did in the 1990s. Rather as the People's Daily, the state newspaper, explained, "Internet Sovereignty" means that "all foreign IT companies operating in China must abide by China's laws and [be] subject to Beijing's oversight."[6]

* * *

Leaving law aside, however, the larger questions of Internet Exceptionalism remain unanswered. It is surely one thing for the Internet to be a living exception to the legal system, a sovereign unto itself in some way. But is the Network an exception as an *information network*, as a means for a nation or world to communicate? Here, surely, the exceptionalist is on far stronger ground. Whatever you might say about efforts to use the Internet to avoid law, we cannot doubt that the "Networks of Networks" has changed the way we communicate in dramatic fashion. Technologically, and in its effects on business, culture and politics, the Internet seems, by almost any account, an exception, different from the way other systems of mass communications have operated, whether the telephone, radio, or the television.

This point seems so obvious as to be commonplace to anyone who's lived through the 1990s. Unlike television, radio and newspapers, which all are speech outlets for a privileged few, the Internet allows anyone to be a publisher. Unlike the private cable networks, the Internet is public and, in its totality, owned by no one. Unlike the telephone system, it carries video, graphics, the Web, and supports any idea anyone can come up with. It has played host to generations of new inventions, from email and the World Wide Web to the search engine, from shops like eBay and Amazon to social networking and blogging. It has challenged and changed industries, from entertainment to banking and travel industries. These features and others are what have made the Network so interesting for so many years.

The question is whether, however, the Internet is different in a *lasting* way. What do I mean, "a lasting way?" I rely on the sense that certain ideas, once spread, seem to lodge permanently, or for centuries at least—*e.g.*, the idea of property, civil rights, or vaccination. Each is an idea that, once received, has a way of embedding itself so deeply as to be nearly impossible to dislodge. In contrast are ideas that, while doubtlessly important, tend, in retrospect, to form a rather interesting blip in history, a revolution that came and went. Will we

---

6 Information Office of the State Council of the People's Republic of China, *The Internet in China*, 2010, **http://www.china.org.cn/government/whitepaper/node_7093508.htm**; *White paper explains 'Internet Sovereignty'*, PEOPLE'S DAILY ONLINE, June 9, 2010, **http://english.peopledaily.com.cn/90001/90776/90785/7018630.html**.

think of the open age of the Internet the way we think of communism, or the hula-hoop?[7]

If the Internet is exceptional in a lasting way, it must be for its ideology as expressed in its technology. And in this sense its exceptionalism is similar to American exceptionalism. Both the Nation and the Network were founded on unusual and distinct ideologies, following a revolution (one actual, another technological). In a typical account, writer Seymour Martin Lipset writes in *American Exceptionalism: A Double-Edged Sword*: "The United States is exceptional in starting from a revolutionary event … it has defined its *raison d'être* ideologically."[8] Or, as one-time Columbia professor Richard Hofstadter wrote in the 20th century, "it has been our fate as a nation to not to have ideologies, but to be one."[9] De Tocqueville put American exceptionalism down to particular features of the United States—the religiosity of its founding, its proximity to yet freedom from Europe, and, as he wrote, "a thousand special causes."[10]

Looking at the Internet, its founding and its development, we can find the same pattern of a revolution, an ideology, and many "special causes." While much of it was purely technical, there were deeply revolutionary ideas, even by technological standards, at the heart of the Internet, even if sometimes they were arrived at in accidental fashion or for pragmatic reasons.

Of course, fully describing all that makes the Internet different would take another *Democracy in America*, and we have the benefit of many writers who've tried to do just that, whether in Katie Hafner and Matthew Lyon's *Where Wizards Stay up Late,* the oral accounts of its creators, classic works like J.H. Saltzer et al., *End-to-End Arguments in System Design*, or Jonathan Zittrain's *The Future of the Internet.*[11]

---

7 I've spent some time thinking about these questions, and I want to suggest that it isn't really possible to answer the question in full without understanding the story of the networks that preceded the Internet. My fullest answer to the question I've posed, then, is in THE MASTER SWITCH (Knopf 2010), an effort to try and find the patterns, over time, that surround revolutionary technologies. This time, unlike in WHO CONTROLS THE INTERNET, when it comes to the broader question of the Internet as a way of moving information, I tend to side with the exceptionalists, though it is a close call.

8 SEYMOUR MARTIN LIPSET, AMERICAN EXCEPTIONALISM 18 (1996).

9 JAMES M. JASPER, RESTLESS NATION 38 (2000).

10 ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 519 (Henry Reeve trans., D. Appleton and Company 1904) (1831).

11 KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996);J. H. Saltzer, D. P. Reed & D. D. Clark, *End-To-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYSTEMS (TOCS) 277-288 (1984); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2009).

To understand what makes the Internet different, the origins of the Internet bear careful examination. First, the Network's predecessors (the telephone, cable, etc.) were all commercial enterprises first and foremost, invented and deployed (in the U.S.) by private firms. The Internet, in contrast, was founded as a research network, explicitly non-commercial and public for the first decade of its existence. Private companies were involved, yes, but it was not a commercial operation in the same sense that, say, the cable networks always were.

Perhaps, thanks to its origins, the Internet was founded with an ideology that was far more explicit than most—a kind of pragmatic libertarianism whose influence remains. The early Internet scientists had various principles that they were proud of. One example is David Clark's memorable adage. "We reject: kings, presidents, and voting. We believe in: rough consensus and running code." Another is found in a famous Request For Comments written by Internet founder Jon Postel, setting forth the following as a principle for network operators: "Be conservative in what you do. Be liberal in what you accept from others."[12]

The Network constituted not just a technological advance, though it was that as well, but also a rejection of dominant theories of system design and, in a deeper sense, a revolution in information governance. The early Internet researchers were designing a radically decentralized network in an age—the mid-1960s—when highly centralized systems ran nearly every aspect of American and world life. In communications this was represented by AT&T, the great monopolist, with its mighty and near-perfect telephone network. But it could also be found in other aspects of society, from the enlarged Defense Department that ran the Cold War, the new, giant government agencies that ran social programs, and enormous corporations like General Motors, IBM, and General Electric.

So when Vint Cerf and his colleagues put the Internet on the TCP/IP protocol in 1982 (its effective "launch"), most information networks—and I don't mean this is a pejorative sense—could be described as top-down dictatorships. One entity—usually a firm or a part of the State (or both), like AT&T or the BBC, decided what the network would be. The Internet, in contrast, has long been governed more like a federation of networks, and in some respects, like a Republic of Users. That is implicit in the ability of anyone to own an IP address, set up a website, and publish information—something never true, and still not true, on any other network.

---

12 Paulina Borsook, *How Anarchy Works*, WIRED (Oct. 1995), **http://www.wired.com/wired/archive/3.10/ietf.html**; Jon Postel, Information Sciences Institute of the University of Southern California, DOD Standard Transmission Control Protocol 13 (1980), *available at* **http://tools.ietf.org/html/rfc761#section-2.10**.

Throughout its history, the universal Network has, true to the governance structure, seen a pattern of innovation that is unlike any other. This too is the subject of much scholarship and popular recognition—the mode of "decentralized innovation" that had led every several years or so to the next wonder, starting with email, through the Web, search engines, online retail, Web video, social networking, and onward. These innovations arrived in a highly disorganized fashion often led by amateurs and outsiders. The spread of computer-networking itself began with amateur geeks glorified in 1980s films like *War Games.*[13] It is hard to think of a truly important Internet invention that came from a firm that predated the Internet. Society-changers like Craigslist, eBay, Wikipedia and blogs are obviously the products of geeks.

* * *

Can it last? Can the Internet remain, in this sense, exceptional? Whatever the Internet's original ideas, it is easy to argue that all this, too, shall pass. The argument from transience suggests that all that seems revolutionary about the Internet is actually just a phase common to speech inventions. In other words, the Internet is following a path already blazed by other revolutionary inventions in their time, from the telephone to radio. Such disruptive innovations usually do arrive as an outsider of some kind, and will pass through what you might call a "utopian" or "open" phase—which is where we are now. But that's just a phase. As time passes, even yesterday's radical new invention becomes the foundation and sole possession of one or more great firms, monopolists, or sometimes, the state, particularly in totalitarian regimes like the Soviet Union or the Third Reich. The openness ends, replaced with better production value and tighter controls. It is, in other words, back to normal, or at least what passed for normal for most of human history.

We might learn from the fate of the broadcast radio, the darling new technology of the 1920s.[14] In the 1920s, opening a radio station was relatively easy, not quite as easy as a website, but within the reach of amateurs. American radio was once radically decentralized, open and rather utopian in its aspirations. But by the 1930s, broadcast in the United States was increasing controlled by the chains—most of all, the National Broadcast Company, NBC, who brought better programming, but also much less of the amateur, open spirit. But that's nothing compared to countries like Germany and the Soviet Union, where radio became the domain of the state, used to control and cajole. In Germany, every citizen was issued a "people's receiver" tuned only to Nazi channels, and within

---

13 War Games (Metro-Goldwyn-Mayer 1983)

14 This story of radio can be found in TIM WU, THE MASTER SWITCH, chaps 3, 5 (2010).

the space of a decade, the free radio had became what Joseph Goebbels called the "spiritual weapon of the totalitarian state."[15]

Yet I find it hard to imagine such a dramatic or immediate fate for the Internet. It seems in so many ways too established, its values too enmeshed in society, to disappear in an instant.

Perhaps it would be more accurate to suggest that there are aspects of the Internet ideology that are more and less likely to fade, to become yesterday's ideas. At one extreme, the Internet's core technological ideas, protocol layering & packet-switching, seem unlikely to go anywhere. The reason is that these techniques have become the basis of almost all information technology, not just the Internet itself. The telephone networks are today layered and packet-switched, even if they don't rely on the Internet Protocol.

More vulnerable, however, are the Internet's early ideas of openness and decentralized operation—putting the intelligence in the edges, as opposed to the center of the network. Originally described by engineers as the E2E principle, and popularly contained in the catch-phrase "Net Neutrality," these principles have survived the arrival of broadband networks. Yet by its nature, Net Neutrality seems easier to upset, for discrimination in information systems has long been the rule, not the exception. There are, importantly, certain commercial advantages to discriminatory networking that are impossible to deny, temptations that even the Internet's most open firms find difficult to resist. So while I may personally think open networking is important for reasons related to innovation and free speech, it seems obvious to me that open networking principles *can* be dislodged from their current perch.

Another open question is whether some of the means of production and cultural creativity that are associated with the Internet are destined for lasting importance. We have recently lived through an era when it was not unusual for an amateur video or blog to gain a greater viewership than films made for tens of millions. But is that, Lessig's "remix culture,"[16] a novelty of our times? We also live in era where free software is often better than that which you pay for. They are the products of open production systems, the subject of Yochai Benkler's *The Wealth of Networks*, the engines behind Linux and Wikipedia and other mass projects—as discussed in Benkler's essay in this collection.[17] Of course such systems have always existed, but will they retreat to secondary

---

15 Quoted in Garth S. Jowett, GARTH JOWETT & VICTORIA O'DONNELL, READINGS IN PROPAGANDA AND PERSUASION 132 (2005).

16 LAWRENCE LESSIG, REMIX: MAKING ART AND COMMERCE THRIVE IN THE HYBRID ECONOMY (2008).

17 YOCHAI BENKLER, THE WEALTH OF NETWORKS (2007).

roles? Or will they perhaps become of primary importance for many areas of national life?

The only honest answer is that it is too early to tell. And yet, at the same time, the transience of *all* systems suggests that at least *some* of what we take for granted right now as intrinsic to our information life and to the nature of the Internet *will* fade.

The reasons are many. It might simply be that the underlying ideas just discussed turn out to have their limits. Or that they are subject to an almost natural cycle—excessive decentralization begins to make centralization more attractive, and vice versa. More sinisterly, it might be because forces disadvantaged by these ideas seem to undermine their power—whether concentrated forces, like a powerful state, or more subtle forces, like the human desire for security, simplicity and ease that has long powered firms from the National Broadcasting Corporation to Apple, Inc.

Whatever the reasons, and while I do think the Internet is exceptional (like the United States itself), I also think it will, come to resemble more "normal" information networks—indeed, it has already begun to do so in many ways. Exceptionalism, in short, cannot be assumed, but must be defended.

* * *

I began this essay with a comparison between Internet and American exceptionalism. Yet I want to close by suggesting we can learn from the comparison in a slightly different sense. I've suggested that there is a natural tendency for any exceptional system to fade and transition back to observed patterns. But even if that's true, what is natural is not always normatively good, not always what we want. For example, it may very well be "natural" for a democracy, after a few decades or less, to ripen into a dictatorship of some kind, given the frustrations and inefficiencies of democratic governance. Cromwell and Napoleon are the bearers of that particular tradition, and it has certainly been the pattern over much of history.

But the idea of American Exceptionalism has included a commitment to trying to avoid that fate, even if it may be natural. Despite a few close calls, the United States remains an exception to the old rule that Republics inevitably collapse back into dictatorship under the sway of a great leader. The Internet, so far, is an exception to the rule that open networks inevitably close and become dominated by the State or a small number of mighty monopolists. Twenty-five years after .COM, we might say we still have a republic of information—if we can keep it.

# Bibliography

In lieu of extensive footnotes, I thought I'd provide here the books and articles that have, implicitly or explicitly, taken on the question of Internet Exceptionalism. Notice that, for those familiar in the field, this may lead to some unusual groupings—but the fundamental question is whether the project in question tries to argue the Internet is magically different or a repeat of age-old problems.

## Exceptionalist Works


- PETER HUBER, LAW AND DISORDER IN CYBERSPACE (1997).
- J. H. Saltzer, D. P. Reed & D. D. Clark, *End-To-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYSTEMS (TOCS) 277-288 (1984).
- NICHOLAS NEGROPONTE, BEING DIGITAL (1996).
- LAWRENCE LESSIG, THE FUTURE OF IDEAS (2002).
- David R. Johnson & David Post, *Law & Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).
- Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2001).
- Susan P. Crawford, *The Internet and the Project of Communications Law*, 55 UCLA L. REV. 359 (2007).
- DAVID POST, IN SEARCH OF JEFFERSON'S MOOSE (2009).
- TIM WU, THE MASTER SWITCH (2010).


## Anti-Exceptionalist Works


- LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE (2006).
- TIM WU & JACK GOLDSMITH, WHO CONTROLS THE INTERNET? (2008).
- Tim Wu, *Cyberspace Sovereignty?*, 10 HARV. J.L. & TECH. 647 (1997).
- Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debate*, 3 J. TELECOMM. & HIGH TECH. L. 23 (2004).
- YOCHAI BENKLER, THE WEALTH OF NETWORKS (2007).
- CORY DOCTOROW, LITTLE BROTHER (2008).


## On the Topic / Mixed


- JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2009).

# Section 230 of the CDA: Internet Exceptionalism as a Statutory Construct

By H. Brian Holland*

## Introduction

Since its enactment in 1996, Section 230 of the Communications Decency Act has become perhaps the most significant statute in the regulation of online content, and one of the most intensely scrutinized. Many early commentators criticized both Congress, for its apparent inability to craft the more limited statute it intended, and the courts, for interpreting the statute broadly and failing to limit its reach. Later commentators focus more clearly on policy concerns, contending that the failure to impose liability on intermediaries fails to effectuate principles of efficiency and cost avoidance. More recently, commentators have argued that Section 230 immunity should be limited because it contributes to the proliferation of anonymous hate speech, intimidation, and threats of violence against traditionally marginalized groups.

Acknowledging the validity of these concerns, this essay nevertheless takes the opposing view, defending broad Section 230 immunity as essential to the evolving structure of Internet governance. Specifically, Section 230 provides a means of working within the sovereign legal system to effectuate many of the goals, ideals, and realities of the Internet exceptionalist and cyber-libertarian movements. By mitigating the imposition of certain external legal norms in the online environment, Section 230 helps to create the initial conditions necessary for the development of a modified form of exceptionalism. With the impact of external norms diminished, Web 2.0 communities, such as wikis[1] and social network services,[2] have emerged to facilitate a limited market in norms and values and to provide internal enforcement mechanisms that allow new communal norms to emerge. Section 230 plays a vital role in this process of

---

* Associate Professor, Texas Wesleyan School of Law. A modified version of this essay originally appeared in the University of Kansas Law Review. *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism,* 56 U. Kan. L. Rev. 369 (2008), **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=979183**.

1 A wiki is a website designed to allow visitors to easily create and edit any page on the site. For more information, see Wikipedia, *Wiki*, **http://en.wikipedia.org/wiki/Wiki** (last accessed Dec. 1, 2010).

2 Social network services are online services designed for users to share messages, links, and media (photos and video) with friends or others with similar interests. Some popular social network services are Facebook, MySpace, and Twitter.

building heterogeneous communities that encourage collaborative production and communication. Efforts to substantially reform or restrict Section 230 immunity are therefore largely unnecessary and unwise.

The essay begins with a brief introduction to Section 230. As interpreted and applied by the judiciary, this statute is now conceived as a broad grant of immunity from tort liability—broad not only in terms of those who can claim its protection but also in terms of predicate acts and causes of action to which such immunity extends.

Working from this foundation, I then seek to position the courts' expansion of Section 230 immunity within the larger debate over Internet governance, suggesting that proponents of expanded immunity are successfully creating what might be characterized as a modified, less demanding form of cyber-libertarian exceptionalism than what Eric Goldman calls, in his essay in this book, the "First Wave of Internet Exceptionalism" (one of "Internet Utopianism"), as articulated in the mid-1990s. The dramatic expansion of Section 230 immunity has in a limited sense effectuated a vision of a community in which norms of relationship, thought and expression are yet to be formed. The tort liability from which Section 230 provides immunity is, together with contract, a primary means by which society defines civil wrongs actionable at law. In the near absence of these external norms of conduct regulating relationships among individuals, the online community is free to create its own norms, its own rules of conduct, or none at all. It is a glimpse of an emergent community existing within, rather than without, the sovereign legal system.

Finally, I make the case for preserving broad Section 230 immunity. As an initial matter, many of the reforms offered by commentators are both unnecessary and unwise because the costs of imposing indirect liability on intermediaries are unreasonable in relationship to the harm deterred or remedied by doing so. Moreover, the imposition of liability would undermine the development of Web 2.0 communities as a form of modified exceptionalism that encourages the development of communal norms, efficient centers of collaborative production, and open forums for communication.

## The Expansion of Section 230 Immunity

In May of 1995, a New York trial court rocked the emerging online industry with its decision in *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[3] holding the Prodigy computer network liable for defamatory comments posted on one of its bulletin boards by a third-party. The key factor in this result was Prodigy's attempt to create a more family-friendly environment through the exercise of editorial control over the bulletin boards and moderating for offensive content.

---

[3] No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

Prodigy was therefore treated as a publisher of the information, rather than a mere distributor, and held strictly liable for actionable third-party content.

Representatives of the online industry argued that the Prodigy decision placed service providers in an untenable position by creating a "Hobson's choice"[4] between monitoring content and doing nothing, thereby insulating the service from liability. Congress responded to the decision by amending the draft Communications Decency Act (CDA) to include a tailored immunity provision addressing the online industry's concerns. As one element of what came to be known as the Good Samaritan provisions of the CDA, Section 230 was generally intended to provide online service providers and bulletin board hosts with immunity from tort liability for the defamatory acts of their users. This was accomplished by addressing those specific elements of common law defamation at issue in the Prodigy decision—editorial control and the distinct treatment of publishers and distributors under the law. To that end, Section 230 provided that no interactive computer service should be treated as the publisher or speaker of third-party content, and that efforts to moderate content should not create such liability.

In the years following the enactment of Section 230, courts consistently extended its application. This trend began in 1997 with the watershed decision in *Zeran v. America Online, Inc.*,[5] in which the Fourth Circuit applied Section 230 to claims that America Online (AOL) should be held liable for the defamatory content posted by one of its users. The plaintiffs claimed liability arose in part because AOL had allegedly failed to remove third-party defamatory messages from its bulletin board system within a reasonable time, refused to post retractions to defamatory messages, and failed to screen for similar defamatory messages thereafter. The court found the plaintiff's tort claims were preempted by Section 230, which rendered AOL immune. In reaching this result, the court rejected a strict reading of Section 230 as being limited to its terms. Although the statute failed to make any explicit reference to distributor liability, which the *Prodigy* decision appeared to leave intact, the court read distributor immunity into the statute, finding distributor liability to be an included subset of the publisher liability foreclosed by the statute. By collapsing the publisher-distributor distinction, the Fourth Circuit adopted the most expansive reading possible of both defamation law and Section 230. Thus, even though AOL knew the statements were false, defamatory, and causing great injury, AOL could simply refuse to take proper remedial and preventative action without fear of liability.

---

4 SAMUEL FISHER, THE RUSTICK'S ALARM TO THE RABBIES (1660), as cited in *Hobson's choice*, Wikipedia, **http://en.wikipedia.org/wiki/Hobson%27s_choice** (last accessed Dec. 1, 2010).

5 129 F.3d 327 (4th Cir. 1997).

Following *Zeran*, and building on that court's reading of both the statute and the policies sought to be effected, courts have extended the reach of Section 230 immunity along three lines: (1) by expanding the class who may claim its protections; (2) by limiting the class statutorily excluded from its protections; and (3) by expanding the causes of action from which immunity is provided.[6] As to the first, courts have interpreted the provision of immunity to interactive computer services to include such entities as Web hosting services, email service providers, commercial websites like eBay and Amazon, individual and company websites, Internet dating services, privately-created chat rooms, and Internet access points in copy centers and libraries. The additional provision of immunity to users of those services promises similar results. Already, one decision has held that a newsgroup user cannot be held liable for re-posting libelous comments by a third party,[7] while another court found a website message board to be both a provider and a user of an interactive computer service.[8]

The second line of extension results from a narrow reading of the term "information content provider," which defines the class for whom there is no immunity. Specifically, courts have held that minor alterations to third-party content does not constitute the provision of content itself, so long as the provider does not induce the unlawful content through the provision of offending raw materials of authorship and where the basic form and message of the original is retained.[9] The third point of expansion has been to extend Section 230 immunity beyond causes of action for defamation and related claims to provide immunity from such claims as negligent assistance in the sale/distribution of child pornography,[10] negligent distribution of pornography of and to adults,[11] negligent posting of incorrect stock information,[12] sale of fraudulently autographed sports memorabilia,[13] invasion of privacy,[14] and misappropriation of the right of publicity.[15]

---

6 *But see* Fair Housing. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (declining to extend Section 230 immunity to Roommates.com for certain categories of content solicited by the site for users in violation of federal fair housing laws).

7 Barrett v. Rosenthal, 146 P.3d 510, 527 (Cal. 2006).

8 DiMeo v. Max, 433 F. Supp. 2d 523, 531 (E.D. Pa. 2006).

9 Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003). *See also* Donato v. Moldow, 865 A.2d 711, 724 (N.J. Super. Ct. App. Div. 2005) (quoting *Batzel v. Smith*).

10 Doe v. Am. Online, Inc., 783 So. 2d 1010, 1017 (Fla. 2001).

11 Does v. Franco Prods., No. 99 C 7885, 2000 WL 816779, at *5 (N.D. Ill. June 22, 2000), *aff'd sub nom.* Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

12 Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000).

13 Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 715 (Cal. Ct. App. 2002).

# Section 230, Internet Governance & Exceptionalism

Situated within the larger debate over Internet governance, the concept of Internet exceptionalism presumes that cyberspace cannot be confined by physical borders or controlled by traditional sovereign governments, and thus that cyber-libertarian communities will emerge in which norms of relationship, thought and expression are yet to be formed. Although these ideas have been subjected to intense criticism and somewhat obscured by recent developments in the governance debates, they remain a touchstone for the cyber-libertarian ideal. This part of the essay seeks to clear space in the governance debates for this vision of exceptionalism, and argues that Section 230 is in some limited way facilitating the emergence of cyber-libertarian communities in a modified, less demanding form.

## Foundational Arguments of Internet Governance

The debate over Internet governance evolved in two surprisingly distinct, albeit convergent stages. The first stage of the governance debate focused on law and social norms, and whether these traditional models of regulating human relations could be validly applied to the online environment. In this context, exceptionalism was conceptualized as a state of being to which the Internet had naturally evolved, apart from terrestrial space. The second stage of the debate introduced network architecture as an important and potentially dominant means of regulating the online environment. In this context, exceptionalism became an objective to be pursued and protected as a matter of choice, rather than a natural state. At a more exacting level, these debates implicated fundamental questions of legitimacy, preference, politics, democracy, collective decision-making, and libertarian ideals.

In the early 1990s, as the Internet began to reach the masses with the advent of the World Wide Web, a particular vision of the online environment emerged to advocate and defend Internet exceptionalism. Described as digital libertarianism or cyber-libertarianism, the vision was one of freedom, liberty, and self-regulation. Cyber-libertarians believed the Internet could and would develop its own effective legal institutions through which rules would emerge. These norms would emerge from collective discourse around behavior,

---

14 Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003).

15 *See id.* at 1122, 1125 (extending § 230 immunity to defendant in claim "alleging invasion of privacy, misapproriation of the right of publicity, defamation and negligence"). *See also* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1118–19 (9th Cir. 2007) (finding that § 230 immunity extends to state-law intellectual property claims, including unfair competition, false advertising, and right of publicity).

relationship, and content, rather than from the control and regulation of network architecture. Control of architecture was seen almost exclusively as an instrument by which to enforce emerging social norms, and not as a means of determining the norms themselves. By the mid-1990s this process of self-regulation was well underway.

At the same time, however, sovereign nations and their constituents increasingly sought to impose existing offline legal regimes on this emerging, resource-rich environment. Many in the online community resisted, perceiving this regulation as a threat to the exceptional nature of the Internet. Advocates of self-regulation envisioned cyberspace as a distinct sphere, apart from physical space. These cyber-libertarian exceptionalists saw the imposition of existing offline legal systems grounded in territorially-based sovereignty as inappropriate. They believed that the online environment should instead be permitted to develop its own discrete system of legal rules and regulatory processes. Self-regulation was preferable in its own right because it had proven so effective in creating the environment sought to be preserved, and also because the alternative seemed devastating. The imposition of external, territorially-based legal regimes would be, the exceptionalists argued, infeasible, ineffective, and fundamentally damaging to the online environment.

Faced with the attempted imposition of offline legal regimes, cyber-libertarians responded by attacking the validity of exercising sovereign authority and external control over cyberspace. According to Professors David Johnson and David Post, two leading proponents of self-governance, external regulation of the online environment would be invalid because Internet exceptionalism—the state of being to which the Internet naturally evolved—destroys the link between territorially-based sovereigns and their validating principles of power, legitimacy, effect, and notice.[16] Most importantly, the Internet's decentralized architecture deprives territorially-based sovereigns of the power, or ability, to regulate online activity. Likewise, extraterritorial application of sovereign law fails to represent the consent of the governed, or to effectuate exclusivity of authority based on a relative comparison of local effects. The loss of these limiting principles results in overlapping and inconsistent regulation of the same activity with significant spillover effect. Deprived of these validating principles, it would be illegitimate to apply sovereign authority and external control in cyberspace.

---

[16] David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996).

A primary challenge to these cyber-libertarian arguments came from Professor Goldsmith, who engaged both their descriptive and normative aspects.[17] In terms of the legitimacy of sovereign regulation, Goldsmith criticized Johnson and Post's limited view of sovereignty and over-reliance on the relationship between physical proximity and territorial effects. Moreover, he argued that they had overstated the impossibility of regulation, mistaking ability for cost; failed to recognize the deterrent effect on extraterritorial actors of local enforcement against end users and network components located within the territory; and mistakenly equated valid regulation with some measure of near-perfect enforcement. Finally, where true conflicts between sovereigns existed, Goldsmith argued that these could be resolved with the same tools used in the offline world—rules of jurisdiction, conflict of laws, enforcement, *etc.* Throughout, Goldsmith struck at Johnson and Post's exceptionalist view of the Internet, implicitly rejecting the ultimate significance of both the technical and communal aspects of that ideal. This critique proved devastating to these early cyber-libertarian arguments.

The governance debate entered its second phase in 1999 with the publication of Professor Lessig's book, *Code and Other Laws of Cyberspace*.[18] Prior to Lessig's book, the governance debate had focused primarily on behavioral and property norms, with the assumption that either existing sovereign law or the law emerging from Internet self-governance would prevail. Network architecture merely provided the means to enforce these norms, particularly those emerging from self-governance. Lessig reconceived Internet exceptionalism as a two-part phenomenon, one regulatory and the other cultural. The former recognizes that many of those features that make the Internet exceptional (in the cyber-libertarian sense) are merely coding choices, and not the innate nature of cyberspace. Within the network, architecture and code are the most basic forms of regulation. Code can be easily changed. Thus, Lessig argued, to protect the cultural aspects of exceptionalism, we must first recognize the exceptional regulatory power of architecture and code within cyberspace, and its pivotal role in preserving or destroying that culture.

Lessig first pointed out that law and social norms are but two means of regulating human behavior. In cyberspace, unlike real space, it is possible for architecture to dominate regulatory structures. Architecture acts as a regulator in the offline world as well—in the form of time, nature, physics, *etc.*—but our laws and social norms are generally conceived with these regulators assumed. Alteration of that architecture is unusually difficult if not practically impossible. In cyberspace, by comparison, architecture in the form of code is remarkably

---

17 Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. Chi. L. Rev. 1199 (1998); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 Ind. J. Global Legal Stud. 475 (1998).

18 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

fluid. Code effectuates a series of choices, from data collection, to anonymity, to access. And code can be changed. Not only is code fluid, but within cyberspace it is a uniquely powerful form of regulation. Rather than regulating behavior and relationships through punishment, deterrence and post-violation corrective action, code provides the means to exercise perfect control and thus perfect regulation—regulation not just of effects, but of the very universe of choices from which an individual actor is able to select.

With this shift in focus, the debate itself evolved. Lessig cautioned that the greatest threat to the exceptional culture of cyberspace comes from the union of perfect control and market forces of commerce. The architectural components that provide the means of perfect control are held almost exclusively by private entities with commercial and political interests distinct from the collective. The invisible hand, Lessig argued, cannot resist the promise of perfect control, and has little or no motivation to protect the fundamental values promoted by cyber-libertarian exceptionalism. According to the cyber-libertarian narrative, barriers that are present in the real world do not exist or are *de minimus* in the online environment. In the context of Internet architecture, exceptionalism can be found in original principles of network design that rely on open protocols and non-discriminatory data transfer—a network that is decentralized, borderless, and with the potential for nearly unlimited data capacity. Indeed, the digital data flowing through this system is itself exceptional, because it is easy to create and manipulate, easy to copy with no degradation in quality, and easy to access and distribute. In the context of online relationships, exceptionalism resides (at the very least) in the interactivity, immediacy, and potential scope of interaction, as well as the opportunity for anonymity. However, the very promise of perfect control is to eliminate many of these choices and the fundamental values they reflect as subservient to commercial goals. In cyberspace, control over coded architecture supplies the means for making this election. Building on this assertion, Lessig argued that in order to protect fundamental values, decisions regarding architecture should emerge from the body politic and collective decision-making, rather than being concentrated in private actors.

For many cyber-libertarians, Lessig's message presented great problems. Although many had already abandoned the argument that the exercise of sovereign authority in cyberspace was normatively invalid, they had not given up (as a matter of preference) the vision of an emergent, self-governed, digital libertarian space. Sovereign legal regimes were still seen as the greatest threat to that vision. Territorial governments should, the cyber-libertarians argued, simply leave cyberspace alone to flourish. From this perspective, Lessig's arguments about the unique regulatory power of architecture and code in cyberspace were largely convincing. But his description of the corrupting influence of perfect control and concentrated private power, and particularly his

call for government regulation to counteract those influences and preserve fundamental values, were difficult to square with most libertarian views.

The debate on net neutrality provides a glimpse of this division. Many commentators, including Lessig, are concerned that the private owners that control the physical/infrastructure layer of the network will, in pursuit of cross-layer vertical integration and increased revenues, privilege certain content or applications. They therefore endorse regulatorily-mandated neutrality as a means of preserving one aspect of Internet exceptionalism. Not surprisingly, many libertarians reject this approach, endorsing instead market-based solutions for effectuating individual choice.

The irony of this debate is fairly apparent. Many who might otherwise have characterized themselves as cyber-libertarian, or at least sympathetic to that vision, are now conflicted. Net neutrality would necessarily be imposed by external sovereign legal systems and subordinated to the control of commercial entities, rather than emerging as a common norm. In the extremes, the issue seems to present a choice between entrenched political power and unregulated market forces, with neither providing adequate protection for individuals. Thus, many of the Internet exceptionalists who sought to segregate the Internet from territorial boundaries, who assumed existing sovereign governments and legal regimes were the greatest threat to the online community, who believed that the computer scientist would remain in control of the network (and thus in control of enforcement), found themselves asking Congress to protect the Internet from private actors and market forces.

## What's Left of Exceptionalism?

What then is left of Internet exceptionalism? In his revolutionary essay *A Declaration of the Independence of Cyberspace*, John Perry Barlow described cyberspace as consisting not of computers, wires, or code, but of "transactions, relationships, and thought itself."[19] It was this vision, this perception of an evolving social space, that guided Barlow's ideal of the culture he sought to preserve—a distinct vision of potential worthy of protection. Indeed, to many early inhabitants of cyberspace, communal control and regulation of network architecture appeared a given, if for no other reason than that perfect external control seemed almost impossible. Freedom of choice in individual expression, human behavior, and relationships were the heart of the online cultural and social ideal that stirred Barlow and other cyber-libertarians.

As it evolved, the governance debate fractured this largely unified vision, distinguishing validity from preference, law and social norms from architecture

---

[19] John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), **http://homes.eff.org/~barlow/Declaration-Final.html**.

and code, technical exceptionalism from cultural exceptionalism, government power from private commercial power, and even libertarian from libertarian. Lessig argued persuasively that the greatest threat to digital libertarianism arose from private actors, unbounded by fundamental values (including constitutional values) and with the ability to exercise perfect control over choice. Lessig's analysis, generally speaking, was focused on the treatment of data as data, based primarily on the identity of its owner and the commercial interests represented. Choice in action was to be controlled by the regulation of owned data, discriminatory treatment of data to the benefit of certain owners, restriction of network access, and similar means. These technical controls would then be bolstered by traditional sovereign law validating those measures.

What seems somewhat obscured in Lessig's architecture-and-code approach (which clearly remains the central concern of the governance debate) is Barlow's original vision of relational libertarianism, with its focus on expression of individual choice and the development of new communal social norms within a system of self-governance. This is the part of Internet exceptionalism that was, in a sense, overwhelmed by the debate over architecture and code. Yet there are some choices, primarily relational, that remain largely unaffected by that debate. In this sphere, the question is not access to choice, the ability to choose, or the available universe of choices, but rather what norms apply to the choices being made outside those controls.

Post argues that fundamental normative values could "best be protected by allowing the widest possible scope for uncoordinated and uncoerced individual choice among different values and among different embodiments of those values."[20] He believes that the imposition of sovereign legal regimes in cyberspace, rather than promoting fundamental values as Lessig argued, would instead deny the digital libertarian culture the opportunity to develop apart from the offline world, with its own set of fundamental values. He argues it is better to serve the private interest (even if powerful and commercially motivated) than the interest of terrestrial sovereigns. Indeed, he sees exceptionalism as requiring self-governance, to the exclusion of external legal norms imposed by sovereign powers, as a precondition to the emergence of a new system of norms.

## Section 230 as a Form of Cyber-Libertarian Exceptionalism

Most would say that Barlow and Post lost the battle. However, this particular strain of Internet exceptionalism, envisioned as self-governance and emerging social norms applicable to relationships between individuals (as opposed to data as data), has been preserved in a modified, less demanding form. Ironically, it is because of sovereign law, not in spite of it, that this occurred. The dramatic

---

20 David Post, *Against "Against Cyberanarchy*," 17 Berkeley Tech. L.J. 1365 (2002).

expansion of Section 230 immunity has effectuated many of the ideals promoted by Post, Barlow, and others, albeit on a limited scale. This expansion has created an environment in which many of the norms and regulatory mechanisms present in the offline world are effectively inapplicable. This is so not because the very nature of cyberspace makes such application impossible, or because sovereign law is necessarily ineffective or invalid, but rather because sovereign law has affirmatively created that condition.

The torts for which Section 230 provides immunity are, together with contract law, the primary means by which society defines civil wrongs actionable at law. These norms of conduct regulate relationships among individuals: articulating wrongs against the physical and psychic well-being of the person (*e.g.*, assault, battery, emotional distress), wrongs against property (e.g., trespass to land, trespass to chattels, conversion), wrongs against economic interests (e.g., fraud, tortious interference), and wrongs against reputation and privacy (e.g., defamation, misappropriation of publicity, invasion of privacy). Section 230 has been interpreted and applied to provide expansive immunity from tort liability for actions taken on or in conjunction with computer networks, including the Internet. Statutory language defining who may claim the protections of Section 230 immunity, including providers of interactive computer services and the users of such services, has been broadly extended. In contrast, the primary limitation on the range of claimants to Section 230 immunity, which is statutorily unavailable to the allegedly tortious information content provider, has been construed fairly narrowly. Moreover, the immunity provided to this expansive cross-section of online participants now reaches well beyond defamation to include a wide range of other tortious conduct and claims. As such, many of the norms of conduct regulating relationships among individuals in the offline world—those civil wrongs actionable at (tort) law—simply do not apply to many in the online world.

Even where the online entity is alleged to be aware of the illegal acts of their users, and to be either actively facilitating those illegal acts or refusing to stop them, the intermediary retains Section 230 immunity. This is true even where the intermediary has the knowledge, technical ability, and contractual right to take remedial action. In the offline world, such active and knowing facilitation would likely violate social norms established in tort law. In the online world, however, the defendants are immune from liability. Established norms, as expressed through the mechanisms of tort law, are neutralized by Section 230 and its judicial interpretations.

In the near absence of these external legal norms, at least within the range of choices being made outside the data-as-data architectural controls, the online community is free to create its own norms, its own rules of conduct, or none at all. The inhabitants may not have a blank slate—criminal law, intellectual property law, and contract law still apply—but much of what Barlow embraced

as central tenets (mind, identity, expression) remain undefined. Section 230 offers a modified version of cyber-libertarian exceptionalism, less demanding of the sovereign and existing offline social norms, and therefore less satisfying. But it is nonetheless a glimpse of that society, maintained by the sovereign legal regime rather than against it. The law now applies to nearly every tort that can be committed in cyberspace. It is nibbling at the edges of intellectual property rights. It protects against the civil liability components of criminal acts. It generally extends to all but the first speaker, who may well get lost in the network to escape liability even without immunity.

# A Case for Preserving Section 230 Immunity

As interpreted by the courts, the immunity provisions of Section 230 have been heavily criticized. Many commentators have argued that by failing to impose indirect liability on intermediaries, significant harms will go undeterred or unremedied, and that Section 230 should be reformed to serve the interests of efficiency and cost allocation. This part of the essay addresses these criticisms directly, concluding that substantially reforming the statute is both unnecessary and unwise because the cost of such liability is unreasonable in relation to the harm deterred or remedied. Indeed, given Section 230's role in facilitating the development of Web 2.0 communities, reforming the statute to narrow the grant of immunity would significantly damage the online environment—both as it exists today and as it could become.

## Evaluating Calls for Reform

Early critics of Section 230 tended to focus on the issues of congressional intent and broad interpretation by the courts. More recent commentators have moved beyond these issues to engage the larger implications of providing such sweeping immunity to online intermediaries, suggesting amendments to Section 230 intended to effectuate policies of efficiency and cost allocation. This critique begins with the premise that in the online environment, individual bad actors are often beyond the reach of domestic legal authorities. This creates a situation in which significant individual harms cannot be legally deterred or remedied, and the fear that the Internet's potential as a marketplace will not be realized. Given these negative conditions, where a third party maintains a certain level of control, the imposition of indirect liability is desirable. The failure to do so may create inefficiencies by failing to detect and deter harmful behavior where the cost of doing so is reasonable. Commentators have argued that, in the online environment, intermediaries are in the best position to deter negative behavior, to track down primary wrongdoers, and to mitigate damages. This is particularly true in regard to information-based torts, the damages of which might be mitigated in many circumstances simply by taking down, prohibiting, or blocking the objectionable content.

At the heart of this attack on Section 230 immunity is the idea that, in the absence of indirect intermediary liability, significant harms will go undeterred or unremedied. These fears are either misplaced or overstated. As an initial matter, it is not clear that a significant number of bad actors are beyond the reach of the law. Advances in technology are making it increasingly possible to locate and identify bad actors online, such that online anonymity is difficult to maintain. Likewise, where the bad actor is identified but is found outside the jurisdiction, sovereign governments have developed methods for resolving disputes to permit the direct extraterritorial application of domestic law, such as rules of jurisdiction, conflict of laws, and recognition of judgments. Indeed, anti-exceptionalists have strenuously argued that the application of sovereign authority to online activity originating outside the jurisdiction is legitimate and valid in large part because of these rules.

Moreover, although the immunity provided by Section 230 arguably mitigates the legal incentives for online intermediaries to deter and remedy certain negative behavior, it does not eliminate those legal incentives. Section 230 expressly states that it has no effect on criminal law, intellectual property law, or communications privacy law. These external norms remain applicable to and enforceable against both content providers and intermediaries in the online environment. Perhaps even more significantly, although Section 230 removes legal incentives to enforce the norms expressed in tort law, law is certainly not the only incentive for an intermediary to act. Communal, commercial and other incentives also play a role. Indeed, Section 230 immunity allows intermediaries the freedom to intervene in a multitude of ways. Thus, individual harms and marketplace security can be addressed through alternate legal regimes and internal incentives.

Furthermore, proponents of indirect intermediary liability concede that even where harms do exist, intermediaries may only rightly be held liable for failing to detect and deter harmful behavior where the cost of doing so is reasonable. It is unclear, however, that the costs of intermedial regulation are reasonable. In terms of remedies and reforms, critics generally suggest some form of the detect-deter-mitigate model, imposing a duty upon the intermediary with the potential for liability in cases of breach. The two most common models are traditional liability (damages) regimes and notice-and-takedown schemes. Proponents of traditional liability schemes generally find theoretical fault with the exceptionalist view of the Internet, and analytical fault with broad judicial interpretations of the statute that collapse distributor-with-knowledge liability into immunity from publisher liability. Proponents of a notice-and-takedown scheme likewise work from a distributor-with-knowledge model that imposes a limited duty of care on intermediaries, but generally acknowledge some degree of exceptionalism that requires a distinct scheme. Most suggest some variation

utilizing elements of the Digital Millennium Copyright Act (DMCA)[21] and the European Union's E-Commerce Directive,[22] wherein intermediary liability is triggered by actual notice of the objectionable content or a standard of reasonable care, and requiring remedial action (e.g., taking down the content at issue).

The costs of these indirect intermediary liability schemes could be great. Under traditional liability rules, intermediaries may be forced to adopt a least-common-denominator approach, resulting in overly-broad restrictions on expression and behavior. A modified distributor-with-knowledge approach, usually in the form of a takedown scheme similar to that employed by the DMCA, may produce the same type of chilling effect. This is potentially exacerbated by the use of a should-have-known standard that can trigger the need to patrol for harmful content, raising costs and leading to even greater overbreadth in application. Moreover, indirect liability reduces incentives to develop self-help technology, such as location or identity tracking software and end-user filters, the development of which was one of Section 230's primary policy goals. Thus, if the scale of undeterred or unremedied harms is minimal, and the negative impact of a detect-deter-mitigate model is significant, then the cost associated with the imposition of indirect intermediary liability is not reasonable.

## Resisting the Urge Toward Homogeny

The case for preserving Section 230 immunity begins by recasting intermediary immunity in terms of exceptionalism, self-governance and norms, because it is precisely the gap between the offline social norms expressed in tort law and the broad immunity provided to online participants that has led to the rather strong criticism of Section 230. As a conceptual matter, communal enforcement presents the greatest challenge to effectuating some modified version of the exceptionalist ideal. When external legal norms are excluded, internal enforcement mechanisms facilitate the emergence of new communal norms to take their place. Much of the criticism of Section 230 stems from the lack of legal enforcement that accompanies immunity, and the resulting inability to form new social norms to replace those of the sovereign. It is important to recognize, however, that Web 2.0 communities, such as wikis and social networks, represent a real and significant manifestation of the exceptionalist vision, because they both facilitate a market in norms and values, and provide the internal enforcement mechanisms necessary for internal norms to emerge. Section 230 plays a vital role in the development of these communities by

---

21 Digital Millenium Copyright Act, Pub. L. 105-304, 112 Stat. 2860 (1998).

22 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT**.

substantially and continually mitigating the primacy of external legal norms within the confines of the community. This permits choice, empowers the intermediary to create a market in social norms, and allows alternate forms and gradations of enforcement. The architecture of the community gives these choices form and substance, backed by an enforcement model, such that communal norms have the opportunity to develop. In this sense, Section 230 and the Web 2.0 model effectuate the emergence of a modified form of exceptionalism. The reforms proposed by most commentators would have a negative impact on these communities, with little benefit beyond those communal norms that are likely to emerge, and should be rejected.

## Exceptionalism, Self-Governance & Social Norms

Exceptionalism does not argue for the absence of social norms. Instead, exceptionalism embraces the idea of cyberspace as an environment in which the authority of external legal regimes is minimal, and where an open market in norms and values works in concert with self-governance to permit the online community to establish its own substantive social norms. Section 230 helps to effectuate a modified form of exceptionalism by moderating the imposition of external legal norms so as to permit a limited range of choices—bounded, at least, by criminal law, intellectual property law and contract law—in which the online community is free to create its own norms and rules of conduct. However, the development of social norms within this environment requires not only the ability to exercise broad individual choice among different values and embodiments of those values, but also some mechanism of communal enforcement through which to effectuate some form of self-governance.

Early proponents of exceptionalism were able to focus on relational libertarian ideals, viewing the Internet as a unique social space in which norms governing thought, expression, identity, and relationship should be permitted to evolve. This focus developed precisely because the mechanisms of enforcement required for self-governance and the evolving definition of emergent social norms were taken for granted. The architecture of enforcement was primarily controlled by a community involved in the process as adherents to the exceptionalist ideal, who could be trusted both to ensure broad individual choice and to utilize the means of enforcement as a tool of self-governance as norms emerged.

As a means of effectuating exceptionalism, the primary weakness of Section 230 is the lack of an enforcement component. Although the modified exceptionalism enabled by Section 230 permits a range of choices, it does nothing to provide enforcement mechanisms to solidify emerging communal norms. Where immunity exists, legal enforcement mechanisms are never triggered. Likewise, the architecture of enforcement relied upon by early exceptionalists is no longer communal or likely committed to the vision of a distinct cyber-libertarian space, but is instead concentrated in private

commercial entities. As a consequence, Section 230 immunity creates a gap: Certain external legal norms are excluded, but internal communal norms are often unable to coalesce to take their place. It is this gap, resulting from the lack of architectural enforcement controls, which fuels criticism of the immunity provision. In application, however, an enforcement model has emerged that mediates the tension between the broad availability of individual value choices and the ability to effectively self-govern so as to permit the development of communal norms.

## Communities of Modified Exceptionalism

Web 2.0 communities are structured as a limited commons and are built on an architecture of participation that operates as a platform for user-created content and collaboration. At the core are principles of open communication, decentralized authority, the freedom to share and re-use, and an idea of the Internet as a social forum or market for exchanging opinions and ideas in search of norms to create a culture based on sharing. Section 230 plays a vital role in the development and maintenance of these architectures by providing intermediaries with limited immunity from liability for the tortious content provided by users. Indeed, in this sense, Section 230 seems to favor the development of Web 2.0 services and the provision of user-based content over the traditional model of providing first-party institutional content.

The parallels between Web 2.0 and Barlow's vision of a communal social space are evident, albeit in modified form. Barlow embraced the potential of an environment premised upon freedom of choice in individual expression, human behavior and relationships. To achieve that potential, he and others believed that regulation by existing sovereign powers must be rejected in favor of self-governance, so that new communal social norms might have the opportunity to emerge. At the heart of this ideal was an affirmation that values participation in the market of expression, ideas and action without the constraint of preconceived value judgments. Web 2.0 promises a somewhat limited version of this environment—existing within sovereign authority, narrowed by certain enduring norms, and confined to segmented communities administered by private entities—by facilitating the market by which norms are tested.

Two of the most common models of these Web 2.0 services, wikis and social networks, are indicative of how Section 230 can effectuate the modified form of cyber-libertarian exceptionalism described above. Partly as a result of the immunity from liability provided by Section 230, these services facilitate the market in social norms by creating enclaves in which users may exercise broad (although not unbounded) individual choice among competing values. At the same time, the intermediary retains control over the architecture and thus the means of enforcement. As the market defines social good through the evolution of communal norms, that architecture may be employed as a mechanism of governance. In the absence of legal incentives, the enforcement

of communal norms is driven by internal incentives, such as the need for financial support from community donations, a communal desire for information integrity, or the need to build an audience for advertising. In some communities, participants may be incentivized by credibility and stature in the form of temporal seniority, post count, rank within the community's governing body, etc.

The online encyclopedia Wikipedia is a specific example of a Web 2.0 community of collective action. Each entry in the Wikipedia database is created and edited by volunteers who are guided by three primary principles: the Neutral Point of View policy, the No Original Research policy, and the Verifiability policy. Registered users can originate new articles, and any user, whether registered or anonymous, can edit an existing article. In the period between Wikipedia's inception in 2001 and 2010, this experiment in voluntary collaborative action produced more than ten million articles.

These activities are overseen by two levels of administrators, administrators and bureaucrats. Administrators (historically called sysops, short for system operators) have the power to edit pages, delete or undelete articles and article histories, protect pages, and block or unblock user accounts or IP addresses. Bureaucrats have the further power to create additional sysops with the approval of the community. In February 2006, in response to a series of significant and persistent acts of vandalism, the co-founder of Wikipedia created an additional layer of protection: Administrators can protect any article so that all future changes must be approved by an administrator.[23] Administrators help facilitate dispute resolution and enforcement. Low-level disputes are resolved in talk pages. Here, moderators guide members to resolution with reference to policies and guidelines developed over the life of the community. Thus, principle values and norms can lead to more specific rules. This approach works in most cases. More serious violations, such as malicious editing of an article (or vandalism), are addressed through fast-repair mechanisms executed by community members. Wikipedia administrators are also able to block user accounts or IP addresses.

As described, the Wikipedia community reflects a modified form of the exceptionalist model, initially allowing for individual choice among a range of values, facilitating a market in social norms, and providing a means of enforcement to effectuate norms as they develop. Indeed, recent studies reflect not only that norms have emerged from this market, but that those norms have solidified and expanded. Through this process, the Wikipedia community is

---

23 *See* Wikipedia, *Wikipedia: Protection Policy*, **http://en.wikipedia.org/wiki/Wikipedia:Protection_policy** (last accessed Dec. 1, 2010).

moving from an immediate focus on particular articles to more generalized concerns for quality of content and community.

Not unexpectedly, open source projects such as Wikipedia are not immune to abuse. In terms of community health, and to protect against these abuses, Wikipedia has adopted a code of conduct and principles of etiquette that stress civility and discourage personal attacks. As discussed above, these norms are enforced through an architecture that is designed to reinforce those norms with an eye towards the health of the community. At the most basic level, this occurs through routine editing by participants. Over time, more complex mechanisms for dispute resolution and enforcement have developed, such that in the past few years administrative and coordination activities have gained importance.

The relationship between architecture and social norms is fascinatingly apparent both in the Wikipedia's architectural choice to track and correlate the IP address of any anonymous user who edits the encyclopedia, as well as the development of a monitoring system that tracks those changes for analysis. This system serves as a mechanism for enforcing social norms, particularly the norm of neutrality in more controversial areas. In terms of more formal enforcement, some edits that might previously have been overlooked are now being reexamined in light of the organization from which they originated. Less formally, but perhaps even more effectively, organizations which are perceived to have breached the norms of the community have faced, and will face, recriminations. Moreover, the entire community is now aware that enforcement of those norms is now more effective, presumably creating a deterrence effect.

The Wikipedia example illuminates a constant process, as choices are narrowed by communal norms that develop and are given life through enforcement mechanisms, such that principle norms generate a breadth of more particular rules. Section 230 immunity plays an important role in this process, permitting the community to evolve and structure itself in the most efficient manner. To a limited extent, Section 230 immunity permits uncoordinated and uncoerced individual choice among different values and among different embodiments of those values. It further allows the intermediary to play an active role in facilitating the market in social norms and in creating enforcement mechanisms as a tool of self-governance. Those enforcement mechanisms can then themselves adapt. This allows not only for the development of distinct community values, but also for a means of tapping into incentives, adapting to evolving norms and conditions, and reducing costs associated with disputes. Within this framework, greater variations in community norms are possible. As communities grow, niche communities are formed at low cost. It is not the global vision of early exceptionalism, but rather a more limited and localized form of modified exceptionalism that functions as a laboratory for testing social norms and values.

## Conclusion

Critics of Section 230 have both overstated the harms arising from immunity and understated the costs of alternate schemes for imposing indirect liability on online intermediaries. At the same time, they have ignored the important role Section 230 plays in the development of online communities. The immunity provided by Section 230 helps to create the initial conditions necessary for the development of a modified form of exceptionalism by mitigating the effect of external legal norms in the online environment. Web 2.0 communities are then able to facilitate a market in norms and provide the architectural enforcement mechanisms that give emerging norms substance. Given Section 230's crucial role in this process, and the growing importance of Web 2.0 communities in which collaborative production is yielding remarkable results, reforming the statute to substantially narrow the grant of immunity is both unnecessary and unwise.

# Internet Exceptionalism Revisited

By Mark MacCarthy*

## Introduction

In the mid-1990s, commentators began debating the best way for governments to react to the development of the Internet as a global communications medium. Internet exceptionalists argued that the borderless nature of this new medium meant that the application of local law to online activities would create insoluble conflicts of law. The exceptionalists believed that as the Internet grew, reliance on local governments to set rules for the new online world would not scale well. Their alternative was the notion of cyberspace as a separate place that should be ruled by norms developed by self-governing communities of users.[1]

Critics of the exceptionalist view responded with a vision of a bordered Internet where local governments could apply local law.[2] In this view, cyberspace is not a separate place. It is simply a communications network that links real people in real communities with other people in different jurisdictions. Governments can regulate activity on this new communications network in many different ways, including by relying on the local operations of global intermediaries. Global intermediaries are the Internet service providers (ISPs), payment systems, search engines, auction sites, and other platform and application providers that provide the infrastructure necessary for Internet activity. Although they are often global in character, they also have local operations subject to local government control. According to critics of the exceptionalist view, governments have the right and the obligation to use this regulatory power over intermediaries to protect their citizens from harm.[3] Conflicts that might arise from this regulatory activity can

---

* Mark MacCarthy is Adjunct Professor in the Communications Culture and Technology Program at Georgetown University. Formerly, he was Senior Vice President for Public Policy at Visa Inc. Substantial portions of this essay were originally published as Mark MacCarthy, *What Payment Intermediaries are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L. J. 1037 (2010), available at **http://btlj.org/data/articles/25_2/1037-1120%20MacCarthy%20WEB.pdf**.

1 *See, e.g.*, David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1387-92 (1996).

2 *E.g.*, Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

3 *See id.* at 1238-39.

be resolved through the normal mechanisms governments use to resolve conflict of law questions.[4]

Governments generally followed the advice of the proponents of regulation, not the regulatory skeptics.[5] And despite some set-backs in First Amendment cases,[6] regulators have continued a steady march toward controlling the Internet by regulating intermediaries.[7] Some legal scholars argue that government reliance on intermediaries to control unlawful behavior on the Internet is justified because putting the enforcement burden on intermediaries is the least expensive way for governments to effectively assert jurisdiction.[8] The key rationale is that governments cannot easily find wrong-doers on the Internet, but intermediaries can. They are best positioned to monitor their own systems. As Mann and Belzley put it, they are the "least-cost avoider."[9]

The defenders of local government jurisdiction over the Internet often rely on historical analogies to buttress their case that local control is inevitable and desirable. Debra Spar developed the thesis that society's reaction to new technologies follows a predictable sequence of innovation, commercial exploitation, creative anarchy, and then government rules.[10] In the innovative stage a new technology is developed, in the second stage it is used in commercial ventures, in the third stage there is a tension between the anarchist impulse and the need for commercial order and stability, and in the final stage society reaches out to regulate the now mature technology to create and

---

4 *Id.* at 1200-01 (arguing that "regulation of cyberspace is feasible and legitimate from the perspective of jurisdiction and choice of law").

5 The U.S. exception is § 230 of the Telecommunications Act of 1996 which immunizes many Internet actors from liability in many contexts for the illegal activity of their users. 47 U.S.C. § 230(c) (2006).

6 *See*, *e.g.*, *Reno v. ACLU*, 521 U.S. 844, 885 (1997) ("The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship."); Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 665 (E.D. Pa. 2004) (finding that a statute requiring ISPs to block access to websites displaying child pornography violated the First Amendment).

7 *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006) (citing many examples of this trend). This Article documents further examples in which payment systems were induced by laws, regulations, pressure, and notions of corporate responsibility to take actions to control the illegal online behavior of people using their systems.

8 *See, e.g.*, Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 249-50 (2005).

9 *Id.* at 249.

10 DEBORA L. SPAR, RULING THE WAVES: CYCLES OF DISCOVERY, CHAOS, AND WEALTH FROM THE COMPASS TO THE INTERNET 11-22 (2001).

maintain the needed stability.[11] The development of radio is the standard example of this pattern. Radio's initial pioneers thought its ability to wirelessly broadcast information from one point to many made government control difficult and unnecessary.[12] But later commercial enterprises actively sought out government regulation in order to end the chaos on the airwaves that prevented broadcasters from reaching their intended audience.[13] Applying Spar's analysis here, the Internet is somewhere between stage three and stage four, where we can expect further regulation of Internet activity under the watchful eye of government. The historical example demonstrates that although every new technology is thought to be outside the jurisdiction of government, this belief usually gives way in time to the realities of government control.

In the case of the Internet, the advent of government control prompted many observers to think the Internet exceptionalists had been routed.[14] However, Internet exceptionalism is still a widely held belief,[15] and the notion that government control of cyberspace is both impossible and illegitimate still motivates much discussion of Internet policy.[16] Moreover, the initial legislative expression of Internet exceptionalism—Section 230 of the 1996 Telecommunications Act—is still on the books. This section provides a safe harbor from indirect liability for what might be called pure Internet intermediaries—those entities providing Internet access service or online

---

11 *Id.*; *see also* Mann & Belzley, *supra* note 9, at 243-44; GOLDSMITH & WU, *supra* note 7, at 124 (relying on Spar's work).

12 *See generally* SPAR, *supra* note 10, at 124-90 (describing the history of radio technology development).

13 *Id.* at 171-72.

14 *See* GOLDSMITH & WU, *supra* note 7, at 14 (asserting that "notions of a self-governing cyberspace are largely discredited").

15 *See generally* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE (David Kairys ed., 2009) [hereinafter Post, IN SEARCH OF JEFFERSON'S MOOSE ] (demonstrating an elegant take on Internet exceptionalism). The heart of the response to Goldsmith is that scale matters and that while it is physically possible and permissible under current "settled" law of cross-border jurisprudence, it is not "workable" to subject all websites to perhaps hundreds of different and possibly conflicting jurisdictions. *See* David G. Post, *Against "Against Cyberanarchy"*, 17 BERKELEY TECH. L.J. 1365, 1384 (2002) [hereinafter Post, *Against "Against Cyberanarchy"*].

16 *See* H. Brian Holland, *supra* (adapted from H. Brian Holland,*In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 U. KAN. L. REV. 369, 397 (2007)). Holland's version of modified exceptionalism is closely connected with the legal principle that online intermediaries are not liable for third party conduct. He asserts that the immunity from liability created by § 230 of the Communications Decency Act "helps to effectuate a modified form of exceptionalism by moderating the imposition of external legal norms so as to permit a limited range of choices—bounded, at least, by criminal law, intellectual property law and contract law—in which the online community is free to create its own norms and rules of conduct." *Id.* at 397.

services.[17] Despite a growing call to revisit this immunity,[18] it has been extended several times. The Internet gambling law, which creates liability for traditional intermediaries such as payment systems, contains a limitation on liability for pure Internet intermediaries.[19] Similarly, the recently passed online pharmacy law exempts pure Internet intermediaries from a general duty to avoid aiding or abetting unauthorized Internet sales of controlled substances.[20] The adoption of these provisions in recent laws might be merely § 230 on automatic pilot, but more likely, some version of Internet exceptionalism is at work in these legislative distinctions.

A recent speech by the Obama Administration's senior communications policymaker, Lawrence Strickling, provides further evidence of the continuing relevance of the Internet exceptionalist perspective.[21] In defending Section 230's limitation on liability, Assistant Secretary Strickling argued:

> This limitation on liability has enabled the creation of innovative services such as eBay and YouTube, which host content provided by others, without requiring that those services monitor every single piece of content available on their sites. Absent this protection against liability, it is hard to imagine that these services would have been as successful as they turned out to be.[22]

Internet exceptionalism is the view that the normal rules that apply to real-world providers of goods and services should not apply to online entities. Secretary Strickling argues for this view on policy grounds. Without it, he asserts, the innovative character of the Internet would come to a halt. The next

---

17 47 U.S.C. § 230(c)(1) (2006) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."). The interpretation of this provision is quite broad. *See*, *e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 330-31 (4th Cir. 1997) (finding that plaintiff's tort claims of defamation were preempted by § 230). The immunity does not extend to criminal law, contract law, or intellectual property law. 47 U.S.C. § 230(e)(1)-(4) (2006).

18 *See, e.g.*, Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 U. CHI. SUP. CT. ECON. REV. 221 (2006), John Palfrey and Urs Gasser, BORN DIGITAL 106 (2008), and Daniel Solove, THE FUTURE OF REPUTATION 125-160 (2007).

19 31 U.S.C. § 5365(c) (2006).

20 Ryan Haight Online Pharmacy Consumer Protection Act of 2008, Pub. L. No. 110-425, § (h)(3)(A)(iii), 122 Stat. 4829-30.

21 Remarks by Lawrence Strickling, Assistant Secretary of Commerce for Communications and Information, to Internet Society's INET Series: *Internet 2020: The Next Billion Users April 29, 2010 available at*
**http://www.ntia.doc.gov/presentations/2010/InternetSociety_04292010.html**

22 *Id.*

YouTube or Google could never emerge because the legal liabilities associated with running such a new business would strangle it.

If the Internet exceptionalists rested their case on the literal impossibility of extending local law to cyberspace then there is not much left to their argument. A "bordered Internet" where intermediaries try to control behavior prohibited by local law is becoming a reality. Most Internet intermediaries have explicit policies that prohibit illegal activities.[23] These general policies are supplemented with specific policies and procedures designed to prevent the use of these systems for specific illegal activities.

Moreover, it is not just voluntary efforts by Internet intermediaries that show how Internet activity can be controlled. Governments have been effectively extending their control over Internet activity through imposing obligations on intermediaries. It has been estimated that at least 26 countries impose some kind of filtering obligations on Internet entities.[24] Recent government actions in France and the United Kingdom impose "graduated response" obligations on ISPs, requiring them to cut off Internet access for alleged repeat copyright violators.[25] It is possible to challenge these extensions of government power

---

23 Participants in Google's advertising programs "shall not, and shall not authorize any party to … advertise anything illegal or engage in any illegal or fraudulent business practice." Google Inc. Advertising Program Terms ¶ 4 (Aug. 22, 2006), *available at* **https://adwords.google.com/select/tsandcsfinder**. MasterCard has rules for both merchants and their acquiring banks: "A Merchant must not submit for payment into interchange … and an Acquirer must not accept from a Merchant for submission into interchange, any Transaction that is illegal." MASTERCARD, MASTERCARD RULES 5.9.7 (2008), *available at* **http://www.merchantcouncil.org/merchant-account/downloads/mastercard/MasterCard_Rules_5_08.pdf**. MasterCard prohibits its issuing banks from engaging in illegal transactions. *Id.* at 3.8.4. Visa has similar rules, for example: "A Merchant Agreement must specify that a Merchant must not knowingly submit, and an Acquirer must not knowingly accept from a Merchant, for submission into the Visa payment system, any Transaction that is illegal or that the Merchant should have known was illegal." VISA, VISA INTERNATIONAL OPERATING REGULATIONS § 4.1.B.1.c (2008), *available at* **http://usa.visa.com/download/merchants/visa-international-operating-regulations.pdf**. Visa's regulations also specify acquirer penalties for merchants engaging in illegal cross-border transactions. *Id.* § 1.6.D.16.

24 RONALD DEIBERT, JOHN PALFREY, RAFAL ROHOZINSKI, JONATHAN ZITTRAIN, ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 1 (2008).

25 Eric Pfanner, *U.K. Approves Crackdown on Internet Pirates*, NEW YORK TIMES, April 8, 2010 at **http://www.nytimes.com/2010/04/09/technology/09piracy.html?scp=1&sq=digital%20economy%20bill%20uk&st=cse**. Eric Pfanner, *France Approves Wide Crackdown on Net Piracy*, NEW YORK TIMES, October 22, 2009, **http://www.nytimes.com/2009/10/23/technology/23net.html?_r=1**. Sometimes the ISPs cooperate in a graduated response policy to settle legal claims. For a review of government and private sector efforts to control online copyright violations, *see* Christina Angelopoulos, *Filtering the Internet for Copyrighted Content in Europe*, IRIS PLUS, March 2009 available at **http://www.obs.coe.int/oea_publ/iris/iris_plus/iplus4_2009.pdf.en**

over Internet activity as unwise, or as a violation of a human right to Internet access or as too costly. But it is no longer plausible to maintain that they are simply impossible.

This conclusion is discussed at length in another essay in this collection that focuses on the traditional payment intermediaries, payment card companies such as Visa, MasterCard, and American Express, as an instructive category of intermediary platforms.[26] Developments over the last several years conclusively demonstrate that these payment intermediaries can control specific illegal activities on the Internet and governments can extend their control to these payment intermediaries.

Thus, the debate over Internet exceptionalism has shifted from the "nature" of the Internet as something intrinsically beyond the control of governments to a problem of choice.[27] Intermediaries can control illegal behavior on the Internet and governments can control intermediaries, but *should* they? And if government should exert control over intermediaries in order to control Internet activities, how should the global legal order be restructured to accommodate their role?

This essay explores the extent to which the experience of payment systems in controlling the illegal online behavior of their users illuminates the debate among the Internet exceptionalists, defenders of the bordered Internet, and the internationalists. It concludes that exceptionalism, in either its original or modified forms, is not the right framework for Internet governance because intermediaries should not defer to the judgments of self-governing communities of Internet users when the judgments conflict with local law. The exceptionalists are correct that a "bordered Internet" will not scale up, but the experience of traditional payment systems points towards international harmonization. If governments are going to use intermediaries to regulate the Internet, they need to coordinate their own laws to make that role possible.

The essay addresses each of the three main approaches to Internet governance: exceptionalism, the bordered Internet, and internationalism. The first section, on exceptionalism, begins with a discussion of the original Internet exceptionalist perspective, which viewed government regulation of the Internet as infeasible and normatively less desirable than government deference to the rules developed by self-governing Internet communities. This is followed by a discussion of Brian Holland's revised version of exceptionalism. Under this approach, the various immunities from intermediary liability established by local jurisdictions enable the development of autonomous Internet norms. Both versions are shown to have significant limitations when viewed in light of

---

26 *See* MacCarthy, *Online Liability for Payment Systems*, *infra* at 230.

27 *See* Holland, *supra* note 16, at 376-77 ("In this context, exceptionalism became an objective to be pursued and protected as a matter of choice, rather than a natural state.").

payment system experiences. The next section explores the "bordered Internet," the idea that in certain cases local governments may properly and unilaterally extend their jurisdiction over Internet activities through intermediaries. Payment intermediaries use standard measures to resolve conflicts of law and follow a practical rule that treats a transaction as illegal if it is illegal in the jurisdiction of either the merchant or the cardholder. This section then discusses limitations on this method of resolving cross-border jurisdictional conflicts. The final section concludes with a discussion and endorsement of the internationalist perspective, according to which local governments should only exercise control over specific Internet activities in a coordinated fashion.

## Internet Exceptionalism: The Original Version

In February 1996, John Perry Barlow identified Internet exceptionalism when he declared cyberspace to be independent of national governments, roughly on the grounds that cyberspace "does not lie within your borders" and that it "is a world that is both everywhere and nowhere, but it is not where bodies live."[28] Conflicts in cyberspace would be resolved not with the territorially-based "legal concepts of property, expression, identity, movement, and context," which "do not apply," to cyberspace because they "are all based on matter, and there is no matter here."[29] Rather, in cyberspace "governance will arise according to the conditions of our world, not yours."[30] Cyberspace "is different."[31]

Almost concurrently, legal scholars David Johnson and David Post made a similar case for Internet exceptionalism.[32] In their view, the Internet destroys "the link between geographical location" and "the *power* of local governments to assert control over online behavior; [and] … the *legitimacy* of a local sovereign's efforts to regulate global phenomena …."[33] The Internet destroys the power of local governments because they cannot control the flow of electrons across their physical boundaries. If they attempted to do so, determined users would just route around the barriers. Moreover, if one jurisdiction could assert control over Internet transactions, all jurisdictions could, resulting in the impossibility

---

28 Declaration of John P. Barlow, Cognitive Dissident, Co-Founder, Elec. Frontier Found., *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), *available at* **http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration**.

29 *Id.*

30 *Id.*

31 *Id.*

32 *See generally* Johnson & Post, *supra* note 1.

33 *Id.* at 1370 (emphasis added).

that all "Web-based activity, in this view, must be subject simultaneously to the laws of all territorial sovereigns."[34] The Internet destroys the legitimacy of local jurisdiction because legitimacy depends on the consent of the governed and "[t]here is no geographically localized set of constituents with a stronger and more legitimate claim to regulate it than any other local group. The strongest claim to control comes from the participants themselves, and they could be anywhere."[35] Since "events on the Net occur everywhere but nowhere in particular … no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws."[36]

Behind these arguments seemed to be an appealing political vision. The ideal envisaged self-organizing groups of people making the rules that applied to their conduct. These rules would not be imposed from the outside, but would be freely chosen by the active participation of the community members. The key was deliberation by free, rational agents in their communities, not imposition of rules by an arbitrary act of will by a distant sovereign. This ideal of participatory democracy was intended, in part, to offset the alienating effects of large-scale modern democracies, which in practice had long failed to provide their members with the sense of community participation that alone seemed to justify the imposition of collective rules.

The way this vision would be implemented on the Internet would be through the development of autonomous communities of Internet users. These Internet communities were largely isolated from "real world" communities. Since it took special care and effort to reach out to participate in them, only those people who really wanted to participate would, and the effects of activities in those communities would be limited to those who chose to participate. Given the structure of the Internet as a communications network, which moved almost all major decisions on content to the edges of the network, a diversity of law could arise in cyberspace as each community developed its own norms for regulating the conduct of its members. People would be free to participate in the communities they wanted, but could easily avoid those they did not like. Enforcement of the community rules would be accomplished through peer pressure, reputational systems, informal dispute resolution mechanisms, and ultimately, banishment. The system as a whole would evolve through a process analogous to biological evolution, where diverse and potentially competing rule sets as embodied in different communities would vie for acceptance in a free marketplace of rules.

---

34 *Id.* at 1374.

35 *Id.* at 1375.

36 *Id.* at 1376.

Internet exceptionalism is thus the view that activity on the Internet should be regulated by Internet community norms, not laws of territorial jurisdictions or globally harmonized laws.[37] It is hard to avoid the sense that the political vision pre-dated the Internet—that the feasibility argument masked the underlying vision and the arrival of the Internet simply created the possibility of implementing the vision in a way that the "real" world did not. To see this, imagine the reaction of Internet exceptionalists to the idea of a world government that would establish uniform global laws. This would eliminate the conflict of law problem. But exceptionalists are even more appalled at the idea of world government control over the Internet than with the idea of nation-state control over it. This suggests that the issue is not feasibility of control, but the value of participative community decision making and diversity.

This early cyber libertarian vision was immediately attacked by those who defended the feasibility and legitimacy of extending local laws to cover Internet activity.[38] As they note, "[t]he mistake here is the belief that governments regulate only through direct sanctioning of individuals…. Governments can … impose liability on intermediaries like Internet service providers or credit card companies."[39] Government action against these intermediaries "makes it harder for local users to obtain content from, or transact with, the law-evading content providers abroad. In this way, governments affect Internet flows within their borders even though they originate abroad and cannot easily be stopped at the border."[40] And these efforts to bring order to the Internet through pressure on intermediaries are often legitimate because they provide "something invisible but essential: public goods like criminal law, property rights, and contract enforcement … that can usually be provided only by governments." [41]

The debate took an interesting twist through the work of Larry Lessig. A key element of the early exceptionalist framework was the idea that the Internet had

---

37 Mann and Belzley describe their view as "consciously exceptionalist" because "specific characteristics of the Internet make intermediary liability relatively more attractive than it has been in traditional offline contexts because of the ease of identifying intermediaries, the relative ease of intermediary monitoring of end users, and the relative difficulty of directly regulating the conduct of end users." Mann & Belzley, *supra* note 9, at 250-51. But this is an odd way of framing the issue. Internet exceptionalism is not simply the view that the Internet should be treated differently from the offline world. The claim is more specifically that the Internet should be free of local jurisdictions. Mann and Belzley's view, which implies that the Internet should be brought under local jurisdictions through the mechanism of intermediary liability, is thus the very opposite of exceptionalism. It is one version of Internet non-exceptionalism.

38 *See generally* Goldsmith, *supra* note 4 (challenging the regulation skeptics).

39 Goldsmith, *supra* note 4, at 1238.

40 GOLDSMITH & WU, *supra* note 7, at 68.

41 *Id.* at 140.

a fundamental nature, which governments did not control, could not alter, and which effectively prevented them from imposing local rules. In his influential book, *Code and Other Laws of Cyberspace*,Lessig took aim at this idea. [42] He pointed out that computer systems, software applications, and communications networks were human creations and that the choices of the architects of these systems were embodied in the code that made it possible for these systems to run. Far from being a natural object, these systems were subject to the decisions of the parties (usually non-governmental entities) that had the right and the ability to create, maintain and alter them.

The initial openness and transparency of the Internet was therefore something that could not be assumed as a fact of nature, but something that needed to be maintained against possible opponents. But unlike the early cyber libertarians, Lessig did not focus on the dangers that local governments might try to control choices by controlling code. He thought the openness of the Internet had to be maintained against the interests of non-governmental parties seeking to advance their own strategic interests. Lessig's initial private sector targets were the network carriers who were seeking to alter the "end-to-end" design of the network in order to pursue their own strategic interests at the expense of application providers, service providers and end users who relied on the neutrality of the Internet to conduct their ordinary activities. In this way, the Internet exceptionalist debate merged with the net neutrality debate and the original defenders of exceptionalism seemed to be faced with the (to them) unattractive dilemma of using local governments to promote Internet values of openness or allowing their Internet choices to be dictated by unaccountable private entities that controlled the fundamental architecture of the Internet.[43]

This attack was so effective that many believe that these notions of a "self-governing cyberspace are largely discredited."[44] But modified versions accept the basic premise that the Internet should be free of local regulation and governed instead by its users. One version of the revived exceptionalism, defended by Brian Holland, focuses on Web 2.0 communities.[45] This view

---

42 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

43 *See* Holland, *supra* note 16 at 108-119 for a summary of this way of connecting the Internet exceptionalist debate with the net neutrality debate.

44 *Id.* at 14.

45 Holland writes:

> By mitigating the imposition of certain external legal norms in the online environment, § 230 helps to create the initial conditions necessary for the development of a modified form of exceptionalism. With the impact of external norms diminished, Web 2.0 communities, such as wikis and social networks, have emerged to facilitate a limited market in norms and values and to provide internal enforcement mechanisms that allow new communal norms to emerge.

argues that together with the immunity provisions of Section 230 of Communications Decency Act, these communities have the potential to allow internal community norms to take the place of external territorially based laws.[46]

## Critique of Internet Exceptionalism

The experience of global payment intermediaries described in a companion article in this volume confirms the view that intermediaries *can* effectively control illegal activity in cyberspace. This still leaves the question of whether intermediaries *should* resist governmental pressure to control the behavior of their users. As a general matter, they should not defer to the judgments of self-governing communities of Internet users when these judgments conflict with local law. As corporate citizens, they have an obligation to obey the laws of the jurisdictions in which they operate, and they simply have no basis to excuse themselves from that duty in order to let online communities determine their own fate. But even when local law does not require them to take action against illegal behavior, their responsibility to keep their systems free of illegal activity means that they often should take specific steps to stop these activities.

The fundamental objection, even to Holland's modified exceptionalism, is that the "law" of Internet communities is not really the law of that community. It is a commercial contract enforceable under the rules of some local jurisdiction, and the terms of the contract are subject to the same kinds of legal and regulatory oversight that bind contracts between people in local jurisdictions. Deferring to these contracts does not usually mean democratic community self-government. Local regulations are needed to fully protect the members of these communities.[47] Moreover, in some cases, the legal discretion granted to intermediaries to control the conduct of their members may be too broad and should be limited by replacing intermediary judgment with public authority decisions. The remainder of this section develops these points.

Even if Internet communities could substantially exclude a significant portion of external legal norms, it still does not follow that internal norms will necessarily emerge from the process of debate and deliberation that Holland envisages. As Holland notes, "external legal norms are excluded, but internal communal norms are often unable to coalesce to take their place" because enforcement is "concentrated in private commercial entities."[48] The hope of his modified Internet exceptionalism is that the intermediaries who control the new Web 2.0 platforms will be driven by internal incentives to accommodate the

---

Holland, *supra* note 16, at 369.

46 *Id.*

47 This Section focuses on competition policy, privacy, and consumer protection as examples.

48 Holland, *supra* note 16, at 398.

wishes of the online communities they create, allowing users to establish norms for their own communities.[49]

But it is not clear that Web 2.0 platforms are likely to grant this kind of democratic self-governance. For example, intermediaries can be subject to pressure. Craig Newmark, the operator of Craigslist, has insisted that he made his decision to remove ads for erotic services as a result of consultation with his online community.[50] But it is also true that Craigslist was under criminal investigation by a number of state attorneys general for violation of state laws against prostitution.[51] One could argue immunity in this case, but Craigslist did not.[52] It complied with a law enforcement request to remove certain postings and the decision to remove these ads will be subject to ongoing oversight by these law enforcement agencies.[53] However, the question remained whether or not Craigslist would take the legal risk if the community voted to keep these ads in place.

These communities are not typically governed by democratic voting procedures that guarantee the consent of the governed. They are governed by contractual terms of service. Often prospective members of these communities have a simple take-it-or-leave-it choice when they decide to join.[54]

---

49 These internal incentives include "the need for financial support from community donations, a communal desire for information integrity, or the need to build an audience for advertising." *Id.* at 400; *see also* Matthew Schruers, *Note: The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 261 ("ISPs respond to content-based complaints as a matter of good business practice for the purpose of maintaining customer goodwill and satisfaction.").

50 *Craigslist Founder Seeks Larger DC Role*, NAT'L J., June 2, 2009, available at **http://techdailydose.nationaljournal.com/2009/06/craigslist-founder-seeks-large.php** (reporting Craig Newmark's comments to the Computers Freedom and Privacy Conference).

51 *See* Brad Stone, *Craigslist to Remove 'Erotic' Ads*, N.Y. TIMES, May 14, 2009, at B1. Craigslist's attorneys asserted immunity under § 230, but chose voluntarily to remove the ads to which various state attorneys general had objected. *Id.* State Attorneys General felt confident that they could bring a case under state criminal law despite the immunity granted by § 230. *Id.* The case was given national attention when a medical student was accused of killing a masseuse whom he met through Craigslist. *Id.*

52 *Id.*

53 *Id.*

54 *See* Johnson & Post, *supra* note 1, at 1380 (describing AOL and Compuserve terms of service as examples of law in cyberspace). Johnson & Post view the rules for an Internet community to be "a matter for principled discussion, not an act of will by whoever has control of the power switch." *Id.* But it is hard to see how terms of service for a typical Internet service or application is anything other than an act of will by the person who controls the service or application. It might satisfy certain legal standards for informed consent, but it is not the product of principled discussion. And this might be the way consumers want it. Online

If consumers do not like the terms of service, then protest can be effective, as in the recent case of users objecting to the change in terms of service unilaterally offered by Facebook. By threatening the privacy rights of the community, the platform stirred up substantial community unrest, and ultimately the new terms of service were withdrawn.[55] But this exit right is not the same as democratic self-governance, and it is not always effective. What if Facebook had not responded to community objections? Would people actually have left, and where would they have gone? Lock-in is a real restriction in social networks.

The exemption from liability based on Section 230 does not mean that online entities are exempt from local law. Often, local law is needed to protect consumers from the actions of Internet intermediaries. Regulation of online communities by governments seems especially timely and urgent in three areas: competition policy, privacy, and consumer protection.

With respect to competition, concentration in particular sectors of the online world should be examined because it can so significantly reduce consumer choice. The Department of Justice has indicated, for example, that it is going to take a more active approach in this area.[56] Along with the Federal Trade

---

communities might not offer to determine their online laws through a political process because the members of the community cannot be bothered. People visit many different websites and use many different web services. It is hard to believe that they want full democratic participation rights to set up the rules for each of these services. And it is implausible that they would actually spend the time, if they were offered the opportunity. The example of privacy policies makes the point. A recent study concluded that if all U.S. consumers read all the privacy policies for all the web sites they visited just once a year, the total amount of time spent on just reading the policies would be 53.8 billion hours per year and the cost to the economy of the time spent doing this would be $781 billion per year. Aleecia M. McDonald & Lorrie F. Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 565 (2008).

55 N.Y. Times, *Facebook, Inc.*, **http://topics.nytimes.com/top/news/business/companies/facebook_inc/index.html?8qa&scp=1-spot&sq=facebook&st=nyt** (last updated May 27, 2009). In 2007, the company had created a community backlash when it introduced an advertising service that allowed a user's online activities to be distributed to other community members. Epic.org: Electronic Privacy Information Center, Social Networking Privacy, **http://epic.org/privacy/socialnet/default.html** (last visited Feb. 3, 2009). In the face of this protest, it provided a simple way for users to decline to participate. *Id.* In February 2009, it proposed new privacy rules according to which users will own and control their own information, and in April it allowed a vote of its users on these new principles. Over 75% of those voting endorse them, and on July 1, 2009 it adopted them. *Id.*

56 Press Release, U.S. Dep't of Justice, Justice Department Withdraws Report on Antitrust Monopoly Law: Antitrust Division to Apply More Rigorous Standard with Focus on the Impact of Exclusionary Conduct on Consumers (May 11, 2009), *available at* **http://www.justice.gov/atr/public/press_releases/2009/245710.pdf**.

Commission (FTC), they have initiated inquiries focused on the search engine market.[57]

Privacy and security rules need to be defined as well. The FTC has taken major action in this area, and is stepping up its enforcement.[58] They are also focusing on the development of a new privacy framework to analyze the basis for the harms associated with privacy violations.[59] Furthermore, the FTC has focused on developing rules for online behavioral advertising.[60] In addition, rules governing privacy for online cloud computing services need to be clarified, perhaps by additional legislation.[61]

Consumer protection rules should be updated to apply more effectively to new developments in electronic commerce including the growth of mobile commerce and user-generated content, the greater availability of digital goods online, and increased numbers of consumers acting as online sellers, and new developments in accountability and payment protection. A timely development might be the harmonization of consumer redress and liability rights across various payment mechanisms.[62]

Finally, the discretion given to Internet intermediaries over which transactions to allow must be subject to public scrutiny. Today, intermediaries exercise

---

57 *See, e.g.*, Miguel Helft, *U.S. Inquiry Is Confirmed into Google Books Deal*, N.Y. TIMES, July 3, 2009, at B3; Miguel Helft & Brad Stone, *Board Ties at Apple and Google Scrutinized*, N.Y. TIMES, May 5, 2009, at B1; Peter Whoriskey, *Google Ad Deal Is Under Scrutiny: Yahoo Agreement Subject of Antitrust Probe, Sources Say*, WASH. POST, July 2, 2008, at D1.

58 *See* Press Release, Fed. Trade Comm'n, Sears Settles FTC Charges Regarding Tracking Software (June 4, 2009), *available at* **http://www.ftc.gov/opa/2009/06/sears.shtm** (reporting that in the Sears case the FTC obtained a settlement from Sears after charging that their consent practices in regard to installing an online tracking program on customers' computers constituted an unfair or deceptive practice).

59 *See* Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 5, 2009, at B1 (stating that David Vladeck, the new head of the FTC's consumer protection division, is rethinking privacy). Vladeck said that "[t]he frameworks that we've been using historically for privacy are no longer sufficient." *Id.* In his view the FTC will begin to consider not just whether companies caused monetary harm, but whether they violated consumers' dignity because, for example, "[t]here's a huge dignity interest wrapped up in having somebody looking at your financial records when they have no business doing that." *Id.*

60 *See* Press Release, Fed. Trade Comm'n, FTC Staff Revises Online Behavioral Advertising Principles (Feb. 13, 2009), *available at* **http://www.ftc.gov/opa/2009/02/behavad.shtm**.

61 *See generally* ROBERT GELLMAN, WORLD PRIVACY FORUM, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING (2009) (discussing these cloud computing issues).

62 Legal payment protections now differ depending on the type of payment product used (debit or credit) and the nature of the payment provider—traditional payment providers like Visa face legal requirements while new payment providers such as cell phone companies do not.

judgment over which transactions are subject to such legal risk that they cannot be allowed. These decisions are made in the context of the business interests and technological capabilities of the intermediaries themselves, but they have important effects on the rights and interests of other parties. Some examples, explained in a companion essay in this volume, include:

- Payment systems effectively decide which Internet gambling transactions are illegal. By choosing to block all coded gambling transactions, the system disadvantages horseracing, state lottery, and Indian gaming transactions that are arguably legal.
- Payment systems take complaints from third parties, make an independent legal assessment of the merits of the case, and withdraw service based on these assessments. In effect, they adjudicate these copyright cases.

These decisions are sound and sensible ways to balance complex and competing interests. However, they are private sector judgments, inevitably subjective and influenced by the particular interests of the parties involved.

Other intermediaries also have enforcement abilities that they can use at their own discretion. For instance, in June 2009, it was reported that a British ISP had agreed to disconnect subscribers who were accused of three instances of infringement by a copyright owner.[63] Allegations of violations would be made by a contractor working for the content owner and transmitted to the ISP.[64] At this point, these decisions are largely up to the payment intermediaries and the ISPs themselves, although in some jurisdictions they are dictated by government requirements,[65] yet their decisions will have profound effects on the shape and

---

63 *See, e.g.*, Danny O'Brien, *Irish ISP Agrees to Three Strikes Against Its Customers*, DEEPLINKS BLOG, **http://www.eff.org/deeplinks/2009/01/irish-isp-agrees-three-strikes-against-its-users** (Jan. 28, 2009).

64 Under the agreement the music labels, instead of going to court to get an order to have the ISP shut off a subscriber's connection, provide evidence of infringement to the ISP directly. *Id.* As O'Brien noted,

> The difference is that an ISP is not a court; and its customers will never have a chance to defend themselves against the recording industry's accusations and "proof." To whom, without judicial oversight, has the ISP obligated itself to provide meaningful due process and to ensure that the standard of proof has been met?

*Id.*

65 The movement toward graduated response would replace this discretion with government processes. Under the recently passed Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet" (High Authority of Diffusion of the Art Works and Protection of the (Copy)Rights on Internet) ("HADOPI") law, French ISPs would be required to suspend Internet access for subscribers who have been subject to three allegations of copyright violations. Catherine Saez, *French HADOPI Law, Now Complete, Can Brandish Its Weapons*, INTELL. PROP. WATCH, Oct. 23, 2009, **http://www.ip-**

direction of electronic commerce. Deferring to the norms of the Internet community in this context means deferring to these private judgments by intermediaries.

There is a role for Internet community decision-making. The best circumstances for deference to law constructed for and by particular Internet communities is when an Internet community's norms do not "fundamentally impinge upon the vital interests of others who never visit this new space."[66] To the extent that an Internet community is self-contained or its activities affect others only on a voluntary basis, then there is a case for deferring.[67]

## Payment Systems & the Bordered Internet

Goldsmith and Wu attack Internet exceptionalism, but they also construct a positive vision of a "bordered Internet."[68] This world would work pretty much as the world worked before the Internet. New regulations would be crafted to deal with the new dangers specifically created by the Internet, but there would be no fundamental need to adjust the basic domestic or international framework.[69]

---

**watch.org/weblog/2009/10/23/french-hadopi-law-now-complete-can-brandish-its-weapons/**. A court review would be required before suspension. *Id.* A similar graduated response program was adopted in Britain in April 2010. See Eric Pfanner, *U.K. Approves Crackdown on Internet Pirates*, NEW YORK TIMES, April 8, 2010, *available at* **http://www.nytimes.com/2010/04/09/technology/09piracy.html**. Whether these graduated response programs are needed is a point of controversy, but they replace ISP discretion with a system of public accountability.

66 Johnson & Post, *supra* note 1, at 1389.

67 *See* POST, IN SEARCH OF JEFFERSON'S MOOSE, *supra* note 15, at 178-86 (describing "massively multi-player online games" or MMOGS as good candidates for this effort at online rule creation). This might be. However, Linden Labs, the creator of Second Life, one of the most famous MMOGs, found it necessary to rely on external banking regulators when it decided to ban the offering of interest or any return on investment in-world without proof of an applicable government registration statement or financial institution charter. Kend Linden, *New Policy Regarding In-World "Banks"*, SECOND LIFE BLOGS, Jan. 8, 2008 06:43:56 PM, **https://blogs.secondlife.com/community/features/blog/2008/01/08/new-policy-regarding-in-world-banks**. Linden Labs properly concluded that it "isn't, and can't start acting as, a banking regulator." *Id.* New rule-making institutions will emerge only if people think that they are real. For this reason, a policy to defer in certain cases should be public and stable in order to provide the opportunity for the development of alternative rules.

68 GOLDSMITH & WU, *supra* note 7, at viii.

69 *Id.* at 149.

Jurisdictional disputes would be one significant problem with the bordered Internet. The initial Internet exceptionalist argument was that Internet activity is simultaneously present in multiple overlapping and inconsistent jurisdictions, and that no one jurisdiction has a better claim to regulate the activity than any other jurisdiction. It would be better to think of the activity as taking place in a separate jurisdiction altogether and have the territorial governments of the world defer to the community norms created there. Goldsmith and Wu's response was that Internet activity was real world activity, taking place in particular jurisdictions, and that local governments could exert control over this activity by attaching obligations to the local operations of global Internet intermediaries.[70] This indirect liability for intermediaries would make it easier to extend local law to the bad actor.[71] Conflict of laws would be handled by the normal mechanisms for resolving these disputes, and ultimately enforced by actions taken against local operations of global intermediaries.[72]

Jurisdiction in cyberspace is a complex topic with many different approaches to assigning both the applicable law and the court of jurisdiction.[73] Questions include determining the location of the transaction, the jurisdiction, and the interests of the parties.[74] An early attempt to deal with these issues in the Internet context was the FTC's approach to consumer protection in the global marketplace.[75] The simplest cross-border electronic transaction implicates transnational concerns. Choice of law debates inevitably follow. The FTC considered arguments for the "country of origin" approach and the "country of destination" approach.[76] Under the country of origin approach, the law of the

---

70 *Id.* at 68-72.

71 Mann & Belzley, *supra* note 9, at 259 ("[On the Internet it is] easier for even solvent malfeasors engaged in high-volume conduct to avoid responsibility either through anonymity or through relocation to a jurisdiction outside the influence of concerned policymakers."). Mann and Belzley also argue that indirect liability makes sense in "cases in which the retailer is located in a jurisdiction outside the United States that will not cooperate with the relevant state regulators." *Id.* at 277.

72 GOLDSMITH & WU, *supra* note 7, at 158-61.

73 *See, e.g.*, Paul S. Berman, *Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era*, 153 U. PA. L. REV. 1819, 1822 (2005) (arguing that judges should adopt a cosmopolitan approach in Internet cases involving choice of law and foreign judgment issues, grounded in the "idea that governments have an interest not only in helping in-state litigants win the particular litigation at issue, but a more important long-term interest in being cooperative members of an international system and sharing in its reciprocal benefits and burdens").

74 *See generally* Goldsmith, *supra* note 4 (discussing many of these theories); *see also* Berman, *supra* note 73, at 1839-40 (discussing various choice-of-law theories that address these questions).

75 FED. TRADE COMM'N, CONSUMER PROTECTION IN THE GLOBAL ELECTRONIC MARKETPLACE: LOOKING AHEAD (2000). The FTC's discussion of applicable law and jurisdiction is especially relevant. *Id.* at 4-11.

76 *Id.*

merchant would apply and the courts of the merchant's country would adjudicate any disputes.[77] Under the country of destination approach, the law of the consumer would apply and the courts of the consumer's country would adjudicate disputes.[78]

The defense of the country of origin approach relied on the difficulty of applying any other legal framework to the electronic marketplace.[79] Only this country of origin framework seems to allow for the growth of global e-commerce. The framework considers problems encountered by small businesses selling in many countries of creating and applying a standard for some variety of "purposeful" targeting. Creating a default rule of the country of origin was deemed to better provide needed uniformity and predictability for online businesses.

This approach has defects. First, it forces consumers to rely on unfamiliar consumer protections. If merchants cannot be expected to know the laws of 180 countries, neither can consumers. Second, it creates a "race to the bottom," whereby unscrupulous merchants can simply locate in a country with weak consumer protections. Third, consumers cannot reasonably be expected to travel to the country of origin to obtain redress. Fourth, consumers could not rely on their own consumer protection agencies for redress either, since these agencies would also be unable to enforce the consumer's home jurisdiction protections.

So neither default rule seemed to suffice. As a practical matter, consumer education, self-regulatory efforts, and the development of codes of conduct by multinational organizations were the means chosen to address the cross–border consumer protection issue.[80] For other issues that could not be addressed

---

77 *Id.* at 2.

78 *Id.* The European Union appeared to take the side of the country of origin in its E-Commerce Directive. European Commission, E-Commerce Directive, **http://ec.europa.eu/internal_market/e-commerce/directive_en.htm** (last visited Feb. 15, 2010). The Directive contains an Internal Market clause "which means that information society services are, in principle, subject to the law of the Member State in which the service provider is established." *Id.*

79 FED. TRADE COMM'N, *supra* note 75, at 4 (discussing the "two fundamental challenges" to a country-of-destination framework, including "the use of physical borders to determine rights in a borderless medium" and compliance costs).

80 In 1999, the OECD issued its Guidelines for Consumer Protection in the Context of Electronic Commerce, which address principles that could be used by electronic commerce merchants in the absence of global consumer protection rules. ORG. FOR ECON. CO-OPERATION & DEV., GUIDELINES FOR CONSUMER PROTECTION IN THE CONTEXT OF ELECTRONIC COMMERCE (1999) [hereinafter OECD GUIDELINES], *available at* **http://www.oecd.org/document/51/0,3343,en_2649_34267_1824435_1_1_1_1,00.html**. The FTC and the OECD held a 10th year anniversary of the release of these guidelines in

through these means, the traditional tools of international conflict of law resolution would have to suffice.[81]

Some commentators such as Paul Berman attempted to reach beyond the traditional dispute resolution mechanisms for resolving conflict of law cases with principles that take into account the realities of multiple community affiliations.[82] His "cosmopolitan pluralism" was "cosmopolitan" because it went beyond the laws of any one particular jurisdiction and recognized the legitimacy of norms created by private parties and communities.[83] It was plural because it did not dissolve the multiplicity of community affiliations and their associated norms into a single world-wide standard. Diversity and conflict would endure and would need to be resolved according to a series of principles that recognized the need to balance competing national norms.[84]

These approaches to resolving jurisdictional disputes in cyberspace have various advantages and disadvantages. However, payment system intermediaries needed a mechanism to address the jurisdictional question that was easy to apply, effective in resolving the dispute, and minimized legal risk to the system or its members. It could not wait for unpredictable, after-the-fact judgments by courts. The idea they developed, discussed in chapter 6 of this book, was that a

---

December 2009. OECD, OECD Conference on Empowering E-Consumers, **http://www.oecd.org/ict/econsumerconference** (last visited Sep. 1, 2010).

81 In an interesting twist, some commentators used the presence of these dispute resolution mechanisms to argue against indirect liability for intermediaries. Why deputize intermediaries to stop illegal activities on the Internet when governments can reach the bad actors and resolve any disputes in the normal way? Responding to the argument that indirect liability is needed because the bad actor is unreachable by law enforcement or aggrieved parties, Holland says:

> As an initial matter, it is not clear that a significant number of bad actors are beyond the reach of the law. Advances in technology are making it increasingly possible to locate and identify bad actors online, such that online anonymity is difficult to maintain. Likewise, where the bad actor is identified but is found outside the jurisdiction, sovereign governments have developed methods for resolving disputes to permit the direct extraterritorial application of domestic law, such as rules of jurisdiction, conflicts of laws, and recognition of judgments.

Holland, *supra* note 16, at 393.

82 Berman, *supra* note 73, at 1862.

83 *Id.*

84 *Id.* Berman's work has affinities with that of political philosophers working in the area of national sovereignty in a global world. *See, e.g.*, Thomas W. Pogge, WORLD POVERTY AND HUMAN RIGHTS 168-95 (2002).

transaction is unacceptable in the payment system if it is illegal in the jurisdiction of either the buyer or the seller.[85]

The payment card approach provides a simple default rule for intermediaries to apply when determining whether to allow transactions in their systems. It eliminates the heavily fact-based balancing assessments needed to determine, on a case-by-case basis, whose law applies. The default rule also does not simply adopt a country of origin or country of destination perspective, each of which is limited. Nor does it leave the transaction in a legal limbo where no law applies.[86]

The payment system experience leads to several observations. First, direct conflicts of law are not as frequent as some anticipated. Technology and payment system practices effectively reduce these conflicts to the rare instance

---

[85] Visa's policy is stated in *International Piracy: The Challenges of Protecting Intellectual Property in the 21st Century: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 110th Cong. 73–82 (2007) at 71 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.). Other payment intermediaries have similar procedures, such as eBay's restriction about selling and shipping illegal goods to the country where they are illegal. eBay, Offensive Material Policy, **http://pages.ebay.com/help/policies/offensive.html** (last visited Feb. 4, 2010) ("[B]ecause eBay is a worldwide community, many of our users live in countries where the possession or sale of items associated with hate organizations is a criminal offense. We can't allow the sale or shipping of these items there.").

[86] The internal application of this rule involves system efficiency and the balance of interests among the stakeholders in the system. If the merchant is in violation of its own country's law, then enforcement is conceptually easy. Merchants discovered in violation of local law either have to stop the transactions or be removed from the system. If the merchant is in violation of the law in a different jurisdiction, things are more complicated. Should the bank of the merchant or the bank of the customer be burdened with the enforcement responsibility? If the merchant has this responsibility, then he must not introduce the illegal transaction into the system and the merchant's bank must not try to process it, then steps must be taken at the merchant's end to stop the transaction. These steps could include: a system decision requiring the merchant to stop these transactions entirely; coding and programming modifications by the merchant, the merchant's processor, or the system operator that would block transactions at the merchant end from entering the system if the customer was from a jurisdiction where the transaction would be illegal; or restricting the transaction to the merchant's own jurisdiction. Alternatively, the enforcement measures could be put on the cardholder side. Merchants could introduce properly-coded transactions into the system and rely on action on the cardholder's side to stop the transaction. This seems to fit the case of Internet gambling, where U.S. law makes Internet gambling illegal for U.S. citizens, and the payment networks responded to the Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) with a coding and blocking system that allowed merchants to continue their services in countries where Internet gambling was illegal, as discussed earlier in this Article. For instance, should merchants be responsible for knowing the laws of all the countries of all the customers they deal with? Perhaps not, but if 90% of their sales are from an offshore jurisdiction, they should be responsible for knowing that sales of their product are legal in that jurisdiction. Violations of the policy would largely be dealt with on a complaint basis.

where the law of one country demands what the law of another country forbids. Directly contradicting laws are more common in "political" areas, where governments are seeking information from intermediaries to enforce local laws against their own citizens.[87]

Second, regulating the Internet by focusing on the local affiliates of global payment operations does not require the use of either the traditional or the new "cosmopolitan" conflict resolution methods. By relying on global payment intermediaries, local jurisdictions reach out to the local affiliates that are totally within their jurisdiction. They do not put burdens on entities in foreign jurisdictions at all. There is literally no conflict and thus nothing to which normal mechanisms of conflict resolution may attach.[88]

Some commentators have correctly pointed out that when the laws of different jurisdictions apply to a single transaction, the ability of any particular jurisdiction to unilaterally regulate the Internet is limited.[89] But intermediaries can reduce these conflicts. Global payment systems can simplify transactions to events in which only a buyer in one jurisdiction and a seller in another are implicated. By concentrating enforcement on intermediaries instead of individuals or merchants, local jurisdictions can take advantage of the economies that these institutions make possible.

The experience of payment intermediaries reveals that, within limits, the differences among conflicting jurisdictions can be managed. The bordered

---

87 *See, e.g.*, Press Release, Privacy Int'l, Europe's Privacy Commissioners Rule Against SWIFT (Nov. 23, 2006), *available at* **http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-546365** (describing the SWIFT case, where SWIFT was required to comply with U.S. demands for access to financial information about European customers in virtue of its operations on US soil, while such compliance put them in violation of the European data protection directive). In addition, passage of the Global Online Freedom Act (GOFA) could put Internet intermediaries in a conflict of law situation with China and other countries. *See* Global Online Freedom Act of 2007, H.R. 275, 110th Cong. (2007). H.R. 275 was introduced by Representative Chris Smith on January 5, 2007 and would require U.S. intermediaries to resist certain orders from countries in which they are doing business. *Id.*

88 Antigua brought a complaint against the U.S. for the enforcement of its gambling laws, but its success was based only on (1) the U.S.'s failure to exclude Internet gambling from the list of services that required open treatment and (2) the idiosyncrasies of U.S. gambling law which appear to allow domestic horse racing to engage in Internet gambling while denying similar opportunities to offshore Internet gambling merchants. But these are technical obstacles created by the interaction of complex U.S. law and international WTO law and are not real conflict of law problems. See Appellate Body Report, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 358-64, WT/DS285/AB/R (Apr. 7, 2005). Op cit. *supra* note 130.

89 See, e.g., H. Brian Holland, *The Failure of the Rule of Law in Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty*, 24 J. MARSHALL J. COMPUTER & INFO. L. 1, 26 (2005).

Internet works on a small scale. The scale is currently small for two reasons: First, he number of cases of governments reaching across borders to inflict their laws on Internet merchants in other jurisdictions is still relatively small. Moreover, in contrast to the rhetoric about the Internet creating a global marketplace, the scope of cross-border commerce itself is still limited. The reality is that the volume of cross-border transactions is not large enough to create a truly substantial cross-border jurisdictional crisis. Currently, only four percent of the sales for electronic commerce merchants in the U.S. come from abroad.[90] And data from Europe show that cross border online transactions are not increasing as fast as overall e-commerce transactions, staying relatively stable from 2006 to 2008 at six to seven percent.[91]

As David Post has warned, the problem the Internet creates for local jurisdictions is one of scale.[92] The bordered Internet simply does not scale up. Global payment systems cannot accommodate an enforcement burden in which each jurisdiction uses payment system mechanisms to enforce each of its local laws on the Internet.

It is not hard to see how we can get into a kind of tragedy of the commons in this area. Each individual extension of local jurisdiction into cyberspace seems small and costless, but collectively the burden becomes unbearable. Governments might feel free to exploit this enforcement mechanism, in the same way that grazers use the commons—under the impression that it is an unlimited resource. However, one of two outcomes will occur as the cross-border rules pile up: Either cross-border transactions will remain small and the potential for the Internet to be a global channel of commerce will not be realized, or the political costs of each government attempting to regulate the e-

---

90 This is based on transaction data from the Visa system. *See International Piracy Hearing*, *supra* note 85, at 75 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

91 Comm'n of the European Cmtys., *Commission Staff Working Document: Report on Cross-Border E-commerce in the EU* 3, SEC (2009) 283 final (Mar. 5, 2009), *available at* **http://ec.europa.eu/consumers/strategy/docs/com_staff_wp2009_en.pdf** ("From 2006 to 2008, the share of all EU consumers that have bought at least one item over the Internet increased from 27% to 33% while cross-border e-commerce remained stable (6% to 7%).").

92 *See* Post, *Against "Against Cyberanarchy"*, *supra* note 15, at 1377 (stating that "scale matters"); *see also* Holland, *supra* note 89, at 29. Holland states:

> The online actor cannot know, as a practical matter, the many laws applicable to a particular act, nor when one or more sovereigns may decide to attempt regulatory action. This is particularly true in those areas of regulation in which morality, religion and culture are at their most influential, such as speech, race, sex, and even intellectual property. Moreover, it is not simply one actor or a few legal systems. It is an exponential multitude.

*Id.*

commerce activities of other countries will mount. Either development reveals the limitations of the bordered Internet as a long-term framework for Internet governance.

Goldsmith and Wu suggest that enforcement of Internet regulations through intermediaries is necessarily limited in size.[93] They suggest that maybe the system will not be able to scale up, but it won't have to.[94] Small countries such as Antigua cannot enforce Internet rules because global intermediaries can simply pull up stakes and leave if the rules are too strict.[95] However, there are a sufficiently large number of countries that global intermediaries will not feel capable of abandoning. If all of them use the intermediary enforcement mechanism, the system will be overwhelmed.

## Internationalism

The fundamentally correct insight of the Internet exceptionalists is that the unilateral imposition of one nation's law onto all Internet activities that cross borders won't scale.[96]

Internationalism might be the way out. It is the idea that the Internet will eventually be governed, at least for some services, by global institutions and arrangements, and that this is the right public policy for local governments to follow in their dealings with illegal cross border Internet transactions.[97] This policy could be implemented through a uniform global standard, or any of a variety of techniques such as World Trade Organization rules that bring local laws into harmony. The basic justification for this policy is similar to the justification for establishing a single uniform national policy that prevents the clash of inconsistent rules at the state level: When activities have widespread and significant effects on those outside the local jurisdiction, then uniform principles or some other coordinating mechanism should be adopted at the higher level.[98] This universalism could promise better laws, whereby the

---

93 GOLDSMITH & WU, *supra* note 7, at 81-82.

94 *Id.* at 81.

95 *See id.* at 160 (suggesting that acting as the Internet police is just a normal cost of doing business for global companies, which they can avoid in a particular case by leaving a country that tried to impose costs that exceeded the benefits of continued presence in the country and thus creating another objection to the bordered Internet to effectively give larger countries a greater role in Internet governance than smaller ones).

96 *See* Johnson & Post, *supra* note 1, at 1390 ("One nation's legal institutions should not monopolize rule-making for the entire Net.").

97 GOLDSMITH & WU, *supra* note 7, at 26.

98 *Id.* ("If the nations of the world agree to a single global law for questions like libel, pornography, copyright, consumer protection, and the like, the lives of Internet users

"[i]nternational standards could reflect a kind of collection of best practices from around the world — the opposite of the tyranny of the unreasonable."[99]

Goldsmith and Wu make several criticisms of internationalism. First, a system of universal laws would be unattractive; it would leave the world divided and discontent because the universal law would be unpopular in large segments of the world population. Second, the system of local national laws would better reflect differences among people. Diversity is a good thing and cannot be taken into account by a universal code that overrides local differences. Third, it is not needed. The conflicts of laws, extraterritoriality, and other considerations are perfectly manageable within the current international framework. For example, since most Internet users do not have assets in other countries, they are effectively subject only to the laws of the country where they live. Only large multinational companies with assets all over the world face the multijurisdictional problem, and they already have to live with that because they are already global. Compliance with a plurality of international laws is simply a cost of doing business for global companies. There's nothing new here that would justify a move to a more harmonized global order. There are extra costs to be sure, but nothing so onerous or burdensome that it would require a move to global law.[100]

The responses to these criticisms are straightforward. An unpopular global law is not the goal. Neither is suppression of diversity the goal. The idea is to integrate local laws in some fashion when the regular conflicts among them prove to be intolerable. When diversity does not create this difficulty, there is no need for integration. If, for example, local governments value diversity enough to refrain from using intermediaries to enforce local laws against actors in other jurisdictions, then there is no need for harmonization of these enforcement efforts. But to the extent that governments want to take global enforcement steps, they also need to take steps to integrate the laws they want

---

become much simpler: no conflicting laws, no worries about complying with 175 different legal systems, no race to the bottom.").

99 *Id.* at 27. Reidenberg also argues that as jurisdictions increasingly conflict there will need to be an overarching harmonization of international rules:

> [O]nline enforcement with electronic blockades and electronic sanctions will cause serious international political conflicts. These conflicts arise because of the impact on territorial integrity. Such conflicts are likely to force negotiations toward international agreements that establish the legal criteria for a state to use technological enforcement mechanisms. This progression leads appropriately to political decisions that will define international legal rules.

Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213, 230 (2003-2004).

100 *See* GOLDSMITH & WU, *supra* note 7, at 152-60.

to enforce. The reason for this is that global intermediaries' costs to mediate the conflicts associated with unilateral attempts at local regulation of the Internet will be so onerous and burdensome that they will cause an unwarranted and unnecessary decline in global interaction.[101]

Berman also describes how the internationalist hope for global standards avoids the conflict of law problem: "if we constructed one universal 'world community' with one set of governing rules, there would never need to be a 'choice of law' in the sense that conflict-of-laws scholars use the term."[102] However, he is critical of this universal world community for two reasons. First, he is critical of this community because of its potential to dissolve community affiliations that provide important emotional connections and opportunities for normative discussion of those connections. Second, he views this universal community as fundamentally unrealistic given the dominance of current notions of nation-state sovereignty.[103]

These objections can be met at the level of generality at which they are cast. We do not need to think of ourselves as primarily world citizens in order to endorse specific global approaches. We can still have deep attachments to local communities and can still debate the relative importance of the overlapping communities we participate in. The global approach endorses the view that self-government "requires a politics that plays itself out in a multiplicity of settings, from neighborhoods to nations to the world as a whole" and "citizens who can abide the ambiguity associated with divided sovereignty, who can think and act as multiply situated selves."[104] But participation in global community and the wisdom to know when the global perspective should take precedence over more local concerns is essential to this vision of self-government in a global world.

The internationalist proposal is to provide global coordination only when necessary. It is to move to global standards when, as a practical matter, the burdens of allowing diverse local rules are too high. The model of national uniform standards is appropriate: not everything has to be done at the national level, but some things should be done there in order to have an efficient and fair national system. Similarly, there is no need to move from the current system to

---

101 Interestingly, the earlier Jack Goldsmith seemed more inclined to accept these practical considerations as a rationale for international harmonization: "When in particular contexts the arbitrariness and spillovers become too severe, a uniform international solution remains possible." Goldsmith, *supra* note 4, at 1235.

102 Berman, *supra* note 73, at 1860.

103 *Id.* at 1860-61.

104 MICHAEL J. SANDEL, PUBLIC PHILOSOPHY: ESSAYS ON MORALITY IN POLITICS 34 (2005).

a world government. But if there are practical ways to improve Internet governance through global harmonization, they should be taken.

If governments are going to use payment intermediaries as enforcers of local law, there are a number of steps that could be taken to coordinate their efforts, including:

- In the Internet gambling context, a move to an internationally-interoperable licensing system that would require each jurisdiction that allows Internet gambling to defer to the licensing decisions of other jurisdictions
- In the copyright context, the continued evolution of uniform copyright rules.

International agreements are one mechanism to create coordinated action. Although controversial because of the secrecy involved in its development, and the sense that affected parties were excluded from participation, the Anti-Counterfeiting Trade Agreement (ACTA) is a reasonable, though flawed, model for action in this area.[105] There are many mechanisms for international coordination. Decisions regarding which mechanisms to use depend on the issue and the fora available for resolution.

Internationalism has its dangers. Why should each jurisdiction have the same regulations on hate speech and the same regulations on alcohol consumption? The answer is that there will be no harmonization where there are such fundamental differences. Intermediaries will be called upon to resolve the issue themselves or they will be caught between warring governments and forced to choose sides. But efforts should be made to minimize such differences when these differences have global consequences, especially when they are superficial differences that reflect no fundamental divisions. For the same reason that we want uniform global technical standards for information and communications technologies, if possible, we want similar legal frameworks if governments are going to enforce laws on the Internet.

These efforts to ease the friction involved in extending government authority to the Internet through a global framework are in line with other efforts to create global frameworks that promote the growth of the Internet. For example, the thirty-first International Conference of Data Protection and Privacy Commissioners, held in Madrid in November 2009, adopted a set of global

---

105 *See* Media Statement, Participants in ACTA Negotiations, *Anti-Counterfeiting Trade Agreement (ACTA),* June 12, 2009, *available at* **http://www.med.govt.nz/templates/Page____40974.aspx**. For a summary of the ACTA process and the content of the agreement, *see* THE ANTI-COUNTERFEITING TRADE AGREEMENT – SUMMARY OF KEY ELEMENTS UNDER DISCUSSION (2009), *available at* **http://www.med.govt.nz/templates/MultipageDocumentTOC____40563.aspx**.

privacy standards.[106] There is also likely to be a renewed push for global consumer protection on the occasion of the tenth anniversary of the Organisation for Economic Co-operation and Development's Guidelines for Consumer Protection in the Context of Electronic Commerce.[107]

Both these efforts relate to the growth of the Internet as a vibrant international marketplace. They do this by building online trust. Global information security standards reassure people that their information is safe no matter what the physical location of the websites they visit. Establishing global privacy standards means that the collection and use of online information will be governed by common principles regardless of a website's jurisdiction and will make it easier for global business to transfer information from one jurisdiction to another in a seamless manner. Finally, effective global consumer protection rules will mean that people will have the information and redress rights they need to shop confidently online no matter where the website is located.

## Conclusion

The initial demand from Internet exceptionalists that the online world be left alone by governments has morphed into the idea that governments should create a global framework to protect and spur the growth of the Internet. The intervening steps in this development are not hard to trace: Internet exceptionalists confused their ideal of self-governing Internet communities with the idea that the Internet was ungovernable because it was a global communications network that crossed borders. This idea of an intrinsically ungovernable Internet was undermined by the recognition that the coding that underlies Internet applications and services is a matter of choice, not

---

106 Artemi R. Lombarte, Dir., Agencia Española de Protección de Datos, Slide Presentation: International Standards on Data Protection & Privacy (2009), *available at* **https://www.agpd.es/portalweb/canaldocumentacion/comparecencias/common/IAPP_Privacy_Summit_09.pdf**. He describes one of the main criteria of the global privacy standards project as "To elaborate a set of principles and rights aimed to achieve the *maximum degree of international acceptance*, ensuring at once a high level of protection." *Id.* (emphasis in original). For the standards adopted, see THE MADRID PRIVACY DECLARATION (Nov. 3, 2009), **http://thepublicvoice.org/TheMadridPrivacyDeclaration.pdf**.

107 OECD GUIDELINES, *supra* note 80; *see also* Org. for Econ. Co-operation & Dev., Conference on Empowering E-Consumers: Strengthening Consumer Protection in the Internet Economy, Programme (2009), *available at* **http://www.oecd.org/dataoecd/33/22/44045376.pdf** (describing the conference). The OECD endorsed steps toward global enforcement of some consumer protection rules in a 2003 report on cross-border fraud and a 2007 report on consumer dispute resolution and redress. *See* Comm. on Consumer Policy, Org. for Econ. Co-operation & Dev., OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (2003), *available at* **http://www.oecd.org/dataoecd/24/33/2956464.pdf**; Comm. on Consumer Policy, Org. for Econ. Co-operation & Dev., OECD Recommendation on Consumer Dispute Resolution and Redress (2007), *available at* **http://www.oecd.org/dataoecd/43/50/38960101.pdf**.

unchangeable nature. If something about this system created difficulties for government control, this could be changed. Further, the idea that governments cannot control the Internet was undermined by the need for the local operations of global intermediaries to provide essential Internet services and the practical ability of governments to control these intermediaries.

Internet intermediaries can control the content of the activities on their online communities, and government can compel or pressure intermediaries to take these steps. Intermediaries have a general obligation to follow the law, and except in extreme cases, they have no right to resist these lawfully established burdens. The establishment of these laws needs to follow all the rules of good policymaking, including imposing an obligation only when the social benefits exceed the social costs. However, a bordered Internet in which each country attempts to use global intermediaries to enforce its local laws will not scale. This is the fundamentally correct insight of the Internet exceptionalists. If governments are going to use intermediaries to enforce local laws, they are going to have to harmonize the local laws they want intermediaries to enforce.

# CHAPTER 4

## HAS THE INTERNET FUNDAMENTALLY CHANGED ECONOMICS?

# Computer-Mediated Transactions

By Hal R. Varian*

Every now and then a set of technologies becomes available that sets off a period of "combinatorial innovation." Think of standardized mechanical parts in the 1800s, the gasoline engine in the early 1900s, electronics in the 1920s, integrated circuits in the 1970s, and the Internet in the last few decades.

The component parts of these technologies can be combined and recombined by innovators to create new devices and applications. Since these innovators are working in parallel with similar components, it is common to see simultaneous invention. There are many well-known examples such as the electric light, the airplane, the automobile, and the telephone. Many scholars have described such periods of innovation using terms such as "recombinant growth," "general purpose technologies," "cumulative synthesis" and "clusters of innovation."[1]

The Internet and the Web are wonderful examples of combinatorial innovation. In the last 15 years we have seen a huge proliferation of Web applications, all built from a basic set of component technologies.

The Internet itself was a rather unlikely innovation; I like to describe it as a "lab experiment that got loose." Since the Internet arose from the research community rather than the private sector, it had no obvious business model. Other public computer networks, such as AOL, CompuServe, and Minitel, generally used subscription models, but were centrally controlled and offered little scope for innovation at the user level. The Internet won out over these alternatives, precisely because it offered a flexible set of component technologies that encouraged combinatorial innovation.

The earlier waves of combinatorial innovation required decades, or more, to play out. For example, David Hounshell argues that the utopian vision of

---

* Univ. of Cal., Berkeley and Google. hal@ischool.berkeley.edu.

1 *See, e.g.*, Martin Weitzman, *Recombinant Growth*, 113 Q. J. OF ECON. 331-360 (1998); Timothy Bresnahan & M. Trajtenberg, *General Purpose Technologies: Engines of Growth?*, 65 J. OF ECONOMETRICS 83-108 (1995), *available at* **http://ideas.repec.org/a/eee/econom/v65y1995i1p83-108.html**; Timothy Bresnahan, *General Purpose Technologies*, *in* HANDBOOK OF THE ECONOMICS OF INNOVATION (Bronwyn Hall & Nathan Rosenberg, eds., 2010); Nathan Rosenberg, *Technological Change in the Machine Tool Industry*, *in* PERSPECTIVES IN TECHNOLOGY 9-31 (1976); ABBOTT PAYSON USHER, A HISTORY OF MECHANICAL INVENTION (revised ed., Dover Publ'ns 1998); and Joseph A. Schumpeter, *The Analysis of Economic Change*, *in* ESSAYS ON ENTREPRENEURS, INNOVATIONS, BUSINESS CYCLES AND THE EVOLUTION OF CAPITALISM 134-149 (Richard V. Clemence, ed., 2000) (originally published in *Review of Economic Statistics*, May 1935).

interchangeable parts took more than a century to be realized.[2] The Web was invented in the early 1990s, but it did not become widely used until the mid-1990s. Since then, we have seen a huge number of novel applications—from Web browsers, to search engines, to social networks—to mention a few examples. As with the Internet, the Web initially had no real business model, but offered a fertile ground for combinatorial innovation.

Innovation was so rapid on the Internet because the component parts were all bits. They were programming languages, protocols, standards, software libraries, productivity tools and the like. There was no time to manufacture, no inventory management, and no shipping delay. You never run out of HTML, just like you never run out of email. New tools could be sent around the world in seconds and innovators could combine and recombine these bits to create new Web applications.

This parallel invention has led to a burst of global innovation in Web applications. While the Internet was an American innovation, the Web was invented by an Englishman living in Switzerland. Linux, the most used operating system on the Web, came from Finland[3], as did MySQL, a widely used database for Web applications.[4] Skype, which uses the Internet for voice communication, came from Estonia.[5]

Of course, there were many other technologies with worldwide innovation, such as automobiles, airplanes, photography, and incandescent lighting. However, applications for the Internet, which is inherently a communications technology, could be developed everywhere in the world in parallel, leading to the rapid innovation we have observed.

## Computer-Mediated Transactions

My interest in this essay is in the economic aspects of these technological developments. I start with a point so mundane and obvious, it barely seems worth mentioning: Nowadays, most economic transactions involve a computer.

---

2 David A. Hounshell, From the American System to Mass Production, 1800-1932: The Development of Manufacturing Technology in the United States (1985).

3 *See* Linus Torvalds & David Diamond, Just for Fun: The Story of an Accidental Revolution (2002).

4 *See* Oracle Corporation, *From Visions to Reality: An Interview with David Axmark, Co-Founder of MySQL AB*, July 2007, **http://dev.mysql.com/tech-resources/interviews/david-axmark.html**.

5 *See* Andreas Thomann, *Skype: A Baltic Success Story*, CREDIT SUISSE GROUP, June 9, 2006, **http://emagazine.credit-suisse.com/app/article/index.cfm?fuseaction=OpenArticle&aoid=163167&coid=7805&lang=EN**.

Sometimes this computer takes the form of a smart cash register, part of a sophisticated point of sale system, or a website. In each of these cases, the computer creates a record of the transaction.

This record-keeping role was the original motivation for having the computer as part of the transaction. Creating a record of transactions is the first step in building an accounting system, thereby enabling a firm to understand its financial status.

Now that computers are in place, they can, however, be used for many other purposes. In this essay, I explore some of the ways that computer mediation can affect economic transactions. These computer mediated transactions, I argue, have enabled significant improvements in the way transactions are carried out and will continue to impact the economy in the foreseeable future.

I classify the impact of computer mediated transactions into four main categories according to the innovation they facilitate:

- New forms of contract;
- Data extraction and analysis;
- Controlled experimentation;
- Personalization and customization.

## Enable New Forms of Contract

Contracts are fundamental to commerce. The simplest commercial contract says, "I will do X if you do Y," as in "I will give you $1 if you give me a cup of coffee." Of course, this requires that the actions to be taken are verifiable. Just asking for coffee does not mean that I will get it. As Abraham Lincoln supposedly remarked, "If this is coffee, please bring me some tea; but if this is tea, please bring me some coffee."[6]

A computer used in a transaction can observe and verify many aspects of that transaction. The record produced by the computer allows the contracting parties to condition the contract on terms that were previously unobservable, thereby allowing for more efficient transactions.

I am not claiming that increased observation will necessarily lead to more efficient contracts. There are counterexamples to the assertion that "more

---

6 Susan L. Rattiner, Food and Drink: A Book of Quotations (2002).

information is better" such as the Hirshleifer example.[7] I am merely claiming that additional information allows for more efficient contracts.

Of course, the study of contracts is a highly developed field in economics. As such, it is hardly novel to suggest that contractual form depends on what is observable. What is interesting, however, is the way that progress in information technology enables new contractual forms.

Consider, for example, a rental-car agency that buys insurance based on accident rates, and that accident rates, in turn, depend on the speed of a vehicle. All renters would prefer to drive within the speed limit if they are compensated with a lower rental fee. However, if there is no way to monitor the speed of a rental car, such a contractual provision is unenforceable. Putting a computer transmitter in the trunk of the car that records the vehicle's speed makes the contract enforceable and potentially makes everyone better off..[8]

The transportation sector has capitalized on the availability of computerized transmitters to create more efficient contracts in many areas.

- Car dealers are selling cars with "starter interrupt" devices that inhibit operations if car payments are missed.[9]
- Similar interrupt devices attached to breath analyzers are mandated for drunk driving offenders in many states.
- Parents can buy a device known as "MyKey" which allows them to limit auto speed, cap the volume on the radio, require seat belt use and encourage other safe-driving habits for teenage drivers.[10]
- In the relevant economics literature, Hubbard and Baker examine a variety of ways that vehicular monitoring systems have impacted the trucking industry.[11]

---

7 Jack Hirshleifer, *The Private and Social Value of Information and the Reward to Inventive Activity*, 61 THE AM. ECON. REV. 561-74 (Sept. 1971), *available at* **http://faculty.fuqua.duke.edu/~qc2/BA532/1971%20AER%20Hirshleifer.pdf**.

8 This is a particularly simple case. If drivers have heterogeneous preferences, those who prefer to speed may be made worse off by the availability of such a device.

9 Associated Press, *For Some High-risk Auto Buyers, Repo Man is a High-tech Gadget*, L.A. TIMES, June 13, 2006, **http://articles.latimes.com/2006/jun/13/business/fi-late13**.

10 Nick Bunkley & Bill Vlasic, *Ensuring Junior Goes for a Mild Ride*, N.Y. TIMES, Oct. 6, 2008, **http://www.nytimes.com/2008/10/07/automobiles/07auto.html**.

11 Thomas N. Hubbard, *The Demand of Monitoring Technologies: The Case for Trucking*, 115 Q. J. OF ECON. 533-560 (2000), http://**www.mitpressjournals.org/doi/abs/10.1162/003355300554845**; George Baker & Thomas N. Hubbard. *Contractibility and Asset Ownership: On-board Computers and Governance in US Trucking*, 119 Q. J. OF ECON. 1443-1479 (2004), http://**www.mitpressjournals.org/doi/abs/10.1162/0033553042476152**.

There are many other examples of computer-mediated contracts. The work of Dana & Spier and Mortimer, provides examples that describe the efficiency gains resulting from revenue sharing in the video tape rental industry.[12]

Video tapes were originally purchased by retail stores from distributors for about $65 per tape. Since the videos were so expensive, stores only bought a few. As a result, the popular videos quickly disappeared from the shelves, making everyone unhappy.

In 1998, retailers and distributors adopted a new business model: a revenue sharing arrangement in which stores paid a small upfront fee of $3 to $8, but split the revenue when the video was rented, with 40% to 60% going to the retailer. Stores no longer had an incentive to economize on purchases, and all parties to the transaction—retailers, distributors, and customers—were made better off.

Sharing revenue at point of sale requires that both parties be able to monitor the transaction. The technological innovations of bar code scanning, the computerized cash register, and computer networks enabled revenue-sharing arrangements.

Of course, when a transaction takes place online, revenue-sharing is much easier. Online advertising is a case in point where revenue from an advertiser for an ad impression or click may be split among publishers, ad exchanges, ad networks, affiliates and other parties based on contractual arrangements.

Although the benefits from computers offering *more* information to contracting parties have only been discussed thus far, there are also cases in which computers can be used to improve contractual performance by *hiding* information using cryptographic methods. A picturesque example is the "cocaine auction protocol" which describes an auction mechanism designed to hide as much information as possible.[13]

Finally, "algorithmic game theory" is an exciting hybrid of computer science and economic theory that deserves mention. This subject brings computational considerations to game theory (how a particular solution can be computed) and

---

12 James D. Dana & Kathryn E. Spier. *Revenue Sharing and Vertical Control in the Video Rental Industry*, XLIX Q. J. OF ECON. 223-245 (2001), *available at* **http://www3.interscience.wiley.com/journal/118972449/abstract**; Julie H. Mortimer, *Vertical Contracts in the Video Rental Industry*, 75 REV. OF ECON. STUDIES 165-199 (2008), **http://www3.interscience.wiley.com/journal/119395822/abstract**.

13 Frank Stajano & Ross Anderson, *The Cocaine Auction Protocol: On the Power of Anonymous Broadcast*, *in* PROCEEDINGS OF INFORMATION HIDING WORKSHOP, LECTURE NOTES IN COMPUTER SCIENCE, 1999, **http://www.cl.cam.ac.uk/ rja14/Papers/cocaine.pdf**.

strategic considerations to algorithm design (whether a particular algorithm is actually incentive-compatible).[14]

## Some History of Monitoring Technologies

Though I have emphasized computer mediated transactions, a computer can be defined quite broadly. The earliest example of an accounting technology I know of that enabled new forms of contract involves Mediterranean shipping circa 3300 B.C.

The challenge was how to write a "bill of lading" for long distance trade in societies that were pre-literate and pre-numerate. The brilliant solution was to introduce small clay tokens, known as "bullae," which were small representations of the material being transported. As each barrel of olive oil was loaded onto a ship, a barrel-shaped token was placed in a clay envelope. After the loading was completed, the envelope was baked in a kiln and given to the ship's captain. At the other end of the voyage, the envelope was then broken open and the tokens were compared to the barrels of oil on the ship as they were unloaded. If the numbers matched, the contract was verified. Later, marks were scratched on the outside of the envelope to indicate the number of tokens inside. Some authors believe that this innovation led to the invention of writing between 3400 and 3300 B.C.[15]

A somewhat more recent example is the invention of the cash register in 1883 by James Ritty.[16] Ritty, a saloon owner, discovered that his employees were stealing money. In response, he developed a device to record each transaction on paper tape, an invention that he patented under the name of "the incorruptible cashier."[17] Ritty's machine became the basis of the National Cash Register (NCR) Company founded in 1884. The NCR device added a cash drawer and a bell that sounded "ka-ching" whenever the drawer was opened, to alert the owner of the transaction, thereby discouraging pilfering. This improved monitoring technology made retailers willing to hire employees

---

14 See NOAM NISAN, TIM ROUGHGARDEN, EVA TARDOS, AND VIJAY V. VAZIRANI, EDS., ALGORITHMIC GAME THEORY (2007) for a comprehensive collection of articles and Hal R. Varian, *Economic Mechanism Design for Computerized Agents*, *in* USENIX WORKSHOP ON ELECTRONIC COMMERCE 13-21 (1995), **http://www.sims.berkeley.edu/hal/Papers/mechanism-design.pdf** for an early contribution to this theory.

15 Jean-Jacques Glassner, Zainab Bahrani, & Marc Van de Miero, The Invention of Cuneiform: Writing in Sumer (2005).

16 MIT School of Engineering, *Inventor of the Week Archive: James Ritty, Cash Register*, April 2002, **http://web.mit.edu/invent/iow/ritty.html**.

17 Cash Register and Indicator, U.S. Patent 271,363 (filed Feb 15, 1882), *available at* **http://www.google.com/patents?hl=en&lr=&vid=USPAT271363**.

outside their immediate families, leading to larger and more efficient establishments.[18]

## Enabling Online Advertising

Online advertising serves as a poster child for algorithmic mechanism design. A Pasadena company called GoTo began ranking search results using an auction.[19] Users did not like this particular form of search, so GoTo switched to using an auction to rank advertisements. In the original auction, ads were ranked by "bid per click" and advertisers paid the amount they bid. After consultation with auction theorists, GoTo moved to a second-price auction: An advertiser paid a price per click determined by the bid of the advertiser in the next lower position.[20]

There is a fundamental divergence of incentives in advertising. The publisher (i.e. the content provider) has space on its Web page for an ad and wants to sell ad impressions to the highest bidders. The advertiser does not care directly about ad impressions, but does care about visitors to its website, and ultimately, the sale of its products. Hence, the publisher wants to sell impressions, but the advertiser wants to buy clicks.

This is similar to an international trade transaction where the buyer wants to pay in euros and the seller wants to receive dollars. The solution in both cases is the same: an exchange rate. In the context of online advertising, the exchange rate is the predicted click-through rate, an estimate of how many clicks a particular ad impression will receive. This allows one to convert the advertiser's offered bid per click to an equivalent bid per impression. The publisher can thus sell each impression to the highest bidder.

This mechanism aligns the interests of the buyer and the seller, but creates unintended consequences. If the advertiser only pays for clicks, he has no direct incentive to economize on impressions. Excessive impressions, however,

---

18 *See* JoAnne Yates, *Business Use of Information and Technology from 1880-1950*, *in* A NATION TRANSFORMED BY INFORMATION: HOW INFORMATION HAS SHAPED THE UNITED STATES FROM COLONIAL TIMES TO THE PRESENT 107-135. (Alfred D. Chandler and James Cortada, eds., 2000) (detailing the role of office machinery in the development of commercial enterprises).

19 *GoTo.com Posts Strong Relevancy Ranking in NPD Survey of Search Engines*, BUSINESS WIRE, April 11, 2000, *available at* **http://www.highbeam.com/doc/1G1-61423181.html**.

20 For accounts of the development of these auctions, see John Battelle, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE (2005); Steve Levy, *Secret of Googlenomics: Data-fueled Recipe Brews Profitability*, WIRED, 2009, **http://www.wired.com/culture/culturereviews/magazine/17-06/nep_googlenomics?currentPage=all**.

impose an attention cost on users, so further attention to ad quality is important to ensure that ad impressions remain relevant to users.

Nowadays, the major providers of search engine advertising all estimate click-through rates along with other measures of ad quality and use auctions to sell these ads. Economists have applied game theory and mechanism design to analyze the properties of these auctions.[21]

## Enabling Data Extraction & Analysis

The data from computer-mediated transactions can be analyzed and used to improve the performance of future transactions.

The Sabre air passenger reservation system offered by American Airlines is an example of this. The original conception, in 1953, was to automate the creation of an airline reservation. However, by the time the system was released in 1960, it was discovered that such a system could also be used to study patterns in the airline reservation process: The acronym Sabre stands for Semi-Automatic Business Research Environment.[22]

The existence of airline reservation systems enabled sophisticated differential pricing (also known as "yield management") in the transportation industry.[23]

Many firms have built data warehouses based on transaction-level data which can then be used as input for analytic models of customer behavior. A prominent example is supermarket scanner data which has been widely used in economic analyses.[24] Scanner data has also been useful in constructing price

---

21 *See, e.g.*, Susan Athey & Glenn Ellison, *Position Auctions with Consumer Search*, 2007. **http://kuznets.fas.harvard.edu/~athey/position.pdf**; Benjamin Edelman, Michael Ostrovsky, & Michael Schwartz, *Internet Advertising and the Generalized Second Price Auction*, 97 AM. ECON. REV. 242-259 (March 2007); Hal R. Varian, *Online Ad Auctions*, 99 AM. ECON. REV. 430-434 (2009).

22 Sabre, *History*, *available at* **http://web.archive.org/web/20080225161359/http://www.sabreairlinesolutions.com/about/history.htm**.

23 Barry C. Smith, John F. Leimkuhler, & Ross M. Darrow, *Yield Management at American Airlines*, 22 INTERFACES 8-31 (1992), *available at* **http://www.jstor.org/pss/25061571** (on the history of yield management in the airline industry). Kalyan T. Talluri & Garrett J. van Ryzin, THE THEORY AND PRACTICE OF REVENUE MANAGEMENT (Kluwer Academic Publishers 2004), **http://books.google.com/books?id=hogoH5LXmyIC** (a textbook explanation of yield management).

24 Aviv Nevo & Catherin Wolfram, *Why Do Manufacturers Issue Coupons? An Empirical Analysis of Breakfast Cereals*, 22 THE RAND J. OF ECON. 319-339 (2002), **http://research.chicagobooth.edu/marketing/databases/dominicks/docs/2002_Why_Do_Manufacturers.pdf**; Igal Hendel & Aviv Nevo, *Measuring the Implications of Sales and Consumer Inventory Behavior*, 74 ECONOMETRICA 1637-1673 (2006), **http://faculty.wcas.northwestern.edu/~ieh758/measuring.pdf**.

indexes,[25] since it allows for much more direct and timely access to prices. The fact that the data is timely is worth emphasizing, since it allows for real time analysis and intervention for businesses and at the policy level.

Hyunyoung Choi and I have used real-time publicly-available search engine data to predict the current level of economic activity for automobile, real estate, retail trade, travel, and unemployment indicators.[26] There are many other sources of real-time data such as credit card, package delivery, and financial data. This has been referred to as "nowcasting" to describe the use of real-time data in estimating the current state of the economy.[27] A variety of econometric techniques are used to deal with the problems of variable selection, gaps, lags, structural changes and so on. Much of the real-time data is also available at state and city levels, allowing for regional macroeconomic analysis.

In the last 20 years, the field of machine learning has made tremendous strides in "data mining." This term was once pejorative, at least among econometricians, but now enjoys a somewhat better reputation due to the exciting applications developed by computer scientists and statisticians.[28] One of the main problems with data mining is over-fitting, but various sorts of cross-validation techniques have been developed to mitigate this problem. Econometricians have only begun to utilize these techniques.[29]

---

25 ROBERT C. FEENSTRA & MATTHEW SHAPIRO, EDS., SCANNER DATA AND PRICE INDEXES (2003); Farm Foundation, *Food CPI, Prices, and Expenditures: A Workshop on the Use of Scanner Data in Policy Analysis*, June 2003, **http://www.ers.usda.gov/briefing/CPIFoodAndExpenditures/ScannerConference.htm**.

26 Hyunyoung Choi & Hal R. Varian, *Predicting the Present with Google Trends*, GOOGLE RESEARCH BLOG, April 2, 2009, **http://googleresearch.blogspot.com/2009/04/predicting-present-with-google-trends.html**; Hyunyoung Choi & Hal R. Varian, *Predicting Initial Claims for Unemployment Benefits*, GOOGLE RESEARCH BLOG, July 22, 2009, **http://googleresearch.blogspot.com/2009/07/posted-by-hal-varian-chief-economist.html**.

27 *See* M. P. CLEMENTS & DAVID F. HENDRY, GREAT BRITAIN STATISTICS COMMISSION, FORECASTING IN THE NATIONAL ACCOUNTS AT THE OFFICE FOR NATIONAL STATISTICS (2003); Jennifer L. Castle & David Hendry, *Nowcasting from Disaggregates in the Face of Location Shifts*, June 18, 2009, **http://www.economics.ox.ac.uk/members/jennifer.castle/Nowcast09JoF.pdf** [hereinafter Castle & Hendry, *Nowcasting*].

28 For a technical overview, *see* TREVOR HASTIE, JEROME FRIEDMAN, & ROBERT TIBSHIRANI, THE ELEMENTS OF STATISTICAL LEARNING: DATA MINING, INFERENCE, AND PREDICTION (2d ed. 2009).

29 *See* Castle & Hendry, *Nowcasting*, *supra* note 27.

## Enabling Experimentation

As Ronald Coase has said, "If you torture the data long enough it will confess."[30] It is difficult to establish causality from retrospective data analysis. It is thus noteworthy that computer mediation allows one to measure economic activity and also conduct controlled experiments.

In particular, it is relatively easy to implement experiments on Web-based systems. Such experiments can be conducted at the query level, user level, or geographic level.

In 2008, Google ran 6,000 experiments involving Web search which resulted in 450-500 changes in the system.[31] Some of these experiments were with the user interface and some were basic changes to the algorithm.[32] The ad team at Google ran a similar number of experiments, tweaking everything from the background color of the ads, to the spacing between the ads and search results, to the underlying ranking algorithm.

In the 1980s, Japanese manufacturers touted their "kaizen" system that allowed for "continuous improvement" of the production process.[33] In a well-designed Web-based business, there can be continuous improvement of the product itself—the website.

Google and other search engines also offer various experimental platforms to advertisers and publishers such as "Ad Rotation," which rotates ad creatives (*i.e.,* the wording of the ad) among various alternatives to choose the one that performs best and "Website Optimizer," a system that allows websites to try different designs or layouts and determine which performs best.

Building a system that allows for experimentation is critical for future improvement, but it is too often left out of initial implementation. This is unfortunate, since it is the early versions of a system that are often most in need of improvement.

---

30 Gordon Tullock, *A Comment on Daniel Klein's 'A Plea to Economists Who Favor Liberty'*, 27 EASTERN ECONOMIC JOURNAL 205 (No. 2, Spring 2001), *available at* **http://college.holycross.edu/RePEc/eej/Archive/Volume27/V27N2P203_207.pdf**.

31 Rob Hoff, *Google Search Guru Singhal: We Will Try Outlandish Ideas, BUS. WEEK*, Oct. 2009, **http://www.businessweek.com/the_thread/techbeat/archives/2009/10/google_search_g.html**.

32 *Id.*

33 For more information on the Japanese kaizen philosophy, *see* MASAAKI IMAI, KAIZEN: THE KEY TO JAPAN'S COMPETITIVE SUCCESS (1986).

Cloud computing, which I will discuss later in the essay, offers a model for "software as service," which typically means software is hosted in a remote data center and accessed via a Web interface. There are numerous advantages to this architecture. It allows for controlled experiments which can, in turn, lead to continuous improvement of the system. Alternatives such as packaged software make experimentation much more difficult.

Ideally, experiments lead to understanding of causal relations that can then be modeled. In case of Web applications there are typically two "economic agents": the users and the applications. The applications are already modeled via the source code that is used to implement them, so all that is necessary is to model the user behavior. The resulting model will often take the form of a computer simulation that can be used to understand how the system works.

Some examples of this are the Bid Simulator and Bid Forecasting tools offered by Google and Yahoo!.[34] These tools give an estimate of the cost and clicks associated with possible bids. The cost per click is determined by the rules of the auction and can be calculated directly; the clicks are part of user behavior and must be estimated with economic forecasting. Putting them together creates a model of the auction outcomes.

## How Experiments Change Business

Because computer mediation drastically reduces the cost of experimentation, there have been changes for the role of management. As Kohavi *et al.* have emphasized, decisions should be based on carefully controlled experiments rather than "the Highest Paid Person's Opinion (HiPPO)."[35]

If experiments are costly, utilizing expert opinions by management is a plausible way to make decisions. When experiments are inexpensive, however, they are likely to provide more reliable answers than opinion, even the opinions of highly paid experts. Furthermore, even when experienced managers have better-than-average opinions, it is likely that there are more productive uses of their time than to sit around a table debating which background colors will appeal to Web users. The right response from managers to such questions should be to "run an experiment."

---

34 For more information on Bid Simulator and Bid Forecasting, *see* Louise Rijk, *Bid Simulator Adds More Transparency to Google AdWords Bidding*, INTERNET MKTG. & BUS. REV., Aug. 10, 2009, **http://www.advmediaproductions.com/newsletter/NL_google-adwords-bid-simulator.html**.

35 Ron Kohavi, Roger Longbotham, Dan Sommerfield, & Randal M. Henne, *Controlled Experiments on the Web: Survey and Practical Guide*, 19 DATA MINING & KNOWLEDGE DISCOVERY 140-181 (2008) **http://www.springerlink.com/content/r28m75k77u145115**.

Businesses have always engaged in experimentation in one form or another. The availability of computer mediated transactions has, however, made these experiments much more inexpensive and flexible than in the past.

## Enabling Customization & Personalization

Finally, computer mediated transactions allow for customization and personalization of interactions by basing current transactions on earlier transactions or other relevant information.

Instead of a "one size fits all" model, the Web offers a "market of one." Amazon.com, for example, makes individual suggestions of items to purchase based on an individual's previous purchases, or on purchases of consumers like that individual. These suggestions can be based on "recommender systems" of various sorts.[36]

In addition to content, prices may also be personalized, leading to various forms of differential pricing. There are certainly welfare effects of such personalized pricing. Acquisiti and Varian examine a model in which firms can condition prices based on past history.[37] The ability of firms to extract surplus, they discover, is quite limited when consumers are sophisticated. In fact, firms have to offer "enhanced services" to justify higher prices.

I have previously suggested that there is a "third welfare theorem" that applies to (admittedly extreme) cases with perfect price discrimination and free entry: Perfect price discrimination results in the optimal amount of output sold while free entry pushes profits to zero, conferring all benefits to consumers.[38]

The same type of personalization can occur in advertising. Search engine advertising is inherently customized since ads are shown based on a user's query. Google and Yahoo! offer services that allow users to specify their areas of interest and then view ads related to those interests. It is also relatively common for advertisers to use various forms of "re-targeting" that allow them to show ads based on users' previous responses to related ads.

---

36 Paul Resnick & Hal R. Varian, *Recommender Systems*, 3 COMM'CNS OF THE ASSOC. FOR COMPUTER MACH. 56-58 (March 1997), **http://cacm.acm.org/magazines/1997/3/8435-recommender-systems/pdf**.

37 Alessandro Acquisiti & Hal R. Varian, *Conditioning Prices on Purchase History*. 24 *MKTG. SCI.* 367-381 (2005), **http://www.sims.berkeley.edu/hal/Papers/privacy.pdf**.

38 Hal R. Varian, *Competition and Market Power*, *in* JOSEPH FARRELL, CARL SHAPIRO, & HAL R. VARIAN, EDS., THE ECONOMICS OF INFORMATION TECHNOLOGY: AN INTRODUCTION, 1-46 (Cambridge Univ. Press 2005). For a theoretical analysis of first-degree price discrimination, see David Ulph & Nir Vulkan, *Electronic Commerce, Price Discrimination, and Mass Customisation*, Nov. 2007, **http://vulkan.worc.ox.ac.uk/wp-content/images/combined-paper.pdf**.

## Transactions Among Workers

Thus far, there has been an emphasis on transactions among buyers, sellers and advertisers. But computers can also mediate transactions among workers. The resulting improvements in communication and coordination can lead to productivity gains, as documented in the literature on the impact of computers on productivity.

In a series of works, Paul David has drawn an extended analogy between the productivity impact of electricity at the end of the nineteenth century and the productivity impact of computing at the end of the twentieth century.[39] Originally, factories were powered by waterwheels which drove a shaft and all of the machines in the factory had to connect to this central shaft. The manufacturing process involved moving the piece being assembled from station to station during assembly.

The power source evolved from waterwheels to steam engines to electric motors. Eventually electric motors were attached to each machine, which allowed more flexibility in how the machines were arranged within the factory. However, factories still stuck to the time-honored arrangements, grouping the same sort of machines in the same location-all the lathes in one place, saws in another, and drills in yet another.

In the first decade of the twentieth century, Henry Ford invented the assembly line. Then, the flexibility offered by electric motors became well appreciated.[40] As David demonstrates, the productivity impact of the assembly line was significant, and over the last century, manufacturing has become far more efficient.[41]

---

39 *See* Paul David, *The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox*, 80 AM. ECON. REV. 355-61 (May 1990) **http://ideas.repec.org/a/aea/aecrev/v80y1990i2p355-61.html** [hereinafter David, *Productivity Paradox*]; Paul David, *General Purpose Engines, Investment, and Productivity Growth: From the Dynamo Revolution to the Computer Revolution.*, *in* E. Deiaco, E. Hornel, & G. Vickery, eds., TECHNOLOGY AND INVESTMENT: CRUCIAL ISSUES FOR THE 90S (1991); Paul David, *Computer and the Dynamo: The Modern Productivity Paradox in the Not-too-distant Mirror*, *in* TECHNOLOGY AND PRODUCTIVITY: THE CHALLENGE FOR ECONOMIC POLICY 315-348 (1991).

40 Ford suggests that the inspiration for the assembly line came from observing the meatpacking plants in Chicago, where animal carcasses were hung on hooks and moved down a line where workers carved off different pieces. If you could use this process to dis-assemble a cow, Ford figured you could use it to assemble a car. See HENRY FORD, MY LIFE AND WORK (Doubleday, Page & Co. 1923).

41 I do not mean to imply that the only benefit from electric motors came from improved factory layout. Motors were also more efficient than drive belts and the building construction was simpler. See David, *Productivity Paradox*, *supra* note 39.

I want to extend David's assembly line analogy to examine "knowledge worker productivity."[42] Prior to the widespread use of the personal computer, producing office documents was a laborious process. A memo was dictated to a stenographer who later typed the document, making carbon copies. The typed manuscript was corrected by the author and circulated for comments. As with pre-assembly line production, the partially-produced product was carried around to different stations for modification. When the comments all came back, the document was re-typed, re-produced and re-circulated.

In the latter half of the twentieth century, there were some productivity enhancements for this basic process, such as White-Out, Post-it Notes, and photocopy machines. Nonetheless, the basic production process remained the same for a century.

When the personal computer became widespread, editing became much easier, and the process of collaborative document production involved floppy disks. The advent of email allowed one to eliminate the floppy disk and simply mail attachments to individuals.

All of these effects contributed to improving the quantity and quality of collaborative document production. However, they all mimicked the same physical process: circulating a document to individuals for comments. Editing, version control, tracking changes, circulation of the documents and other tasks remained difficult.

Nowadays, there is a new model for document production enabled by "cloud computing."[43] In this model, documents live "in the cloud," meaning in some data center on the Internet. The documents can be accessed at any time, from anywhere, on any device, and by any authorized user.

Cloud computing dramatically changes the production process for knowledge work. There is now a single master copy that can be viewed and edited by all relevant parties, with version control, check points and document restore built in. All sorts of collaboration, including collaboration across time and space, have become far easier.

---

42 See Peter F. Drucker, *Knowledge-worker Productivity: The Biggest Challenge*, 41 CAL. MGMT. REV. 79-94 (1999).

43 Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, & Matei Zaharia, *Above the Clouds: A Berkeley View of Cloud Computing*, Feb. 10, 2009, **http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html** [hereinafter *Above the Clouds*]. *See also*, Wikipedia, *Cloud Computing*, **http://en.wikipedia.org/wiki/Cloud_computing**.

Instead of passing the document amongst collaborators, a single master copy of the document can be edited by all interested parties (simultaneously if desired). By allowing workflow to be re-organized, cloud computing changes knowledge worker productivity the same way that electricity changed the productivity of physical labor.

## Enabling Deployment of Applications

As previously mentioned, cloud computing offers what is referred to as "software as a service." This architecture reduces support costs and makes it easier to update and improve applications.

Cloud computing, however, does not only offer "software as a service." It also offers "platform as a service," which means that software developers can deploy new applications using the cloud infrastructure.

Nowadays, it is possible for a small company to purchase data storage, hosting services, an application development environment, and Internet connectivity "off the shelf" from vendors such as Amazon.com, Google, IBM, Microsoft, and Sun.

The "platform as a service" model turns a fixed cost for small Web applications into a variable cost, dramatically reducing entry costs. Computer engineers can both explore the combinatorial possibilities of generic components to create new inventions and can actually purchase standardized services in the market in order to deploy those innovations.

This development is analogous to the recent history of the book publishing industry. At one time, publishers owned facilities for printing and binding books. Today, due to the strong economies of scale inherent in this process, most publishers have outsourced the actual production process to a few specialized book production facilities.

Similarly, in the future, it is likely that there will be a number of cloud computing vendors that will offer computing on a utility-based model. This production model dramatically reduces the entry costs of offering online services, and will likely lead to a significant increase in businesses that provide such specialized services.[44]

The hallmarks of modern manufacturing are routinization, modularization, standardization, continuous production, and miniaturization. These practices have had a dramatic impact on manufacturing productivity in the twentieth

---

44 *Above the Clouds*, *supra* note 43.

century. The same practices can be applied to knowledge work in the twenty-first century.

Computers, for example, can automate routine tasks such as spell-checking and data retrieval. Communications technology allows tasks to be modularized and routed to the workers best able to perform those tasks. Similar to how the miniaturization of the electric motor allowed physical production to be rearranged in 1910, the miniaturization of the computer—from the mainframe, to the workstation, to the PC, to the laptop, and to the mobile phone—allows knowledge production to be rearranged on a local and global scale.

## Enabling Micro-Multinationals

An interesting implication of computer mediated transactions among knowledge workers is that interactions are no longer constrained by time or distance.

Email and other tools allow for asynchronous communication over any distance, which allows for optimization of tasks on a global basis. Knowledge work can be subdivided into tasks, much like physical work in Adam Smith's hypothetical pin factory.[45] But even more, those tasks can be exported around the world to where they can most effectively be performed.

For example, consultants at McKinsey routinely send their PowerPoint slides to Bangalore for beautification. There are many other cognitive tasks of this sort that can be outsourced, including translation, proofreading, document research, *etc.* Amazon.com's Mechanical Turk is an intriguing example of how computers can aid in matching up workers and tasks.[46] As of March 2007, there were reportedly more than 100,000 workers from 100 countries who were providing services via the Mechanical Turk.[47]

The dramatic drop in communications costs in the last decade has led to the emergence of what I have termed "micro-multinationals."[48] Nowadays, a 10- or 12-person company can have communications capabilities that only the largest

---

45 ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 18-21 (Edwin Cannan, ed., Methuen & Co., Ltd. 1904) (1776), **http://www.econlib.org/library/Smith/smWN.html**.

46 Wikipedia. *Amazon Mechanical Turk*, **http://en.wikipedia.org/wiki/Amazon_Mechanical_Turk**.

47 Jason Pontin, *Artificial Intelligence, with Help From the Humans*, N.Y. TIMES, March 25 2007, **www.nytimes.com/2007/03/25/business/yourmoney/25Stream.html ?ex=1332475200en=cd1ce5d0bee647d5ei=5088partner=rssnytemc=rss**.

48 Hal Varian, *Technology Levels the Business Playing Field*, N.Y. TIMES, Aug. 25 2005, **http://www.nytimes.com/2005/08/25/business/25scene.html**.

multinationals could afford 15 years ago. Using tools like email, websites, wikis, voice over IP, and video conferencing, tiny companies can coordinate workflow on a global basis. By sending work from one time zone to the next, these companies effectively work around the clock, giving them a potential competitive advantage over firms that are restricted to one time zone.

Many micro-multinationals share a common history: A student comes to the United States for graduate school. They use the Internet and the collaborative tools available in scientific workgroups. Some get bitten by the start-up bug. They draw on their friends and colleagues back home, who have other contacts living abroad. The collaborative technologies previously mentioned allow such loose groups to collaborate on producing computer code, which may end up as a working product.

As Saxenian has pointed out, "emigration" means something quite different now than it did 30 years ago.[49] As she puts it, a "brain drain" has been replaced by a "brain circulation." We now have a host of collaborative technologies that allow an immigrant to maintain ties to his social and professional networks in his home country.

## Conclusion

I began this essay with a discussion of combinatorial innovation and pointed out that innovation has been so rapid in the last decade because innovators around the world can work in parallel, exploring novel combinations of software components. When the innovations are sufficiently mature to be deployed, they can be hosted using cloud computing technology and managed by global teams, and even by tiny companies. Ideally, these new services can serve as building blocks for new sorts of combinatorial innovation in business processes that will offer a huge boost to knowledge worker productivity in the future.

---

49 ANNALEE SAXENIAN, THE NEW ARGONAUTS: REGIONAL ADVANTAGE IN A GLOBAL ECONOMY (2006).

# Decentralization, Freedom to Operate & Human Sociality

By Yochai Benkler*

## Three Stories of Innovation in the Networked Information Economy

In 1994, two groups of software engineers were working on the next generation of critical software: a Web server; the software that a website runs to respond to requests from users. One group was within Microsoft, understanding that the next generation of critical infrastructure would be the Web, and trying to extend its market from the operating system to the Web server. The other was a group of developers led by Brian Behlendorf, formerly from the group of academic computing engineers from the University of Illinois in Urbana-Champagne, who were patching up the server developed in tandem with the development of Mosaic, the first graphical interface to access the Web, at Urbana-Champagne. They called it a patchy server, which became the name of the resulting open source project: Apache server. Anyone who would have predicted that the system, built by a scrappy set of developers, who adopted a licensing approach that asserted no exclusive rights over their output, and were working in an area considered strategically critical by the largest company in the field and that was developing a product in direct competition, would win would have been laughed out of the room. And yet, it moves (as Galileo famously said, defending his theories of the Earth's orbit around the Sun). Over 15 years, through two boom and bust cycles, Apache has held 50-60% of the market share in Web servers (in the summer of 2010, it was about 55%), while Microsoft's Web server market share has hovered between 25% and 35% (about 25% in summer of 2010).

In 1999, two of the most insightful economists looking at the new rules for the information economy opened their book with an analysis of how Microsoft's move into the market in encyclopedias embodied the new challenges created by the digital economy. In February of 2001, the developer of one of several ongoing efforts to develop an online encyclopedia half gave up and dumped about 900 stubs onto an open source platform, under a license that let anyone edit it and gave no one power to veto. This made participation easy, but control relatively hard. And no one was paid to write or edit the encyclopedia. It was probably the ugliest technical system for encyclopedia development being experimented with at the time. Five years later, this ugly duckling would be

* **Yochai Benkler** is the Berkman Professor of Entrepreneurial Legal Studies at Harvard, and faculty co-director of the Berkman Center for Internet and Society.

identified by a study done by the staff at *Nature* as having roughly similar error rates as Britannica for science articles. By 2009, Microsoft's Encarta encyclopedia product was discontinued. Wikipedia has come to embody the fundamental changes we have to deal with when trying to understand the networked information economy.

In 2001 a Swedish and Danish entrepreneur invested in software developed by three Estonian programmers and released a brilliant new solution for peer-to-peer file sharing: Kazaa. Thanks to the fact that the firm was based in the Netherlands, where Dutch law provided it greater immunity from suit by record labels, Kazaa quickly became a major platform after the demise of Napster.[1] By 2003, the same group of entrepreneurs and programmers had launched a peer-to-peer voice telephony application built on the same basic architecture as Kazaa: Skype. Theoretically, Skype should not have worked. For close to two decades, the Internet Protocol's "first-come, first-served," treat-all-packets-on-a-best-efforts-basis approach was thought to prevent serious voice over Internet applications from working well. And yet, here was this small company providing better quality, encrypted, end-to-end communications, using the users' own computers and connections as its basic infrastructure. They did not need to control the flow of packets in the network to provide Quality-of-Service assurances. They just provided service of a quality that was good enough for the price: free for calls from one Skype user to another, soon followed by very low rates for calls to regular phones. In 2005, eBay bought Skype for over $2.5 billion.

## Radical Decentralization of Physical, Human & Social Capital

The three stories above outline the basic transformative elements of the networked information economy. We have seen a radical decentralization of the most important forms of capital in the most advanced sectors of the economy: physical, human, and social capital. For the first time since the Industrial Revolution, the most important inputs into the core economic activities of the most advanced economies are widely distributed in the population. Technologically, the change begins with physical capital: Processing, storage, communications, and sensing hardware have come to be developed in packages of sufficiently low cost to be put in service by individuals for their own personal use. These advances are capable of mixing consumer use with production activities. The rapid increase in physical capabilities emphasizes continuous rapid innovation as a core dimension of growth and welfare which, in turn, emphasizes human capital.

---

[1] Napster itself was a college dorm room experiment, one of many that flourished at that time, which dramatically and permanently changed the landscape of the music industry.

Human capital too is, by nature, widely distributed in the population, and is extremely sticky and hard to aggregate or transfer effectively from one individual to another. While we measure education when we try to quantify human capital, that is far from all of what human capital really entails. Certainly it does partly entails acquired, codified knowledge of the kind we get in education; but that is only one part of it. Creativity, insight, experience—all these go into answering the critical question: Will this individual come up with an idea, and even more importantly, will this interaction and conversation among a given set of individuals result in an interesting set of ideas emerging?

Organizationally, the increased emphasis on interactions among human beings responding to surprising new opportunities has increased the importance of loosely-coupled interactions beyond slower-moving group boundaries like firms. These new organizational frameworks and the cooperative dynamics they require depend on lightweight, flexible mechanisms that we all carry for interacting with other people. That is, they depend on human sociality. This basic set of protocols for non-destructive human interaction is also fundamentally and widely shared in the population. They are not locked up in the cabinets of smart corporate lawyers' incorporation forms or major deal documents. They are the core social and psychological features of human beings that have co-evolved, physically and culturally, to allow us to be the kinds of social creatures we in fact are—warts and all.

This distributed network of human beings, possessing the physical, human, and social capital that they do, are now connected in a global network of communications and exchange that allows much greater flow and conversation, so that many new connections are possible on scales never before seen. Together, these mean that conversations and new ideas—but more importantly, pilots, experiments, and toy implementations of these new ideas—are cheap and widespread, and innovation happens everywhere, all the time, at low cost. The vast majority of ideas go nowhere, just as the vast majority of experiments fail. But the sheer scale of experimentation has meant that the network has reliably provided the flow of innovation that we have come to expect and depend on, and it has largely come from unpredictable corners rather than from yesterday's innovators or the previous decades' large firms.

As a result of these basic dynamics, in the networked information economy, experimentation, continuous learning and improvement, low-cost prototyping, deployment, iteration, and adoption are more important than well-behaved innovation investments. Social behavior plays a much larger productive economic role than it could when physical capital requirements meant that, however good an idea someone had, transitioning it to a platform that could actually be adopted by consumers/users was simply too expensive to do except through a system of contracts and investment—through a more-or-less formal corporate model. In the networked information economy, *freedom to operate is*

*more important than power to appropriate*, and *voluntarism and sociality are more important than formal contract, and play an important role alongside corporate organization.*

## Freedom to Operate is More Important than Power to Appropriate

The story of open source software is the core story about the importance of freedom to operate and loosely-coupled association that transcends contract and corporate structure. What makes a software development project "open source" is that the output of the development activity, the code, is released under a copyright license that allows anyone to look at, modify, and redistribute the code and modifications to it. This means that anyone, anywhere, can come to the state of the art in the code, adopt it, adapt it, and release it, building on the innovative contributions of others with complete freedom to operate with and on it. In a networked environment where human capital resides in many places, and where it is impossible for anyone firm to hire all the smartest people (or more to the point, to hire all the people who are likely to have the most relevant and powerful insights for any new challenge), a system that depends on open access to the universe of available resources, projects, and collaborators on them will outperform a system that only allows people who have already been identified, recruited, and contracted with based on past projections of what would be important for working on a new problem.

The licensing aspect of open source software raises another important aspect of change. Historically, assuring the owner of financial capital of the soundness of an entrepreneur was the critical factor. To do so, it was necessary to possess property in core inputs, and a network of contracts for flows of what could not reliably or efficiently be owned, like supply relations. Today, assuring a steady and reliable flow of complementary contributions from other developers is as important to maintain a high rate of innovation, experimentation, and adaptation as securing the complementary financial inputs. At the early stages, complementary contributions from other developers are *more* important than financial inputs.

With the rise of peer production, radically distributed collaborative production on the open source model, adoption of licensing terms like those of free and open source software, or Creative Commons, becomes an important avenue to secure those complimentary human investments in the project. Where it is impossible to assure that you will always employ the right people, open source licensing has become an increasingly common strategy for entrepreneurs and large firms alike to improve the probability that they will be able to attract the complimentary rapid development contributions they need, in the time frame they need it, on currently-unpredicted challenges to assure high-velocity innovation. Formalized freedom to operate, in the form of open source licensing, is coupled with a strong pre-commitment by the firms that undertake

the limitations it imposes on their power to appropriate, so as to assure potential collaborators against defection with regard to the fruits of the common, firm-boundary-crossing enterprise. Increasingly this is also becoming a way for firms that compete in some domains, such as software services, to engage in pre-competitive cooperation on the development of core necessary tools, like the Linux kernel and operating system, the Apache Web server, *etc.*

## Voluntarism & Sociality Become More Important than Formal Contract

Another important characteristic of the networked information economy is the critical role of knowledge and creativity. These require uniquely human inputs, and are persistently uncontractible. That is, you can neither define for explicit codification nor characterize for monitoring over time, what it means to be creative, or insightful, or usably knowledgeable in context where an innovation challenge occurs. As a result, tacit knowledge and insight are necessarily and always imperfectly defined for, or monitored through, contract. To assure the right motivations and orientation towards finding new solutions to challenges, it is necessary for an economy at large, as it is for any given organization, to harness the non-contractible motivations of individuals to the knowledge and innovation task at hand. This is not new, in the sense that literature on high-commitment, high-performance organizations has been around for decades, and management theory keeps flowing back and forth between periods that emphasize explicit material rewards and monitoring to control employees shirking their responsibilities, and periods where the limitations of those approaches become clearer, and the benefits of models that depend on a more holistic, human view of what is required to create a motivated workforce prevail.

In the networked information economy, where so much of what needs to be done is uncontractible and so many of those who need to be engaged are not even in a position to have a contractual relationship, the role of sociality and cooperative human systems designs that aim to engage, and depend on social, moral, and emotional motivations as well as, and often instead of, material motivations, has become much larger. Wikipedia, in my three stories, stands as the ultimate example of a system that critically depends on these non-material motivational vectors, mediated through a technical-social platform that is optimized to engage these motivations and allow people to cooperate over a system that provides great freedom to operate, no power to appropriate, and tremendous room for social organization and interaction (which all have their own warts and bumps).

Rather than the traditional formal modes of organization—be they a formal corporation based on contracts, or formal, stable associations on the model of rotary clubs or unions—the new forms of social networks (not the

Facebook/MySpace-type websites, but the actual social phenomenon) permit people to have more loosely-coupled social associations, in which they can participate for some of the time, and combine their investments with many others who are similarly loosely-tied to each other, and may spend their time at different rates, and in different enterprises, during the course of their day, week, or year. Together, these new forms of loose association, based on social signals rather than price signals or a formal corporate managerial hierarchy, form what I have called peer production. They are not, by any stretch of the imagination, going to replace all production activities built on more formal, structured models. Anyone who claims that the argument is one of replacement misunderstands the claim.

The new models of production do, however, come to play a significant productive role in an environment that continues and will continue to be occupied by more traditional forms. They create new sources of competition—as in the case of Wikipedia displacing Encarta—and new forms of complementary sources of innovation and other inputs—as in the case of open source software and the software services industry. They do not herald the death of traditional market/firm-based production. To argue otherwise would be silly. But it would be equally silly to simply assume away a major new organizational innovation. *Peer production and cooperative human systems are a new way to harness a latent but massively productive force. They make the line between production and consumption fuzzy, and offer new pathways to harness the time, insight, experience, wisdom and creativity of hundreds of millions of people around the world to perform tasks that, until a decade ago, we only knew how to perform through formal models of employment and contract.* They are an organizational innovation that anyone ignores at their peril. Just ask the Departments of Defense or State how they feel about WikiLeaks.

## Innovation Anywhere & Everywhere Over an Open Network

The story of Skype rounds out the core changes that the networked information economy presents. In the mid-twentieth-century, the epitome of innovation was Bell Labs. With enough Nobel laureates to make the most ambitious academic physics departments green with envy and massive investment from monopoly profits, Bell Labs is where we got the transistor on which the entire information economy is built. It is, indeed, where we got information theory itself. The Bell system also epitomizes the organizational model of the mid-twentieth-century. "One System, One Policy, Universal Service" was how the company's legendary President, Theodore Vail, put it 100 years ago.[2] According to this model of thought, if the Internet was ever to carry that most delay-

[2] AT&T, *Milestones in AT&T History*, **http://www.corp.att.com/history/milestones.html** (last accessed Aug. 17, 2010).

sensitive of all services, voice, we would have to change how we manage packets. Best effort delivery[3] just wouldn't do it. Someone needed to manage the network and decide—this packet, which carries voice, is more latency sensitive, while that packet, which carries email or a Web page, can wait. But, as it turns out, this persistent prediction was false. And the people who proved it false were not working for Bell Labs. Indeed, it was probably impossible for anyone inside one of the current incarnations of the Bell system to have done so. It was, instead, left to three Estonian developers and a couple of Dutch and Danish edgy entrepreneurs to do so. They were not the only ones to try. Others did too—VocalTec in Israel was among the first; but they were too early.

The point is that in a global networked information environment, innovation can come from anywhere; insights of various forms can find each other, and experimentation and implementation are cheap to do from anywhere to anywhere else. Massive experimentation is followed by massive failures. But the failures are generally cheap, at least by societal standards. And the successes can be readily disseminated, adopted, and generalized on a major global scale in very short time frames. Variation, selection, adaptation and survival/replication through user adoption, rather than planning and high investment, have repeatedly offered the more robust approach in this new complex and chaotic environment. Rapid, low cost experimentation and adaptation on a mass scale, underwritten by the ease of cheap, fast implementation and prototyping, and cheap widespread failure punctuated by a steady flow of unpredictable successes have been more important to innovation and growth in the networked economy than models of innovation based on higher-cost, more managed innovation aimed at planning for predictable, well-understood returns.

## Implications for Human Systems Design

We live our lives through systems: organizational systems, like corporations, states, or nonprofits; technical systems, like the interstate highway system or the Internet; institutional systems like law, both public and private, or social conventions; and cultural, as in our belief systems for how we know things to be true, such as religion, or science. To a great extent, these systems are too complex for us to construct deterministic, fully understood interventions that will clearly lead to desired outcomes, along whatever dimension we think is important: efficiency, freedom, security, or justice. But we nonetheless apply ourselves to the task. We try to use management science to design better organizational strategies; we try to use law to refine and improve our legal

---

[3] "Best effort delivery describes a network service in which the network does not provide any guarantees that data is delivered or that a user is given a guaranteed quality of service level or a certain priority." Wikipedia, *Best effort delivery*, **http://en.wikipedia.org/wiki/Best_effort_delivery** (last accessed Aug. 17, 2010).

system; we invest enormous amounts in designing better technical systems, and so forth.

The characteristics of the networked information economy require that in our efforts at systems design we emphasize openness and freedom to operate over control and power to appropriate and that we emphasize human sociality and diverse motivations for diverse types over optimizing for material interests and letting everything else sort itself out. At a practical level, technical open design has made the largest and most powerful steps. Anchored in the very decision to separate TCP from IP, and make the core Internet protocol as open as it can be, and continuing to the central role that open standards have played in the development of the Web, XML, and WiFi, to name just a few, a continuous emphasis on openness already has substantial support and inertia, although it is always under pressure from firms that think they can get an edge by owning a de-facto standard, or controlling a technical choke point that would allow them to extract rents. In management science, we are seeing, slowly and in some senses at the periphery, efforts to learn the lessons of open source software and apply them to collaboration across firm boundaries and strategic management of the knowledge ecology that a firm occupies.

In law, the most important battleground in the tension between the control-oriented approach and the freedom-to-operate approach is intellectual property. Only this year Amazon received a patent for social networking[4] that reads more-or-less like a description of Facebook, launched four years before Amazon had even filed its patent application. But not everything is so silly. This summer, the Librarian of Congress exempted iPhone jailbreaking from the Digital Millennium Copyright Act's anti-circumvention provisions.[5] If there is any single policy domain in which it is important to apply what we have learned about the new networked information economy, it is in the area of intellectual property. It is also the area where there is the largest potential for intellectual and political programmatic overlap between libertarians and progressives.

---

4 Stan Schroeder, *Amazon Patents Social Networking System, Winks at Facebook*, MASHABLE/TECH, June 17, 2010, **http://mashable.com/2010/06/17/amazon-patents-social-networking-system/**.

5 Copyright Office, Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, July, 28, 2010, **http://www.copyright.gov/1201/**.

# A Common Agenda on Intellectual Property for the Networked Information Economy

From the perspective of economic analysis, information is a public good. Once someone creates new information or knowledge, anyone can use it without reducing its availability for anyone else. Its marginal cost is therefore zero, and that is its efficient price. However, for information to be available at a price of zero, the person who produced it must find some other mechanism to extract value from their investment in creating the information. Otherwise, having information available at its marginal cost today (zero) will lead to less production tomorrow.

The overwhelming majority of information, knowledge, and culture is produced without the need to rely on explicit, intellectual-property-based mechanisms to appropriate its benefits. Firms continuously innovate in their processes so as to lower their costs and improve their profits; but they do generally not patent their innovations and license them or exclude competitors from using them. Individuals innovate and develop experience about their workplace to improve their own performance; people read news and create commentary for each other, and appropriate the benefits of what they find socially. Governments invest in R&D and reap the benefits through higher growth, greater military might, *etc.* Nonprofits and academic institutions invest in information, knowledge, and cultural production, and so forth. All these approaches have their own advantages and disadvantages; but economic survey after survey for the past few decades has shown that even in industrial innovation, a minority of sectors relies on patents, and the majority relies on a range of supply-side and demand-side improvements in appropriability that come from developing the information and either using it without exchanging it or disseminating it and relying on first-mover advantages, network effects, marketing and reputational benefits, *etc.*

The only industries that are still dependent on intellectual property protections are the pharmaceutical industry for patents and Hollywood, the recording industry, and much of book publishing for copyright. Even newspapers and magazines are not so dependent on IP. They are, rather, advertising-supported media. They depend on release of the information to capture demand-side benefits for their paying clients in a two-sided market—the advertisers.

The reason that it is important to remember this quick recap of innovation and Patents & Copyrights Economics 101 is that it helps us to see that patents and copyrights represent a government decision to prohibit everyone from using ideas or information that they can practically use, in order to serve a public purpose—supporting a subset of business models for the creation of new information, knowledge, and culture. Now, it is perfectly acceptable for

government to prohibit some actions in order to serve the public good. We prevent companies from selling food unless it is labeled in certain ways to serve public health; we prohibit violence to increase public security, and so forth. But we try to do so only when there is indeed a good reason.

Sometimes, we combine prohibitions with a market in permissions. Tradeable emissions permits are a classic example where we think it is more efficient to allow firms to trade in their permissions than to simply have direct regulation. Patents and copyrights are exactly like tradeable emissions permits. They are a market-based approach toward the regulatory problem of how to prevent people who want to use the existing universe of information and knowledge that they possess in ways that will undermine future knowledge production and innovation. We prohibit everyone from using certain classes of information and knowledge, and we create a market in permissions to use that information. We call these permissions "copyrights" or "patents." What is important to remember is that these permissions markets create a drag on freedom to operate on current innovation and knowledge creation, and they create a drag on innovation in all industries that, unlike pharmaceutical or blockbuster movie markets, do not heavily depend on such permissions markets.

For progressives, the best way to understand patents and copyrights is through the prism of free speech: These are government regulations on what and how we can say things; and how we can use what we know, that are implemented in pursuit of legitimate government ends—aiding innovation and creative expression by some industries—at the expense of that freedom. As with any limitation on speech and learning, it has to be supported by very good reasons. It is not at all clear whether our contemporary economic understanding of the functioning of copyright law in particular, and patent law to a lesser extent, provide sufficient support for such significant restrictions on free speech.

For libertarians, the best way to understand patents and copyrights is as a regulatory system that imposes limitations on how individuals can act on knowledge they possess in pursuit of their own goals. It is a regulatory system that creates and allocates permissions to generate market-based transfer mechanisms; but a regulatory system in pursuit of a government program, which embodies the judgment that certain business models used to sustain innovation and expression are more effective than others, and supports those deemed more effective *at the expense of those other approaches.*

Both approaches should lead to a significant downward revision in the level of acceptable intellectual property enforcement that the United States pursues. Let me offer one example, which provides the basic structure of the problem: How long should a copyright last? If we thought that copyrights were really property, the answer would be something like forever. The U.S. Constitution, as well as the laws of practically every other country, instead limit the term of copyright,

understanding that there is a big difference between the need of exclusivity in a thing that, if one person uses, another cannot, and exclusivity in an idea or expression that anyone can use without making it any less available for anyone else. The former is a proper object of property. The latter is a proper object of regulation of individual freedom for so using the thing, but only to the extent justified by property.

So how long should copyright terms be? Let's try this thought experiment: Imagine that you are someone with an idea for a movie. You walk in to a group of hypothetical investors and you tell them: "Here's my idea, here's the audience for it, and so here is my projection for how much money we will make on it." The investors ask you: "What are your assumptions about timing? By when will we see our return?" Now, imagine that you answered: "We won't really break even in the first seventy years, but just you wait until years seventy to ninety-five: We'll be making millions!" You would be laughed out of the room. "OK, let's try it with not making money the first twenty years, but making a killing in the years twenty to thirty." You get the point.

If copyright is intended to assure that there is enough appropriability to attract investment in creating a new expression, but it is a regulatory form that restrains the freedom of others to operate in pursuit of that goal, then its term should be keyed to the term necessary to attract investors. Given today's discount rates in the relevant industries—that is, how quickly investors need to turn a profit before they will decide to put their money in some other enterprise—that likely means 18 months; maybe it means three to five years. It is possible that different industries have different levels of patience. But fundamentally, the overwhelming majority of the social cost created by the 95-year term of copyright—let alone the repeated practice of retroactive extension of copyright for works already created in response to the then-existing incentives-system—is incurred without any benefit for investment purposes. No sane investor today cares about returns on an investment in these kinds of fields (as opposed to, say, power plants or utilities) that are ten years out. For software, maybe the correct period is 18 months; for novels, maybe 10 years, although even there, the relevant party is the publisher's decision to publish, not the author's decision to write—because copyright-based monetization runs through the publisher's business decision, not the author's. In patents, maybe the correct period is 20 years for pharmaceuticals. Maybe more; or maybe less. But the principle for all these is the same: The period of copyright or patent protection should be backed out of reasonable investment assumptions and discount rates, not pulled out of the lobbying process, which is always skewed in favor of the small number of firms that possess these rights and against the millions of potential innovators who do not yet know that this or that piece of regulated access to information will get in their way five years from now.

The details of what might go on a major intellectual property reform that should be supported by both libertarians and progressives may differ among commentators. The core structure of the reasons for change are the same: (a) Strong patents and copyrights benefit some business models over others, and in particular place a strong drag on the radically distributed, chaotic, innovation-everywhere-by-everyone model of the networked information economy in favor of twentieth-century models of much more stable and controlled markets like those of Hollywood and the recording industry; (b) There is a big difference between the level of exclusivity needed to attract investment at the margin, and the level of exclusivity that maximizes its owner's ability to extract rents; the size of the difference between the minimal necessary to attract innovation and the rent-maximizing level of protection is equal to the amount the incumbents are willing to spend on lobbying to keep the line at the maximal point, as opposed to the minimally-necessary point; and (c) The lines in fact should be drawn where the marginal effect is to attract investment, not where rents can be maximized. The academic community has spent years trying to refine a set of interventions that could improve access to information, knowledge and culture, while having minimal impact on incentives to invest. The following represent some of the most promising of these ideas.

- **Copyright term:** Copyright terms should be keyed to actual market requirements and the discount rate in the business. Copyright that is any longer than necessary to attract the marginal investor that makes a difference between the project happening or not represents pure rent extraction and is a drag on innovation and creativity.
- **Renewal of existing copyrights:** There are mountains of existing materials (animal shots from documentaries from the 1960s; explosions and action shots from 1970s B movies; *etc.*) that could provide the grist for new models of creative mashup tools and sites, but instead sit unused and unusable because the rights are excessively tied up. Existing copyrights should be required to be renewed periodically, initially for a nominal price, and later on in the life of a copyright for escalating fees, rising to a level no greater than necessary to make a copyright owner think: is their *any* real market for this thing, rather than focing holders to make fine distinctions about the value of the work, on one hand, or simply automatically renewing everything, whether or not it has any market, because it's cheaper to renew than to review continued viability. Those works that continue to be of even small commercial value will be renewed. Those that continue to be of emotional significance will be renewed. All others will become freely usable upon failure to re-register.

- **Reinstate the *Sony* doctrine[6] by legislative reversal of the Supreme Court's *Grokster* decision[7]** – In the midst of the panic over peer-to-peer filesharing, the Supreme Court moved away from its long-standing precedent that an innovator cannot be forced to foresee and prevent the potentially-infringing uses of its new product (in the *Sony* case, the VCR). As long as there are substantial noninfringing uses, innovators are immune to suit by copyright owners whose works are being infringed by users of the innovator's product. In *Grokster* the Supreme Court created a more intention-based, fact-intensive inquiry that imposes greater litigation risk on entrepreneurs who innovate on the Net with anything that can possibly be used to infringe existing copyrights. This is an unnecessary drag on Internet innovation and entrepreneurship in favor of the movie and recording industries.
- **Eliminate business methods patents:** Few innovations are as unnecessary as a law intended to give business people an incentive to improve their business model. The incentive to develop a new business model is that it makes more money for its inventor. There is no need for an additional government-granted monopoly on doing business in this way. The Federal Circuit, which created this new doctrine 12 years ago, tried to walk it back in the *Bilski* case,[8] but the Supreme Court recently held[9] that the particular way that the federal Circuit went about doing so was indefensible. Nonetheless, it appears that a majority of the Supreme Court would support some other, better-reasoned reversal.
- **Eliminate software patents:** There is fairly significant evidence that software patents are unnecessary, and that software development is heavily based on service models, time to market, network effects, customer habits, *etc.* On the other hand, patents get in the way of open source development, and throw a monkey wrench into the model of rapid innovation by anyone, anywhere, distributable everywhere. They create unnecessary barriers to entry that reduce the freedom to operate and experiment, and thereby harm innovation.

---

6 *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), available at **http://en.wikipedia.org/wiki/Sony_Corp._of_America_v._Universal_City_Studios,_Inc**.

7 *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), available at **http://en.wikipedia.org/wiki/MGM_Studios,_Inc._v._Grokster,_Ltd**..

8 *In re Bilski*, 545 F.3d 943, 88 U.S.P.Q.2d 1385 (Fed. Cir. 2008), available at **http://en.wikipedia.org/wiki/In_re_Bilski**.

9 *Bilski v. Kappos*, 561 U.S. ___, 130 S. Ct. 3218 (2010), available at **http://en.wikipedia.org/wiki/Bilski_v._Kappos**.

- **Create a "band" of exempt experimentation, both commercial and non-commercial, whereby use of existing copyrighted or patented information or knowledge does not trigger liability:** Today, to the extent that there are exemptions they are spare and niggardly. Using just three notes from a prior recording and mashing them up into a completely new song does not, under present copyright law, count as "de minimis."[10] Academic experimentation on a patented drug that does not result in any alternative drug that competes but merely begins to create the path to one does not come within patent law's "research exemption."[11] These attitudes—none forced by the language of the statutes—reflect a judicial temperament that seems to think of copyright and patents in a Blackstonian "sole and despotic dominion"[12] mindframe, an approach that was never true of real property under common law, and would, even in terms of pure theory, be disastrous if applied to knowledge and information. The idea would be to develop a relatively robust space for experimentation which, if it led to products and sales, would entitle the owner of the prior, enabling innovation or creative expression to claim some share of the profits of the downstream innovator or creator. The critical point of such an approach would be to allow millions of experiments to run without liability or its risk, while at the same time assuring that truly enabling innovations for those experiments that do succeed can share in the commercial upside of their contributions to downstream innovation.
- **Continue to expand the exemptions from the Digital Millennium Copyright Act[13] wherever that Act's provisions place a drag on interoperability and innovation in systems that depend on access to existing platforms and systems:** Federal courts have begun to reject claims under the DMCA that are efforts by copyright owners to use digital rights management to throw a monkey wrench into the works of a competitor. For example, Lexmark tried to make it hard for competitors who wanted to compete on toner for its printers by creating a chip and software handshake between the printer and the toner cartridge. When a competitor reversed engineered the handshake so that their microchip-enabled toner cartridge could work with

---

10 *Bridgeport Music, Inc. v. Dimension Films*, 410 F.3d 792 (6th Cir. 2005), available at **http://en.wikipedia.org/wiki/Bridgeport_Music,_Inc._v._Dimension_Films**.

11 *Madey v. Duke University*, 307 F.3d 1351 (2002).

12 SIR WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, Book II Ch. II , Clarendon Press (Oxford) 1765-1769, available at **http://en.wikipedia.org/wiki/Commentaries_on_the_Laws_of_England**.

13 17 U.S.C. §§ 1201-1205, available at **http://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act#Anti-circumvention_exemptions**.

> Lexmark printers, Lexmark argued that in order to build their competing cartridge, the competitor had to make a copy of the handshake software, which in turn required them to get around the encryption protecting that piece of copyrighted software. In other words, the competitor had violated the DMCA by circumventing the digital rights management encryption that protected their copyrighted handshake software. The court rejected the argument, emphasizing that a program copy whose core function was interoperability did not violate the DMCA.[14]

In this short a piece, I neither aim for an exhaustive list nor offer a detailed analysis of each of the proposals identified. Instead, I offer these as an initial draft of a range of policies that would increase freedom to operate in the networked information economy, and reduce the drag of the current system of copyrights and patents on both commercial and social enterprises that have played a critical role in the explosive innovation we have experienced on the Internet in the past decade and a half.

## Conclusion

The networked information environment has introduced a period of radically decentralized capitalization of some of the core economic sectors in the most advanced economies. As a result, growth is coming to depend increasingly on innovation from individuals and companies at the edges, operating as the few successful experiments out of thousands of similar experiments that go nowhere. Many of these experiments are commercial. Many are non-commercial. Many combine the two. As a system, this open, chaotic, complex innovation system requires freedom to operate. It needs to take advantage of its technical, economic, and social structure more than it needs power to control uses as in prior models of well-behaved appropriation. Moreover, the diversity of models of experimentation, and the increasingly fuzzy line between production and consumption, between the social and the economic, suggest that for purposes of economic production and growth, formal contract and corporate structure are playing a less important role than they did in the prior century relative to the increasingly important role played by loosely-structured voluntarism and human sociality.

---

14 Lexmark International, Inc. v. Static Control, 387 F.3d 522 (6th Cir. 2004).

# The Economics of Information: From Dismal Science to Strange Tales

By Larry Downes*

## Heroes

It was a fight over nothing.

In 2008, 12,000 members of the Writers Guild of America staged a withering strike against the major Hollywood studios. It lasted three months, interrupted dozens of TV series, and delayed several big-budget films. The two sides reportedly lost more than $2 billion. Yet the sole issue in the dispute was when and how revenues from the Internet and other digital distribution of entertainment would be allocated.[1]

So far, no such revenues exist.

Online distribution of movies and especially TV is a recent phenomenon, powered by ever-faster data transmission speeds, the continued spread of broadband technologies into the home, and improved protocols for file compression. It seems certain that profitable models for delivering Hollywood content to computers, personal digital assistants (PDAs), cell phones, and other non-TV devices will emerge. But in these early days, as with music before it, it isn't clear what those models will be. Will they be supported by advertising? Will content be pay-per-view or based on all-you-can-eat subscriptions? Will consumers prefer to own or rent?

As industry ponders these unanswerable questions, consumers are doing much of the innovating themselves as they did with earlier, less bandwidth-intensive content such as text and music. Users of YouTube, BitTorrent, and all variations of video streaming or file-sharing applications, in the interest of speed

---

* **Larry Downes** is an Internet analyst and consultant, helping clients develop business strategies in an age of constant disruption caused by information technology. He is the author of **UNLEASHING THE KILLER APP: DIGITAL STRATEGIES FOR MARKET DOMINANCE** (Harvard Business School Press 1998) and, most recently, of **THE LAWS OF DISRUPTION: HARNESSING THE NEW FORCES THAT GOVERN LIE AND BUSINESS IN THE DIGITAL AGE** (Basic Books 2009). This essay is adapted from THE LAWS OF DISRUPTION.

1 Michael White & Andy Fixmer, *Hollywood Workers Return to Work After Ending Strike*, BLOOMBERG, Feb. 13, 2008, **http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aKdwR9oC54WM**.

and experimentation, do not bother with the niceties of obeying the law (Viacom's $1 billion lawsuit against YouTube and Google is currently on appeal).[2]

Why did the two sides risk so much fighting over revenue that doesn't yet exist from channels that haven't been invented? The writers say they took a stand in large part because they did not do so in the early days of videocassette sales and rentals. When the profitable models finally arrived, the writers believed they got a much worse deal. Because media sales and rentals now represent the largest share of entertainment income, missing the boat has been painful for writers.

The studios argued that until it is clear how and when money is to be made from digital distribution, pre-assigning residual royalties to writers would limit the studios' ability to experiment with different distribution and partnership models. They made the same argument with videotapes.

Ultimately, new rates for residual royalties were agreed upon for categories including downloaded rentals and sales, ad-supported streaming media, short clips, and promotional uses. Whether these prove to be favorable rates, or even the right categories, remains to be seen. Either way, media will continue to migrate to the Internet at the expense of other forms of distribution.

## The Strange Behavior of Non-Rivalrous Goods

It is hard to say if anyone made the right decisions in the writers' strike, in part because the tools for valuing information products and services, even for present uses, are terrible. You will look in vain at the balance sheets of companies whose sole assets are information—including much of the entertainment industry, as well as professional services such as doctors, lawyers, and consultants—to find any useful measure of the current or future value of the company's real assets. While management gurus sing the praises of developing a company's intellectual capital, financial reporting systems ignore it.

Accountants refer to all the valuable information in a business—its information assets—as intangibles. As the name suggests, these are assets that never take a physical form as do factories and inventory. Unlike physical assets, information assets are generally not counted in calculating the total worth of an enterprise. For the most part, a company's human resources, brands, and good relationships with customers and suppliers—let alone its copyrights, patents, trade secrets, and trademarks—are left off its balance sheet. The value of the

---

2 *See* Adam Ostrow, *Viacom Loses $1 Billion Again YouTube*, MASHABLE, June 23, 2010, **http://mashable.com/2010/06/23/youtube-wins-viacom-lawsuit/**.

company's information, at least as far as accounting is concerned, is basically nothing.

Why? Accountants have argued for years that information and other intangibles are so different economically from material goods that traditional methods of valuation just don't apply. As an asset, the explanation goes, information behaves precisely the opposite of its tangible counterparts: Capital assets lose value as they are used, equipment becomes obsolete, and raw materials are depleted. Brands and reputations, by contrast, become more valuable the more they are exercised, in theory generating revenue forever. You cannot determine the price of a logo or a customer relationship with the same tools you use to depreciate a tractor.

Fair enough. But that doesn't explain why accountants have done so little to develop valuation techniques that apply to information assets. A dangerous result of that failure is that few managers understand information or how it generates value. Even CEOs of large companies regularly get it wrong when they talk casually about "trademarking an idea" or "copyrighting a word." (You cannot do either.)

As information becomes more central to economic performance, the failure to account for its value has become dangerous. Executives, especially in public businesses, are compensated based on the health of their companies' balance sheets. To the extent that information value doesn't appear there, it's understandable that many companies don't put much, if any, effort into developing or managing those assets.

That's unfortunate because the strategic cultivation of information assets is beneficial in many ways. Consider Harrah's Entertainment, which operates casinos worldwide in places where gambling is legal.

When former business school professor Gary Loveman joined the company as chief operating officer in 1998, he decided to look for underutilized assets on the company's balance sheet. He found them in Harrah's data warehouse. Like most casino chains, Harrah's had implemented a rewards program that gave customers special benefits for using their membership cards while playing slot machines. Harrah's was collecting vast amounts of information on its "factory floor," but had done very little to put that data to use.

A detailed review of the collected information upended several long-standing myths about where Harrah's made the most money. Most of the company's profits came from a quarter of its customers. Those customers were not, however, the "cuff-linked, limousine-riding high rollers [Harrah's] and [their]

competitors had fawned over for many years."[3] Instead, Harrah's discovered that the high-profit customers were regular visitors, many of them recent retirees. They made frequent trips to the casino and spent steadily, if modestly, at its gaming tables, restaurants, and hotels.

Harrah's quickly reconfigured its customer-facing activities, including check-in, complimentary meals, and special promotions, orienting them toward the actual, as opposed to the presumed, best customers. The result was a changed enterprise, one that consistently outperforms its competition.

Even though the balance sheet never reported the value of the diamonds Loveman found when he looked in his data mine, his information assets were by no means worthless. In 2006, Harrah's was sold to a private equity partnership at a price that valued the information at more than $1 billion, representing a 30% premium in the total purchase price.[4] Today, Gary Loveman remains CEO of the company, a position he has held since 2003.

The writers' strike and the Harrah's story teach an important lesson about the economics of information. Just because information value is indeterminate doesn't mean it's worthless. Not by a long shot. The Hollywood writers and producers clearly did not think so, nor did the buyers of Harrah's.

Consider another example: Search giant Google has $20 billion in assets, mostly cash, on its balance sheet. The company, however, even on the lowest day of the stock market in ten years, was worth nearly $100 billion—more than five times its book value. Somebody has figured out, at least in part, how to value the company's information assets.

Digital life is made up of information. It comes in a wide range of types, including private data, speech, news and entertainment, business practices, and information products and services such as films, music, inventions, and software. But all information operates under a common set of economic principles. So to thrive in the next digital decade, you must understand the basic elements of information economics.

In modern economic terminology, goods are categorized as either "private" or "public" goods. Most goods in our industrial economy are private goods. Purely private goods are those that can be possessed by only one person at a

---

3 Gary Loveman, Diamonds in the Data Mine, HARV. BUS. REV., May 2003. *See also* Julie Schlosser, *Teacher's Bet,* FORTUNE, March 8, 2004, **http://money.cnn.com/magazines/fortune/fortune_archive/2004/03/08/363688/index.htm**.

4 Ryan Nakashima, *Harrah's Entertainment Accepts Buyout Bid from Private Equity Group*, USA TODAY, Dec. 19, 2006, **http://www.usatoday.com/money/industries/2006-12-19-harrahbuyout_x.htm**.

time ("rivalrous") and whose use can be limited to that person or with whomever she might share it ("excludable"). If I own a barrel of oil, then you don't own it, unless I sell it to you, in which case I no longer have it. Once it's used, it's gone forever—no one has it anymore.

Public goods, by contrast, can be used by more than one person at the same time ("non-rivalrous"), and limiting access to them is difficult, if not impossible ("non-excludable"). The classic example in economics textbooks is national defense. Either everyone has this good or nobody does. The military protects everyone, including those who do not pay taxes. Defensive missiles cannot be programmed to leave a single house unguarded.

Information is an archetypically non-rivalrous good. As Thomas Jefferson famously wrote, "He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me."[5] Once a composer completes a song, there's no physical limit to how many people can perform it simultaneously. There is a cost associated with its creation, but the composer incurs no additional cost no matter how many times the work is played. Regardless of how often it is performed, the composition still exists. In fact, it becomes more valuable the more freely it's shared—it becomes more popular, maybe even a "hit."

So information is non-rivalrous, but is it also excludable? Until recently, the answer in practice was often no. That's because many information products that sprang from the creativity of the human mind could not easily be distributed without first being copied to physical media such as books, newspapers, or, in the case of music, CDs and records. In that transformation ("demassification," in Alvin Toffler's terminology[6]), information lost its excludable property, looking more like the barrel of oil than like national defense. It's easy to limit access to the barrel of oil—there's only one, after all. The song, once recorded and duplicated, is harder to control, but it's still possible to exclude those who didn't pay for a copy or pay for the right, as in radio, to broadcast it.

Information, until recently, was a public good in theory but in practice behaved more like a private good. The need to reduce it to physical media masked its true nature, and gave rise to seemingly incongruous terminology that includes "stealing an idea," "pirating content," and, most significantly, "intellectual property." After more than five hundred years of Gutenberg's moveable type, we're so conditioned to experiencing information through mass-produced media that we equate the cost of the media with the value of the content. As

---

5 Letter from Thomas Jefferson to Isaac McPherson (Aug. 13, 1813), *available at* **http://press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html**

6 *See generally* ALVIN TOFFLER, THE THIRD WAVE (1980).

John Perry Barlow poetically put it, until the advent of electronic distribution through the Internet, "the bottle was protected, not the wine."[7]

For information products, that protection—the ability to exclude—is almost entirely a function of law: The law of copyright makes it a crime to "copy" information without permission. Copyright gives the composer the exclusive right to make or authorize performances of a song, for example, or to record it and produce copies. At the same time, copyright outlaws the production of copies by anyone else, including someone who purchased a legal copy.

By limiting both the performance and production of a song, copyright transforms non-rivalrous information into a rivalrous physical good. But the alchemy of copyright is starting to fail as digital technology makes it easier to distribute songs electronically. Given the Internet, it's now much harder to limit who gets to hear a song and when. A copy no longer requires expensive recording and pressing equipment, or access to a costly and very visible retail distribution network.

Although the composer can legally exclude those who do not buy authorized copies of his work, his ability to police that right is increasingly expensive, often costing more than it's worth. You can't realistically stop people from humming your tune, even if they do it out loud. And now you can't really stop them from sharing copies of a digital recording, either.

Other than the composer herself, however, consumers are also potentially harmed by the transformation of information goods back to their non-rivalrous state. There were and remain important reasons for legal systems that treat information as if it were a rivalrous good.

Copyright, for example, is designed to maximize the value of the up-front investment that information producers must make. If copyright didn't exist, you could simply buy a recording of the song, reproduce it, and sell your own copies. Because your total investment would be only the cost of a single copy, your version would likely be cheaper than the one marketed by the composer himself. In theory, the composer would find it difficult to recover his creative investment, making him less likely to undertake his important work in the first place. Ultimately, everyone would be worse off.

But copyright's value comes at a high price. By imposing costs on the exchange of information that otherwise would not exist, the law neutralizes many of the valuable features of non-rivalrous goods.

---

7 John Perry Barlow, *The Economy of Ideas,* WIRED 2.03, 1994, **http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html**.

Fortunately, this special power is limited. Even with copyright, some forms of sharing are perfectly legal. Libraries can loan out the same copy of a recording to as many people as want to hear or play it, one at a time. Fans who purchased their own copy are likewise free to loan it to their colleagues, or even to resell their copy to a used record store or through online services such as Amazon Marketplace or eBay.

Copyrights also have an expiration date. In the United States, for example, copyrights lasts 70 years beyond the life of the author or 120 years for certain works.[8] After this period, the work is no one's property—the public can use it however they want to. Anyone can perform the work, make copies of it, adapt it, or incorporate it into new works. It becomes forever after a purely non-rivalrous good.

Copyright protection is also limited to the producer's particular expression and not the underlying ideas. The ideas in a song (love conquers all, love stinks) are non-rivalrous from the moment the song is written.

Consider a 1996 court case involving sports statistics. In the days before the Web and wireless data devices, sports fans who were not attending a game could get up-to-the-minute information from a dedicated paging device from Motorola called Sportstrax. Sportstrax employees watched sporting events on TV and entered key information (*e.g.,* who had the ball or who had scored) into a computer system. A few minutes later, Sportstrax customers would be paged with short updates.

Motorola was sued by the National Basketball Association, which claimed the transmission of information by pager violated its copyright in the broadcast of games.[9] The court disagreed. Sporting events are not "authored," the judges noted, and are therefore not protected by copyright in the first place. Game data, including interim scores, are facts, not a particular expression of an information producer. Facts are non-rivalrous, outside the protection of copyright.

Today, pagers have given way to cell phones that can take photographs and videos and share them via the Internet. Popular television programs such as "American Idol" have armies of fans who watch the show and write blogs about each performance even as they're watching them. So long as the actual performances aren't being copied, however, the commentary is perfectly legal.

---

8 17 U.S.C §§ 302- 03.

9 Nat'l Basketball Assoc. v. Motorola, Inc., 105 F.3d 841 (2d Cir. 1997), **http://www.law.cornell.edu/copyright/cases/105_F3d_841.htm**.

As these examples suggest, the challenge for copyright and other laws controlling information has always been to strike the right balance between incentives for creators and the value that the public derives from unfettered use. It's a balance that is constantly being unsettled by new technologies, a problem that has accelerated with the advent of the digital age.

On one hand, information technology has greatly lowered the cost of creating and distributing information including books, movies, and recorded music. But the same technologies have also made it easier to make and distribute unauthorized copies which are, in many cases, perfect replicas of the original. Should information laws be tightened or relaxed in the next digital decade? Do producers need more protection from copyright laws, or do consumers deserve greater freedom? Are new information uses made possible by software applications such as YouTube, Facebook and Flickr, creating more value than they destroy, and for whom?

## The Five Principles of Information Economics

Unfortunately, many of those debating these questions—and there are many, including lawmakers, industry leaders, and consumer groups—don't understand the economic properties of information any better than do the accountants who refuse to measure it. So it's worth summarizing the five most important principles of information economics. It's even better to memorize them:

### Renewability

Information cannot be used up. It can be enhanced or challenged, it can become more or less valuable over time, but once it has been created, it can be used over and over again. In the end it exists as it began. Most new information, moreover, is created from other information, making it a renewable energy source. In electronic form, neither its production nor its use generates waste products that damage the environment. In that sense, information is the ultimate "green" energy.

The online encyclopedia Wikipedia, for example, isn't written by hired experts. It's written by volunteers who post articles on subjects they either know or think they know something about. Within certain limits, anyone else can edit, correct, or change entries. Over time, the articles evolve into a useful and reliable form. No money changes hands in either the creation of Wikipedia or its use.

## Universality

Everyone has the ability to use the same information simultaneously. Blog entries, news articles, and YouTube videos can be enjoyed simultaneously by an unlimited number of people. The only distribution costs are the photons on a screen. Each consumer, moreover, may have a completely different reason for consuming the same information, and perhaps her own response to it. She may be inspired to respond with information of her own.

Facebook, for example, is comprised almost entirely of user-generated content. Users are constantly commenting on status updates, photographs, and other information posted by their friends, and inviting each other to join interest groups or play information games.

## Magnetism

Private goods operate under the law of supply and demand: The greater the supply, the lower the price you can charge for it, and vice versa. The value of information, on the other hand, increases as a function of use. Information value grows exponentially as new users absorb it. The more places my brand or logo appears, the higher the value customers attach to all my goods. Use makes the brand more, not less, valuable.

This increase in value accelerates as the information spreads, creating a kind of magnetic pull that generates network effects. Since no one owns the Internet's protocols, for example, these standards have spread easily, resulting in the explosive growth that began in the 1990s. The standards are now more valuable than when only a few people used them.

## Friction-Free

The more easily information flows, the more quickly its value increases. In electronic form, information can move in any direction at the speed of light. It experiences no decay along the way, arriving at its destinations in the same form as when it departed. For many kinds of information, including languages, religious doctrines, and advertising, the ease of transfer helps to improve society—or at least the profits of those who disseminate it. The cheaper it is to spread the word, the more likely and quickly it will be spread.

There is, however, an inherent paradox: The frictionless spread of information can undermine the incentives for its production. Content producers, including authors, musicians, news organizations, and movie studios, invest heavily in the production of new information. To recover their investment, information producers must charge for its use. Economically, however, even the simplest payment schemes (subscriptions, for example) slow the natural tendency of information to move freely. Since information flows along the path of least

resistance, markets look for ways to avoid fees. In that sense, new technologies often subvert old business paradigms, even when the inventors of those technologies didn't intend for them to do so.

## Vulnerability

Information's value does share one property with tangible goods: It's not indestructible. Value can be destroyed through misuse. If you license your company's name (and thus its reputation) to an inferior product or a product that does not have a clear connection to your brand, you risk confusing consumers about what your brand stands for. Value can also be destroyed by a third party, perhaps a competitor offering a knockoff product that looks like yours but is of lesser quality. Or an identity thief can appropriate your name and credit history to borrow money from banks or credit card companies. When the thief disappears, not only is the money gone, so is your reputation.

Information can also be a victim of its own success. It is now so easy to produce, distribute, and consume information that users are experiencing overload. Today, websites, e-mails, blogs, text messages, and even "tweets"—brief messages that reflect the thoughts of a user on Twitter—all compete for users' limited time. As the sources of information and the volume produced expand rapidly, consumers find it increasingly difficult to limit their exposure to information of real value to them.

* * *

It's easy to see these five principles in action in digital life. Consider Google. One might wonder how a company can be worth anything, let alone $100 billion, when it charges absolutely nothing for its products and services. You can search Google's databases and use its e-mail service day and night without spending a penny; you can store photos on its Picasa photo service, create documents with its online word processing software, view Google Maps, and share videos on its YouTube service for free. Indeed, the company is determined to have as many people as possible take complete advantage of it.

Even though databases and other services are what consumers want and therefore represent the source of the company's value, Google does not hoard those assets as if they were barrels of oil to be used only when necessary. It treats them instead as non-rivalrous goods that increase in value as more people use them.

The company isn't being generous. Google makes nearly all its money by renting out advertising space to companies whose products and services complement the things consumers do when they are using Google. If information "wants to be free," then let it be as free as possible, and make all the profits from the collateral effects of the network. That's the company's

simple business strategy, one that has created remarkable new value even as it disrupts the assumptions of every industry the company touches.

And for social networking sites, just giving away content isn't good enough. These companies also have to find ways to get users to help them develop their sites in the first place. Companies like Facebook, MySpace, and their professional equivalent, LinkedIn, are constantly adding free tools and gadgets to make their products more compelling. Once a service reaches the tipping point (Facebook now has 500 million users!), the search for ways to make money begins in earnest, including premium services and targeted advertisements. But thanks to the weird economics of information, there remain powerful reasons not to charge the users for the core product—ever.

## The Problem of Transaction Costs

There's one additional aspect of information economics that is essential to understand. The frictionless transfer of information and the problem of information overload suggest that the economy of digital life is a kind of machine. Like the best engines, it can operate with remarkable efficiency—provided its parts are kept lubricated and free of foreign matter. Already, technologies perfected during the last digital decade have ruthlessly eliminated waste in our increasingly efficient online lives. Still, the information economy is not perfect. It suffers, like its physical counterpart, from a kind of inefficiency, what economist Ronald Coase first called "transaction costs."

Coase came to the United States from England as an economics graduate student in 1931. Only twenty years old, Coase had a revolutionary agenda. Struggling to reconcile the socialism of his youth with the free-market sensibility of his professors, Coase saw big companies as proof that centralizing activities could work on a grand scale. If he could learn how big companies did it, Coase imagined, then perhaps the lessons could be applied to big governments as well. Oddly enough, no one had ever asked why companies existed, and certainly no one had ever thought to ask the people who were running them.

What Coase learned made him swear off socialism forever, and led to the publication of an article that changed economic thinking forever—an article cited as revolutionary sixty years later, when Coase received the Nobel Prize in Economics.

In "The Nature of the Firm," Coase argued that there is a price not only to what companies buy and sell, but also to the process of buying and selling it.[10] Buyers and sellers have to find each other, negotiate deals, and then

---

10 Ronald H. Coase, *The Nature of the Firm*, 4 ECONOMICA 368-405 (Nov., 1937), **http://aetds.hnuc.edu.cn/uploadfile/20080316211913444.pdf**.

consummate them. This activity was neither especially easy nor without costs. Coase therefore argued that companies were becoming bigger because markets were, relatively speaking, too expensive.

Coase called the price of doing a deal its "transaction cost." The existence of transaction costs, he believed, explained why companies were internalizing more and more activities, especially repeated functions like buying raw materials and marketing. For these activities, maintaining an inside function such as a purchasing department was cheaper than relying for each individual purchase on whoever might happen to be in the market.

To understand why, let's take a simple example. Say you work for an average-size company and you've run out of paper clips. Almost assuredly, you will get your paper clips not by leaving your office to drive to the office supply store but by going down the hall to the supply cabinet, where your company's purchasing department maintains an inventory of basic supplies. Your company will, in fact, keep such basic supplies on hand as a matter of course, without giving much thought to the cost of carrying this inventory. This holds true even if buying and distributing office supplies have nothing to do with what your business does. Your company is likely to keep paper clips on hand even if there is no discount for buying in bulk.

Why? Even if you could get paper clips on your own for the same price, you still have to go out and get them. This means finding the stores that carry them and learning how much they charge. Then you have to choose between the closest store and the one with the best price. At the checkout stand, you need to make sure you are really charged what the store advertises. If the clips are somehow defective, you have to take them back and demand replacements or some other remedy.

And that's just for a simple transaction. Imagine instead that you're buying raw materials needed to manufacture a jet airplane. There is the additional effort of negotiating a price, writing a contract, inspecting the goods, and, potentially, invoking the legal system to enforce the terms and conditions. It's better, you say, to own the supplier or at least to buy in bulk and avoid all that trouble. That "trouble" is transaction costs.

Working from Coase's basic idea, economists have identified six main types of transaction costs:

- **Search costs**: Buyers and sellers must find each other in increasingly diverse and distributed markets.
- **Information costs**: For buyers, learning about the products and services of sellers and the basis for their cost, profit margins, and

quality; for sellers, learning about the legitimacy, financial condition, and needs of the buyer, which may lead to a higher or lower price.

- **Bargaining costs**: Buyers and sellers setting the terms of a sale, or contract for services, which might include meetings, phone calls, letters, faxes, e-mails, exchanges of technical data, brochures, meals and entertainment, and the legal costs of contract negotiations.
- **Decision costs**: For buyers, comparing the terms of one seller to other sellers, and processes such as purchasing approval designed to ensure that purchases meet the policies of the organization; for sellers, evaluating whether to sell to one buyer instead of another buyer or not at all.
- **Policing costs**: Buyers and sellers taking steps to ensure that the good or service and the terms under which the sale was made, which may have been ambiguous or even unstated, are translated into the behavior expected by each party. This might include inspecting the goods and any negotiations having to do with late or inadequate delivery or payment.
- **Enforcement costs**: Buyers and sellers agreeing on remedies for incomplete performance. These include everything from mutual agreements for a discount or other penalties to expensive litigation.

As this list suggests, transaction costs range from the trivial (turning over a box of paper clips to see the price) to amounts greatly in excess of the transaction itself (imagine if you were seriously injured by a defective paper clip flying off the shelf and sticking you in the eye). In fact, economists Douglass North and John Wallis have estimated that up to 45%of total economic activity consists of transaction costs.[11] Eliminating them entirely would translate to a staggering $4.5 trillion in annual savings in the United States alone, eliminating much of the work done by accountants, lawyers, advertisers, and government agencies.

One needn't go that far to improve economic performance, however. Firms are created, Coase concluded, because the additional cost of organizing and maintaining them is cheaper than the transaction costs involved when individuals conduct business with each other using the market. Firms, while suffering inefficiencies of their own, are more efficient at certain types of activities than the market. Technologies—in 1937, Coase had in mind telephones, in particular—improved the performance of one or both, constantly resetting the balance between what was best to internalize and what was best left to the market.

---

[11] John Joseph Wallis & Douglass C. North, *Measuring the Transaction Sector in the American Economy*, *in* LONG-TERM FACTORS IN AMERICAN GROWTH 95-162 (Stanley L. Engerman & Robert E. Gallman, eds. 1986), **http://www.nber.org/chapters/c9679**.

So which functions should a firm perform internally? The deceptively-simple answer is only those activities that cannot be performed more cheaply in the market or by another firm. In fact, as Coase says, a firm will tend to expand precisely to the point where "the costs of organizing an extra transaction within the firm become equal to the costs of carrying out the same transaction by means of an exchange on the open market."[12]

For some activities, say plumbing, the open market works relatively well, and the need for plumbers to form large firms to avoid transaction costs has never arisen. For the large-scale operations of integrated manufacturers, such as Boeing and General Motors, which require coordination, heavy capital investment, and complex distribution systems, the firm is the only economically viable solution.

Coase believed economists should turn their attention to the practical problem of uncovering transaction costs wherever they occur and eliminating those that are unnecessary. Doing so, he hoped, would, among other things, help reduce the need for government intervention. A great deal of regulation and liability laws, Coase argued, were unconscious efforts to overcome transaction costs for certain types of activities, such as accidents and pollution. But the regulations themselves generate so many transaction costs that in many cases doing nothing at all would have produced a better result. To find out how much law and regulation are optimal requires a better understanding, once again, of the costs involved.

Coase had hoped his elegant proof would get economists working on the real problem at hand. Ironically, all he did was make economics more esoteric. Instead of lowering themselves to the kind of empirical research that was common in other social sciences, economists simply dispose of Coase in an opening footnote. They "assume a frictionless economy" and then proceed to develop elaborate mathematical models of behavior in a purely theoretical universe. Rather than join his quest, most economists retreated to more abstract models of economic behavior, which Coase dismisses as little more than a "vast mopping-up exercise" of loose ends left by Adam Smith's seminal 18th century work, *The Wealth of Nations*.

Increasingly frustrated with his economist colleagues, Coase instead took up residence at the University of Chicago's law school. Economists, he came to see, avoided information, and misused the few sources, such as government data, that were readily available. Economics had become a shell game. "If you torture the data enough," he wrote, dismissing much of modern economic

---

12 Coase, *The Nature of the Firm*, *supra* note 10.

analysis, "nature will always confess."[13] If that was all economists could do, Coase decided he was no economist. Awarded the Nobel Prize in 1991, Coase began his acceptance speech on a note of despair. "In my long life I have known some great economists," he told the committee, "but I have never counted myself among their number nor walked in their company."[14]

Look at the performance of the economy over the past twenty years and it's easy to sympathize with Coase's frustration. The "rational" stock market still booms and busts. Cyclical industries continue to overexpand and then overcontract. Efforts at creating an open global economy without trade barriers are met with rioting mobs. National banking regulators read every tea leaf they can find and still go to bed wondering if they have cut rates too soon or too late, too much or too little, or even if their cuts have made an iota of difference. While most economists fiddle with formulas, the economy is burning. Without a better understanding of the nature of transaction costs, we'll never be able to predict—let alone improve—what seem to be the most basic elements of economic behavior.

That, in any case, is the real world. In the digital world, the problem is not only less severe, but also solvable. The free flow of information made possible by digital technology is decreasing the friction of transaction costs in a variety of interactions. From global price comparisons to searches of much of the world's knowledge to auctions for anything, the cost of deal-making is plummeting. The Internet is driving down all six types of transaction costs. That's what's made the Internet so disruptive in the last decade, and what will continue to drive dramatic consumer, business, and regulatory changes in the next digital decade.

Consider a few examples:

1. **Search costs**: Technology connects people across geographical, time, and national borders. Automatic notifications for obscure collectibles on eBay, finding old friends through the "People You May Know" feature on Facebook, or letting your TiVo pick programs for you that it thinks you might like to watch—each of these reduces search costs, sometimes dramatically. Restaurant and other business reviews available directly on cell phones make it easier to find just the right place no matter where you are. There's even an iPhone application uses GPS technology to help you find your car in a crowded parking lot!

---

13 Ronald H. Coase, *How Should Economists Choose?*, G. Warren Nutter Lecture in Political Economy, American Enterprise Institute (1982).

14 Ronald H. Coase, *Nobel Prize Lecture*, Dec. 9, 1991, **http://nobelprize.org/nobel_prizes/economics/laureates/1991/coase-lecture.html**.

2. **Information costs**: Technology creates standard data structures that can be searched and consolidated over a growing network of computers. The asymmetry of sellers concealing data has eroded, radically changing the way people buy cars, real estate, and investment securities. Free or subscription services including CarFax, Zillow, and Yahoo! Finance give buyers an abundance of valuable information that was previously inaccessible at any price. Online dating services such as Chemistry.com increasingly use sophisticated profiling technology to suggest compatible matches.

3. **Bargaining costs**: The exchange of information can now take place digitally and is captured in databases for easy reuse in subsequent transactions. Instant publication of classified ads on Craigslist means many local transactions are completed within minutes. Business-to-business transactions increasingly rely on libraries of standard terms. The nonprofit Association for Cooperative Operations Research and Development (ACORD), for example, uses the XML data standard to create standard forms used by insurance and reinsurance agents and brokers offering life, property, and other lines of products.

4. **Decision costs**: Visibility to expanded online markets gives both buyers and sellers a better picture of minute-to-minute market conditions. Several insurance websites, including Progressive.com, provide instant quotes and comparisons to the prices of their competitors. Cell phone users can compare prices from online merchants while shopping at retail stores, putting added pressure on merchants to match or beat those prices or offer other incentives, including delivery or after-sales support. Online gamers can check the reputation of potential participants to decide whether to allow them to join their teams.

5. **Policing costs**: Transactions conducted with system-to-system data transfers create a more complete record of the actual performance of the participants, which can then be captured and queried. For goods purchased online, most merchants now provide direct access to detailed shipping and tracking information from expediters such as UPS or FedEx or even standard delivery from the postal service. Some merchants, including Dell Computers, provide information about the manufacturing process, allowing customers to track their products before they are even shipped. Most software products now collect bug and other failure information in real time, automatically installing updates and repairs. Players of the online World of Warcraft game can "speak" directly to in-game employees or robots whenever they have a problem.

6. **Enforcement costs**: Electronic records can simplify the process of resolving disputes over what was agreed upon or what did or did not occur. Online payment services such as PayPal offer elaborate dispute resolution

functions that include mediation and arbitration when buyers and sellers cannot resolve their differences, along with insurance and guaranteed satisfaction. These are all supported by the collection of end-to-end transaction data documenting the actual performance of buyers and sellers. Bloggers can quickly whip up electronic mobs to put pressure on companies, politicians, or celebrities whose behavior they feel does not comply with agreed-upon standards.

## Conclusion: Conflicts at the Border

Digital technology, as I argued in my 1998 book, "Unleashing the Killer App,"[15] has created a corollary to Coase's observation about business organizations. As transaction costs in the open market approach zero, so does the size of the firm—if transaction costs are nonexistent, then there is no reason to have large companies. For products constructed entirely or largely out of information, we now stand on the verge of what Don Tapscott and Anthony Williams call "peer production," where just the right group of people come together to apply the right set of skills to solve complex problems, whether in business or otherwise.[16] I called this phenomenon "The Law of Diminishing Firms."

Technology is changing the dynamics of firms, making them smaller but more numerous. This, however, is good for the overall economy. Efficiency translates to savings of time, money, and decreased waste. Productivity, customer satisfaction, and the availability of customized products and services have improved dramatically. Keeping in touch across time zones and long distances gets easier, as does organizing diverse groups of people for social, political, or business reasons. The average consumer can now edit an online encyclopedia, post news and photos as a citizen journalist, or operate a home-based business that can produce and distribute just about anything.

Now for the bad news. Our current legal system, forged in the factories of the Industrial Revolution, was designed to maximize the value of rivalrous goods. It cannot be easily modified to deal with the unique economic properties of information. Worse, the crushing overhead of regulations and lawsuits, which may no longer be cost-effective even in the physical world, adds even less value when applied to the lower-transaction-cost-environment of digital life.

Increasingly, the old rules do little more than hold back innovation for the benefit of those who cannot or do not know how to adapt to the economics of digital life. In many cases, inefficient laws are propped up by failing businesses

---

15 LARRY DOWNES & CHUNKA MUI, UNLEASHING THE KILLER APP: DIGITAL STRATEGIES FOR MARKET DOMINANCE (1998).

16 DON TAPSCOTT & ANTHONY WILLIAMS, WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING (2003).

that are not eager to see their advantages erased. Sometimes those fighting transformation are powerful business interests, including large media companies, real estate agents, and even some of the technology companies whose products fuel the digital revolution.

Resistance may also come from the users themselves. In digital life, private information can be invaluable in deciding who to interact with, either for business or for interpersonal transactions. As advances in technology bring more private information online, powerful emotions have been activated. Citizens in much of the world believe their rights to privacy are being violated, not only by businesses but by their classmates and neighbors.

Perhaps most worrisome, governments are taking advantage of lower transaction costs to improve the technology of surveillance, raising fears of the dystopic world described by George Orwell in his novel "1984."

Lower transaction costs have also proven useful to criminals and terrorists, who operate freely and anonymously in digital realms. Sometimes their crimes exploit the vulnerability of information, as in the case of identity theft and other forms of Internet fraud. More ominously, virtual gangs are able to attack the infrastructure of the Internet itself, releasing viruses and other harmful software that incapacitate servers, destroy data, or, in the case of spam, simply waste people's most precious resource: time.

Perhaps the most difficult problems of information economics, however, involve the plasticity of information in electronic form. Technology has made it possible to realize the remarkable potential of information to be shared and even enhanced by as many people as are interested. Inevitably, every new innovation that supports this creative urge runs headlong into laws protecting information as property—laws that treat public goods as if they were private goods. Although such laws may be necessary, they have proven unduly rigid in their current form, sparking some of the most vitriolic fights on the digital frontier.

The explosion of digital technology at home, at work, and in government, coupled with the economics of information, has created a perfect storm. Our industrial-age legal system will not survive this social transformation. After the flood, as in previous technological revolutions, a new legal paradigm will emerge to guide the construction of laws better suited to digital life.

Implementing these new laws will require a great deal of coordination and collaboration. Most of all, it will require considerable courage on the part of those who live in both the physical and digital worlds. The next digital decade, like the last one, will proceed in fits and starts, with surprising changes of cast and characters, allies becoming enemies and enemies finding common ground.

Some winners and losers will prove, in retrospect, to have been easily predicted. Others will come from nowhere.

The only thing certain is the author of the script: the poorly-understood but increasingly critical economic properties of information.

# The Regulation of Reputational Information

By Eric Goldman*

## Introduction

This essay considers the role of reputational information in our marketplace. It explains how well-functioning marketplaces depend on the vibrant flow of accurate reputational information, and how misdirected regulation of reputational information could harm marketplace mechanisms. It then explores some challenges created by the existing regulation of reputational information and identifies some regulatory options for the future.

## Reputational Information Defined

Typical definitions of "reputation" focus on third-party cognitive perceptions of a person.[1] For example, *Black's Law Dictionary* defines reputation as the "esteem in which a person is held by others."[2] Bryan Garner's *A Dictionary of Modern Legal Usage* defines reputation as "what one is thought by others to be."[3] The Federal Rules of Evidence also reflect this perception-centric view of "reputation."[4]

---

* Associate Professor and Director, High Tech Law Institute, Santa Clara University School of Law. Email: **egoldman@gmail.com**. Website: **http://www.ericgoldman.org**. In addition to a stint as General Counsel of Epinions.com, a consumer review website now part of the eBay enterprise, I have provided legal or consulting advice to some of the other companies mentioned in this essay. I prepared this essay in connection with a talk at the Third Annual Conference on the Law and Economics of Innovation at George Mason University, May 2009.

1 As one commentator explained:

> Through one's actions, one relates to others and makes impressions on them. These impressions, taken as a whole, constitute an individual's reputation—that is, what other people think of you, to the extent that their thoughts arise from what they know about you, or think they know about you.

Elizabeth D. De Armond, *Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation*, 41 VAL. U.L. REV. 1061, 1065 (2007).

2 BLACK'S LAW DICTIONARY (8th ed. 2004).

3 BRYAN A. GARNER, A DICTIONARY OF MODERN LEGAL USAGE (1990).

4 *See*, *e.g.*, FED. R. EVID. 803(19), 803(21).

Although this definition is useful so far as it goes, I am more interested in how information affects prospective decision-making.[5] Accordingly, I define "reputational information" as follows:

> information about an actor's past performance that helps predict the actor's future ability to perform or to satisfy the decision-maker's preferences.

This definition contemplates that actors create a pool of data (both subjective and objective) through their conduct. This pool of data—the reputational information—can provide insights into the actor's likely future behavior.

## Reputation Systems

"Reputation systems" aggregate and disseminate reputational information to consumers of that information. Reputation systems can be mediated or unmediated.

In unmediated reputation systems, the producers and consumers of reputational information communicate directly. Examples of unmediated reputation systems include word of mouth, letters of recommendation and job references.

In mediated reputation systems, a third-party publisher gathers, organizes and publishes reputational information. Examples of mediated reputation systems include the Better Business Bureau's ratings, credit reports/scores, investment ratings (such as Morningstar mutual fund ratings and Moody bond ratings), and consumer review sites.

The Internet has led to a proliferation of mediated reputation systems, and in particular consumer review sites.[6] Consumers can review just about anything online; examples include:

- eBay's feedback forum,[7] which allows eBay's buyers and sellers to rate each other.
- Amazon's product reviews, which allows consumers to rate and review millions of marketplace products.
- Yelp.com, which allows consumers to review local businesses.

---

5 Luis M.B. Cabral, *The Economics of Trust and Reputation: A Primer* (June 2005 draft), **http://pages.stern.nyu.edu/~lcabral/reputation/Reputation_June05.pdf** (treating information about reputation as inputs into Bayesian calculations).

6 Indeed, this has spurred the formation of an industry association, the Rating and Review Professional Association. **http://www.rarpa.org**.

7 **http://pages.ebay.com/services/forum/feedback.html**.

- TripAdvisor.com, which allows consumers to review hotels and other travel attractions.
- RealSelf.com, which allows consumers to review cosmetic surgery procedures.
- Avvo.com, which allows consumers to rate and review attorneys.
- Glassdoor.com, which allows employees to share salary information and critique the working conditions at their employers.
- Honestly.com,[8] which allows co-workers to review each other.
- RateMyProfessors.com, which allows students to publicly rate and review their professors.
- DontDateHimGirl.com, which allows people to create and "find profiles of men who are alleged cheaters."[9]
- TheEroticReview.com, which allows johns to rank prostitutes.[10]

## Why Reputational Information Matters

In theory, the marketplace works through an "invisible hand": consumers and producers make individual and autonomous decisions that, without any centralized coordination, collectively determine the price and quantity of goods and services. When it works properly, the invisible hand maximizes social welfare by allocating goods and services to those consumers who value them the most.

A properly functioning invisible hand also should reward good producers and punish poor ones. Consumers allocating their scarce dollars in a competitive market will transact with producers who provide the best cost or quality options. Over time, uncompetitive producers should be drummed out of the industry by the aggregate but uncoordinated choices of rational and informed consumers.

However, given the transaction costs inherent in the real world, the invisible hand can be subject to distortions. In particular, to the extent information

---

8 Honestly.com was previously called Unvarnished. *See* Evelyn Rusli, *Unvarnished: A Clean, Well-Lighted Place For Defamation*, TECHCRUNCH, Mar. 30, 2010, **http://techcrunch.com/2010/03/30/unvarnished-a-clean-well-lighted-place-for-defamation/**.

9 PlayerBlock is a similar service, tracking undesirable dating prospects by their cellphone number. *See* Leslie Katz, *Is Your Date a Player? Send a Text and Find Out*, CNET News.com, Oct. 22, 2007, **http://news.cnet.com/8301-10784_3-9802025-7.html**.

10 *See* Matt Richtel, *Sex Trade Monitors a Key Figure's Woes*, N.Y. TIMES, June 17, 2008. PunterNet is another website in this category, providing reviews of British sex workers. John Omizek, *PunterNet Thanks Harriet for Massive Upswing*, THE REGISTER, Oct. 5, 2009, **http://www.theregister.co.uk/2009/10/05/punternet_harman/**.

about producers is costly to obtain or use, consumers may lack crucial information to make accurate decisions. To that extent, consumers may not be able to easily compare producers or their price/quality offerings, in which case good producers may not be rewarded and bad producers may not be punished.

When information is costly, reputational information can improve the operation of the invisible hand by helping consumers make better decisions about vendors. In this sense, reputational information acts like an invisible hand guiding the invisible hand (an effect I call the "secondary invisible hand"), because reputational information can guide consumers to make marketplace choices that, in aggregate, effectuate the invisible hand. Thus, in an information economy with transaction costs, reputational information can play an essential role in rewarding good producers and punishing poor ones.

Given this crucial role in marketplace mechanisms, any distortions in reputational information may effectively distort the marketplace itself. In effect, it may cause the secondary invisible hand to push the invisible hand in the wrong direction, allowing bad producers to escape punishment and failing to reward good producers. To avoid this unwanted consequence, any regulation of reputational information needs to be carefully considered to ensure it is improving, not harming, marketplace mechanisms.

Note that the secondary invisible hand is, itself, subject to transaction costs. It is costly for consumers to find and assess the credibility of reputational information. Therefore, reputation systems themselves typically seek to establish their own reputation. I describe the reputation of reputation systems as a "tertiary" invisible hand—it is the invisible hand that guides reputational information (the secondary invisible hand) to guide the invisible hand of individual uncoordinated decisions by marketplace actors (the primary invisible hand). Thus, the tertiary invisible hand allows the reputation system to earn consumer trust as a credible source (such as the Wall Street Journal, the New York Times or Consumer Reports) or to be drummed out of the market for lack of credibility (such as the now-defunct anonymous gossip website JuicyCampus).[11]

## Thinking About Reputation Regulation

This part explores some ways that the regulatory system interacts with reputation systems and some issues caused by those interactions.

---

11 Matt Ivester, *A Juicy Shutdown*, JUICYCAMPUS BLOG, Feb. 4, 2009, **http://juicycampus.blogspot.com/2009/02/juicy-shutdown.html**.

## Regulatory Heterogeneity

Regulators have taken divergent approaches to reputation systems. For example, consider the three different regulatory schemes governing job references, credit reporting databases and consumer review websites:

- Job references are subject to a mix of statutory (primarily state law) and common law tort regulation.
- Credit reporting databases are statutorily micromanaged through the voluminous and detailed Fair Credit Reporting Act.[12]
- Consumer review websites are virtually unregulated, and many potential regulations of consumer review websites (such as defamation) are statutorily preempted.

These different regulatory structures raise some related questions. Are there meaningful distinctions between reputation systems that support heterogeneous regulation? Are there "best practices" we can observe from these heterogeneous regulatory approaches that can be used to improve other regulatory systems? These questions are important because regulatory schemes can significantly affect the efficacy of reputation systems. As an example, consider the differences between the job reference and online consumer review markets.

A former employer giving a job reference can face significant liability whether the reference is positive or negative.[13] Giving unfavorable references of former employees can lead to defamation or related claims;[14] and there may be liability for a former employee giving an incomplete positive reference.[15]

Employers may be statutorily required to provide certain objective information about former employees.[16] Otherwise, given the potentially no-win liability regime for communicating job references, most knowledgeable employers

---

12 15 U.S.C. §§ 1681-81x.

13 *See* Tresa Baldas, *A Rash of Problems over Job References*, NAT'L L.J., Mar. 10, 2008 ("Employers are finding that they are being sued no matter what course they take; whether they give a bad reference, a good reference or stay entirely silent.").

14 1-2 EMPLOYMENT SCREENING § 2.05 (Matthew Bender & Co. 2008) (hereinafter "EMPLOYMENT SCREENING").

15 Randi W. v. Muroc Joint Unified Sch. Dist., 14 Cal. 4th 1066 (1997).

16 These laws are called "service letter statutes." *See* EMPLOYMENT SCREENING, *supra* note 14. Germany has a mandatory reference law requiring employers to furnish job references, but in response German employers have developed an elaborate system for coding the references. Matthew W. Finkin & Kenneth G. Dau-Schmidt, *Solving the Employee Reference Problem*, 57 AM. J. COMP. L. 387 (2009).

refuse to provide any subjective recommendations of former employees, positive or negative.[17]

To curb employers' tendency towards silence, many states enacted statutory immunities to protect employers from lawsuits over job references.[18] However, the immunities have not changed employer reticence, which has led to a virtual collapse of the job reference market.[19] As a result, due to mis-calibrated regulation, the job reference market fails to provide reliable reputational information.

In contrast, the online consumer review system is one of the most robust reputation systems ever. Millions of consumers freely share their subjective opinions about marketplace goods and services, and consumer review websites keep proliferating.

There are several possible reasons why consumer review websites might succeed where offline reputation systems might fail. My hypothesis, discussed in a companion essay in this collection, is that the difference is partially explained by 47 U.S.C. § 230, passed in 1996—at the height of Internet exceptionalism—to protect online publishers from liability for third party content. Section 230 lets websites collect and organize individual consumer reviews without worrying about crippling legal liability for those reviews. As a result, consumer review websites can motivate consumers to share their opinions and then publish those opinions widely—as determined by marketplace mechanisms (*i.e.,* the tertiary invisible hand), not concerns about legal liability.

The success of consumer review websites is especially noteworthy given that individual reviewers face the same legal risks that former employers face when providing job references, such as the risk of personal liability for publishing negative reputational information. Indeed, numerous individuals have been sued for posting negative online reviews.[20] As a result, rational actors should find it imprudent to submit negative reviews; yet, millions of such reviews are published online. A number of theories might explain this discrepancy, but one theory is especially intriguing: Mediating websites, privileged by their own liability immunity, find innovative ways to get consumers over their fears of legal liability.

---

17 *See* Baldas, *supra* note 13.

18 The immunizations protect employer statements made in good faith. EMPLOYMENT SCREENING, *supra* note 14.

19 *See* Finkin & Dau-Schmidt, *supra* note 16.

20 *See*, *e.g.*, Wendy Davis, *Yelp Reviews Spawn At Least Five Lawsuits*, MEDIAPOST ONLINE MEDIA DAILY, Jan. 21, 2009, **http://www.mediapost.com/publications/?fa=Articles.printFriendly&art_aid=98778**; Agard v. Hill, 2010 U.S. Dist. LEXIS 35014 (E.D. Cal. 2010).

What lessons can we draw from this comparison? One possible lesson is that reputation systems are too important to be left to the market. In other words, the tertiary invisible hand may not ensure accurate and useful information, or the costs of inaccurate information (such as denying a job to a qualified candidate) may be too excessive. If so, extensive regulatory intervention of reputation systems may improve the marketplace.

An alternative conclusion—and a more convincing one to me—is that the tertiary invisible hand, aided by a powerful statutory immunity like Section 230, works better than regulatory intervention. If so, we may get better results by deregulating reputation systems.

## System Configurations

Given the regulatory heterogeneity, I wonder if there is an "ideal" regulatory configuration for reputation systems, especially given the tertiary invisible hand and its salutary effect on publisher behavior. Two brief examples illustrate the choices available to regulators, including the option of letting the marketplace operate unimpeded:

**Anti-Gaming**. A vendor may have financial incentives to distort the flow of reputational information about it. This reputational gaming can take many forms, including disseminating false positive reports about the vendor,[21] disseminating false negative reports about the vendor's competitors, or manipulating an intermediary's sorting or weighting algorithm to get more credit for positive reports or reduce credit for negative reports. Another sort of gaming can occur when users intentionally flood a reputation system with inaccurate negative reports as a form of protest.[22]

Do regulators need to curb this gaming behavior, or will other forces be adequate? There are several marketplace pressures that curb gaming, including competitors policing each other,[23] just as they do in false advertising cases.[24] In

---

21 Lifestyle Lift Holding, Inc. v. RealSelf Inc., 2:08-cv-10089-PJD-RSW (answer/counterclaims filed March 3, 2008), **http://www.realself.com/files/Answer.pdf** (alleging that Lifestyle Lift posted fake positive reviews about its own business to an online review website).

22 For example, consumers protesting the digital rights management (DRM) in EA's Spore game flooded Amazon's review site with one-star reviews, even though many of them actually enjoyed the game. *See* Austin Modine, *Amazon Flash Mob Mauls Spore DRM*, THE REGISTER, Sept. 10, 2008, **http://www.theregister.co.uk/2008/09/10/spore_drm_amazon_effect/**. A similar protest hit Intuit's TurboTax 2008 over its increased prices. *See* Steven Musil, *Amazon Reviewers Slam TurboTax Fee Changes*, CNET NEWS.COM, Dec. 7, 2008, **http://news.cnet.com/8301-1001_3-10117323-92.html**.

23 *See* Cornelius v. DeLuca, 2010 WL 1709928 (D. Idaho Apr. 26, 2010) (a marketplace vendor sued over alleged shill online reviews posted by competitors).

addition, the tertiary invisible hand may encourage reputation systems to provide adequate "policing" against gaming. However, when the tertiary invisible hand is weak, such as with fake blog posts where search engines are the only mediators,[25] government intervention might be worth considering.

**Right of Reply**. A vendor may wish to publicly respond to reputational information published about it in an immediately adjacent fashion. Many consumer review websites allow vendors to comment or otherwise reply to user-supplied reviews, but not all do. For example, Yelp initially drew significant criticism from business owners who could not effectively reply to negative Yelp reviews because of Yelp's architecture,[26] but Yelp eventually relented and voluntarily changed its policy.[27] As another example, Google permitted quoted sources to reply to news articles appearing in Google News as a way to "correct the record."[28]

Regulators could require consumer review websites and other reputation systems to permit an adjacent response from the vendor.[29] But such intervention may not be necessary; the tertiary invisible hand can prompt reputation systems to voluntarily provide a reply option (as Yelp and Google did) when they think the additional information helps consumers.

## Undersupply of Reputational Information

There are three primary categories of reasons why reputational information may be undersupplied.

---

24 *See*, *e.g.*, Lillian R. BeVier, *A Puzzle in the Law of Deception*, 78 VA. L. REV. 1 (1992).

25 *See* Press Release, New York Office of the Attorney General, Attorney General Cuomo Secures Settlement With Plastic Surgery Franchise That Flooded Internet With False Positive Reviews, July 14, 2009, **http://www.ag.ny.gov/media_center/2009/july/july14b_09.html**.

26 See Claire Cain Miller, *The Review Site Yelp Draws Some Outcries of Its Own*, N.Y. TIMES, Mar. 3, 2009.

27 *See* Claire Cain Miller, *Yelp Will Let Businesses Respond to Web Reviews*, N.Y. TIMES, Apr. 10, 2009.

28 *See* Dan Meredith & Andy Golding, *Perspectives About the News from People in the News*, GOOGLE NEWS BLOG, Aug. 7, 2007, **http://googlenewsblog.blogspot.com/2007/08/perspectives-about-news-from-people-in.html**.

29 *See* Frank A. Pasquale, *Rankings, Reductionism, and Responsibility*, 54 CLEV. ST. L. REV. 115 (2006); Frank A. Pasquale, *Asterisk Revisited: Debating a Right of Reply on Search Results*, 3 J. BUS. & TECH. L. 61 (2008).

## Inadequate Production Incentives

Much reputational information starts out as non-public (*i.e.,* "private") information in the form of a customer's subjective mental impressions about his/her interactions with the vendor. To the extent this information remains non-public, it does not help other consumers make marketplace decisions. These collective mental impressions represent a vital but potentially underutilized social resource.

The fact that non-public information remains locked in consumers' heads could represent a marketplace failure. If the social benefit from public reputational information exceeds the private benefit from making it public, then presumptively there will be an undersupply of public reputational information. If so, the government may need to correct this failure by encouraging the disclosure of reputational information—such as by creating a tort immunity for sites that host that disclosure, as Section 230 does, or perhaps by going further. But there already may be market solutions to this problem, as evidenced by the proliferation of online review websites eliciting lots of formerly non-public reputational information.

Further, relatively small amounts of publicly disclosed reputational information might be enough to properly steer the invisible hand. For example, the first consumer review of a product in a reputation system creates a lot of value for subsequent consumers, but the 1,000th consumer review of the same product may add very little incrementally. So even if most consumer impressions remain non-public, perhaps mass-market products and vendors still have enough information produced to keep them honest. At the same time, vendors and products in the "long tail"[30] may have inadequate non-public impressions put into the public discourse, creating a valuable opportunity for comprehensive reputation systems to fix the omission. However, reputation systems will tackle these obscure marketplace options only when they can keep their costs low (given that consumer interest and traffic will, by definition, be low), and reputation system deregulation helps reduce both the costs of litigation as well as responding to takedown demands.

---

30 Chris Anderson, *The Long Tail*, WIRED, Oct. 2004, **http://www.wired.com/wired/archive/12.10/tail.html**.

## Vendor Suppression of Reputational Information

Vendors are not shy about trying to suppress unwanted consumer reviews ex post,[31] but vendors might try to suppress such reviews ex ante. For example, one café owner grew so tired of negative Yelp reviews that he put a "No Yelpers" sign in his café's windows.[32]

That sign probably had no legal effect, but Medical Justice offers an ex ante system to help doctors use preemptive contracts to suppress reviews by their patients. Medical Justice provides doctors with a form agreement that has patients waive their rights to post online reviews of the doctor.[33] Further, to bypass 47 U.S.C. § 230's protective immunity for online reputation systems that might republish such patient reviews, the Medical Justice form prospectively takes copyright ownership of any patient-authored reviews.[34] (Section 230 does not immunize against copyright infringement). This approach effectively allows doctors—or Medical Justice as their designee—to get reputation systems to remove any unwanted patient reviews simply by sending a DMCA takedown notice.[35]

Ex ante customer gag orders may be illegal. In the early 2000s, the New York Attorney General challenged software manufacturer Network Associates' end user license agreement, which said the "customer will not publish reviews of this product without prior consent from Network Associates, Inc." In response, the New York Supreme Court enjoined Network Associates from restricting user reviews in its end user license agreement.[36] Medical Justice's scheme may be equally legally problematic.

From a policy standpoint, ex ante customer gag orders pose serious threats to the invisible hand. If they work as intended, they starve reputation systems of the public information necessary to facilitate the marketplace. Therefore,

---

31 *See* Eric Goldman, *Online Word of Mouth and Its Implications for Trademark Law*, *in* TRADEMARK LAW AND THEORY: A HANDBOOK OF CONTEMPORARY RESEARCH 404 (Graeme B. Dinwoodie and Mark D. Janis eds.) (2008) (discussing lopsided databases where all negative reviews are removed, leaving only positive reviews).

32 Stefanie Olsen, *No Dogs, Yelpers Allowed*, CNET NEWS.COM, Aug. 14, 2007, **http://news.cnet.com/8301-10784_3-9759933-7.html**.

33 Lindsey Tanner, *Doctors Seek Gag Orders to Stop Patients' Online Reviews*, ASSOCIATED PRESS, Mar. 3, 2009, **http://www.usatoday.com/news/health/2009-03-05-doctor-reviews_N.htm**.

34 Michael E. Carbine, *Physicians Use Copyright Infringement Threat to Block Patient Ratings on the Web*, AIS'S HEALTH BUSINESS DAILY, Mar. 30, 2009, **http://www.aishealth.com/Bnow/hbd033009.html**.

35 17 U.S.C. § 512(c)(3).

36 People v. Network Associates, Inc., 758 N.Y.S.2d 466 (N.Y. Sup. Ct. 2003).

regulatory efforts might be required to prevent ex ante customer gag orders from wreaking havoc on marketplace mechanisms.

## Distorted Decision-Making from Reputational Information

Reputational information generally improves decision-making, but not always. Most obviously, reputational information relies on the accuracy of past information in predicting future behavior, but this predictive power is not perfect.

First, marketplace actors are constantly changing and evolving, so past behavior may not predict future performance. For example, a person with historically bad credit may obtain a well-paying job that puts him or her on good financial footing. Or, in the corporate world, a business may be sold to a new owner with different management practices. In these situations, the predictive accuracy of past information is reduced.[37]

Second, some past behavior may be so distracting that information consumers might overlook other information that has more accurate predictive power. For example, a past crime or bankruptcy can overwhelm the predictive information in an otherwise-unblemished track record of good performance.

Ultimately, a consumer of information must make smart choices about what information to consult and how much predictive weight to assign to that information. Perhaps regulation can improve the marketplace's operation by shaping the information that consumers consider. For example, if some information is so highly prejudicial that it is likely to distort consumer decision-making, the marketplace might work better if we suppress that information from the decision-maker.[38]

At the same time, taking useful information out of the marketplace could create its own adverse distortions of the invisible hand. Therefore, we should tread cautiously in suppressing certain categories of information.

---

37 *Cf.* Note, *Badwill*, 116 HARV. L. REV. 1845 (2003) (describing how companies can mask a track record of bad performance through corporate renaming).

38 *Cf.* FED. R. EVID. 403 ("Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury…"). This fear underlies a French proposal to enact a "right to forget" statute. *See* David Reid, *France Ponders Right-to-Forget Law*, BBC CLICK, Jan. 8, 2010, **http://news.bbc.co.uk/2/hi/programmes/click_online/8447742.stm**.

## Conclusion

Although "reputation" has been extensively studied in a variety of social science disciplines, there has been comparatively little attention paid to how regulation affects the flow of reputational information in our economy. Understanding these dynamics would be especially valuable in light of the proliferation of Internet-mediated reputation systems and the irresistible temptation to regulate novel and innovative reputation systems based on emotion, not necessarily sound policy considerations.

# CHAPTER 5

## WHO WILL GOVERN THE NET IN 2020?

# Imagining the Future of Global Internet Governance

## By Milton Mueller*

When discussing who (or what) will govern the Internet in 2020, people tend to want predictions. They want authoritative statements from experts. They want you to tell them what *will* happen. But an honest scholar of Internet governance would never attempt to meet that demand. The problem is not just that the future of Internet governance is uncertain, subject to the influence of many complex variables. The problem is that its future is, literally, indeterminate. While it is correct that there is an ongoing struggle over the governance of the Internet, we cannot know how it will come out.

Forget about predictions and forecasts. It's better to have a clear conception of how we *want* the Internet to be governed. This means that we need to be able to *imagine* feasible futures and to *create* strategies to realize them.

Let's step back. Why is Internet governance an interesting problem in the first place? Why does contemplating the Internet's future require imagination and creativity? Because there is a tension, even a contradiction, between the existing institutions for regulating communications and information, and the technical capabilities and processes of open internetworking. Existing institutions are organized around territorial, hierarchical nation-states; the process of internetworking, on the other hand, provides globalized and distributed interoperation amongst all the elements of an increasingly powerful and ubiquitous system of digital devices and networks.

This technical capability puts pressure on the nation-state in five distinct ways.

1. It globalizes the *scope* of communication. Its distance-insensitive cost structure and non-territorial addressing and routing architecture make borderless communication the default; any attempt to impose a jurisdictional overlay on its use requires additional (costly) interventions.
2. It facilitates a quantum jump in the *scale* of communication. It massively enlarges our capacity for message generation, duplication, and storage. As a programmable environment, it industrializes information services, information collection, and information retrieval. The sheer volume of

---

* **Milton Mueller** teaches and does research on the political economy of communication and information. His new book **NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE** (MIT Press, 2010) provides a comprehensive overview of the political and economic drivers of a new global politics.

transactions and content on the Internet often overwhelms the capacity of traditional governmental processes to respond—but that same scalability can transform governmental processes as well.

3. It *distributes control*. Combined with liberalization of the telecommunications sector, the Internet protocols have decentralized and distributed participation in and authority over networking and ensured that the decision-making units over network operations are not necessarily closely aligned with political units, as they were in the days of post, telephone and telegraph monopolies.
4. It *grows new institutions*. Decision-making authority over standards and critical Internet resources rests in the hands of a transnational network of actors that emerged organically alongside the Internet, outside of the nation-state system. These relatively young but maturing institutions, such as the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN), and Regional Internet Address Registries (RIRs) provide a new locus of authority for key decisions about standards and critical resources.
5. It *changes the polity*. By converging different media forms and facilitating fully interactive communication, the Internet dramatically alters the cost and capabilities of group action. As a result, radically new forms of collaboration, discourse, and organization are emerging. This makes it possible to mobilize new transnational policy networks and enables new forms of governance as a solution to some of the problems of Internet governance itself.

Transnational scope, boundless scale, distributed control, new institutions and radical changes in collective action capabilities—these factors are transforming national control and sovereignty over communication and information policy, setting in motion new institutional forms and new kinds of geopolitical competition. The governance of global Internetworking is thus a relatively new problem created by socio-technical change. The future of Internet governance will be driven by the clash between its raw technical potential and the desire of various incumbent interests—most notably nation-states—to assert control over that potential.

While the Internet poses novel governance problems, how we solve them cannot be predicted. It depends vitally on our ability to accurately diagnose the economic, technical and political forces at work and on our ability to imagine strategies, mechanisms and techniques that can harness those forces to do what we want to do. Thus, to repeat, it is better to invest our mental resources in conceptualizing and enacting feasible visions of how we *want* the Internet to be governed than it is to invest in making deterministic predictions.

## The Pace of Change

2020 is not very far away. Ten years is the blink of an eye when it comes to institutional development at the global level. Proof of this can be found by glancing back ten years from our current vantage point of 2010. Despite the Internet's reputation for rapid change, the basic issues and problems of Internet governance have not changed much since 2000. Yes, there has been turbulence in the market economy, with specific firms rising and falling. But the cast of institutional characters that regulate or govern Internetworking was already well in place by 2000. The organically developed Internet institutions such as the IETF, the Internet Society, and the Internet address registries[1] already existed. On the other hand, the U.S. government and its rival nation-states were entering the scene. ICANN, with its unilateral control by the U.S. government, had already emerged as the uncomfortable compromise between the a-national "Internet community" and the community of states. The seeds of the tensions among the U.S., the E.U. and the BRIC[2] nations caused by U.S. pre-eminence in that regime were already sown. There was already theoretical talk of cyberwar (though this has picked up dramatically in the last few years). There were already efforts to block and filter Internet content, though these have become increasingly refined. Peer-to-peer file sharing was already beginning to drive copyright holders mad (Napster was started in 2000). Whatever change has taken place since 2000 has been evolutionary rather than revolutionary.

## Disruption or Continuity?

It is possible to identify some aspects of the current Internet governance regime that could disrupt the existing evolutionary trajectory. I divide them into two distinct categories: the geopolitical and the techno-economic.

### Geopolitical Factors

**The Root**: One of the most important geopolitical factors is still U.S. control of the root of the name and numbering hierarchies. This control is bound up with the issue of the singularity of those roots and the universal interoperability of the Internet. Here the U.S. is pre-eminent, and along with that pre-eminence come forms of responsibility and danger. A policy misstep or mistake can disrupt the *status quo*. Will the U.S. finally fully privatize ICANN, or will it "internationalize" it? Will the Internet Assigned Numbers Authority (IANA) contract[3] be competitively bid, or routinely reassigned to ICANN, keeping it

---

1 Users are assigned IP addresses by Internet service providers (ISPs), who usually obtain larger blocks of IP addresses from a Regional Internet Registry (RIR).

2 Brazil, Russia, India, and China

3 The IANA contract is a contract between the U.S. Commerce Department that authorizes ICANN to perform what is commonly referred to as the IANA function, a bundle of technical operations that includes the registration and allocation of IP addresses,

subordinate to the United States government? The governance issues related to the root and control/coordination hierarchies have intensified as the technical community (usually funded by U.S. government contracts) has moved to "secure" the Internet by making access to and use of critical identifier resources reliant upon cryptographic key hierarchies. The harder the U.S. government tries to rigidify its existing forms of institutional control over Internet resources, the more likely it becomes that the Internet will fragment.

**Cyber-Warfare**: Military conflict is always a potent source of institutional disruption. Geopolitically, the U.S. is pursuing a dangerously contradictory agenda. On the one hand it insists on retaining pre-eminent control of Internet standards, protocols and virtual resources and maximizing the dependence of the rest of the world on them. On the other hand it wants to treat cyberspace as a "national asset" and develop an overwhelming cyber-warfare and cyber-weapons capability based on those very same standards, protocols and resources. But insofar as cyberspace is militarized, its status as a globalized platform for information and communication among the business and civil society is undermined. Contradictions abound here, and as they play out, the chances of a structural change increase.

**Free Trade in Information Services**: The U.S. approach to Internet freedom is driven as much by economics as by ideology and ethics. Due to its liberal policies, the U.S. leads the world in the supply of Internet-based information services. Of course the rest of the world will gradually catch up, but the natural state of Internet-based information services is to be transnational, accessible anywhere in the world, and so suppliers who would challenge the Googles and Facebooks must be transnational as well. The contradiction between the open Internet and various forms of trade protectionism in the content industries—including the cultural protectionism that is often disguised as support for "diversity"—could be a key driver of Internet governance. Advocates of civil liberties and communication rights need to forge common ground with advocates of free trade and market liberalism for anything important to happen here.

## Techno-Economic Factors

**Unlicensed Wireless Broadband**: A great deal of the consolidation of control over the Internet is contingent upon the access bottleneck. The fewer market players in the Internet service provider space, the easier it becomes for states and state-favored monopolies to blunt and channel the potential of information and communication technology. Thus, new access technologies like unlicensed wireless broadband become critical factors shaping the future. If they can take

---

management of the Internet root server system, and maintenance of the authoritative root zone file for the domain name system.

root and disrupt current market structures around the supply of Internet access, the arrangements for governance and control will need to be reconsidered. With greater choice of access arrangements, the less feasible it becomes for governments to impose onerous regulatory arrangement upon consumers through intermediaries.

**DPI and Net Neutrality**: A key characteristic of the Internet so far has been the "end-to-end" principle, which put the processing intelligence for applications and services at the end points and made the network a relatively simple packet-forwarding system. Deep packet inspection (DPI) is a new technological capability that could lead to a wholesale departure from that principle. Developed in response to legitimate concerns about efficient bandwidth management and the detection and interception of malware, it increases the awareness and control of the network intermediary over the traffic coursing through its system. This is a fateful shift of control. Needless to say, there are demands to extend its capabilities to less technical forms of intervention, such as censorship, copyright protection or national security-oriented surveillance of communications. At the same time, concerns about privacy, network neutrality, and competition policy have put legal and regulatory checks upon the usage of DPI. This is an arena that goes to the heart of Internet governance in the future.

## Two Visions

Two visions of possible futures should help to illustrate how these themes *might* play out, but more importantly, how I think they *ought* and ought *not* play out.

### The Dark Vision

Picture a world in a long-term global recession, one that lasts the better part of the decade we are discussing. There is growing conservatism—by which I mean increasingly nationalist and ethnocentric attitudes, a growing impatience with, and rejection of, the rigors of market liberalism, and a greater willingness to trade freedom and innovation for security and stability. In such a scenario of recession-driven reaction, trade barriers rise. Hostility to immigration and "offshoring" grows. Internet-based communications become increasingly confined to national spaces. There is blocking and filtering of content at the national level; the full linkage of online identity to national identity; the licensing of content, application and service providers at the national level; the subordination of information flows to the surveillance needs of national governments. Infrastructure providers stop expanding and rely on national broadband subsidy plans. As this happens, the major U.S. Internet/media corporations succeed in minimizing competition and maximize rent-seeking in an increasingly mature, stable market. With the number of players winnowed down, these corporations will make disastrous concessions to governments seeking to extend their authority over cyberspace in areas such as online identity

and identification, online surveillance, security practices, protectionist standards and content regulation. Some variant of a Google-Verizon merger spawns the AT&T of the 21st century, a dominant private sector entity with its own commercial interests, but one whose markets and fortunes follow the flag of U.S. policy worldwide. Reacting to its quasi-sponsorship by the State Department, other countries erect barriers. In this context, with national security and a cyber- version of the military-industrial complex becoming the main driver of international policy, the U.S. government eventually participates in the strangling of its own progeny.

As the U.S. develops an overwhelming cyber-warfare and cyber-weapons capability, the rest of the world revolts. The U.S. provokes a cyber-cold war, or perhaps even a short "hot war" with Russia and China, and uses it to rationalize and extend many of the controls. The European Commission—but not European civil society—will side with the U.S., effectively paralyzing and subordinating Europe's ability to contribute anything constructive, much less innovative, to the Internet governance debates. The Internet world fragments on linguistic grounds, with the English-speaking or English-dominant world drifting away from the Chinese, Korean, Russian and Japanese societies.

## The Bright Vision

It's easy enough to describe that scenario because it seems to be the road we are already on. It is much harder to imagine a better future, one that is both feasible and consistent with the interests and capabilities of current actors. But let's give it a try. In another work, I've tried to describe the basic nature of what I call a *denationalized liberalism* as the guide to the future of Internet governance.[4]

At its core, a denationalized liberalism favors a universal right to receive and impart information regardless of frontiers, and sees freedom to communicate and exchange information as fundamental, primary elements of human choice and political and social activity. Political institutions should seek to build upon, not undermine or reverse, the limitless possibilities for forming new social aggregations around digital communications. In line with its commitment to freedom, this ideology holds a presumption in favor of networked, associative relations over hierarchical relations as a mode of transnational governance. Governance should emerge primarily as a byproduct of many unilateral and bilateral decisions by its members to exchange or negotiate with other members (or to refuse to do so). This networked liberalism thus moves decisively away from the dangerous, conflict-prone tendency to build political institutions around linguistic, religious, and ethnic communities. Instead of rigid, bounded communities that conceal domination with the pretense of homogeneity and a

---

4 MILTON MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE (MIT Press: 2010).

"collective will," this liberalism offers governance of communication and information through more flexible and shifting social aggregations.

Although committed to globalism in the communicative sector, networked liberalism recognizes that, for the time being, people are deeply situated within national laws and institutions regarding such basic matters as contracts, property, crime, education, and welfare. It is characterized not by absolute hostility to national and subnational governments as such, but rather by an attempt to *contain* them to those domains of law and policy suited to localized or territorialized authority. It seeks to detach the transnational operations of Internet infrastructure and the governance of services and content from those limited jurisdictions as much as possible, and to prevent states from ensnaring global communications in interstate rivalries and politico-military games. This requires a complete detachment of Internet governance institutions from nation-state institutions, and the creation of new, direct accountability relationships for Internet institutions.

Such an ideology needs to answer tough questions about when hierarchical exercises of power are justified and through which instruments they are exercised. A realistic denationalized liberalism recognizes that emergent forms of control will arise from globally networked communities. It recognizes that authoritative interventions will be needed to secure basic rights against coercive attacks, and that network externalities or bottlenecks over essential facilities may create a concentrated power with coercive effect. It should also recognize the exceptional cases where the governance of shared resources requires binding collective action. Insofar as collective governance is necessary and unavoidable, a denationalized liberalism strives to make Internet users and suppliers an autonomous, global polity, with what might be called *neodemocratic* rights to representation and participation in these new global governance institutions. The concept of democracy is qualified by the realization that the specific form of democratic governance associated with the territorial nation-state cannot and should not be directly translated into the global level. However, it *does* maintain the basic objectives of traditional democracy: to give all individuals the same formal rights and representational status within the institutions that govern them so that they can preserve and protect their rights as individuals. Such a liberalism is not interested, however, in using global governance institutions to redistribute wealth. That would require an overarching hierarchical power that would be almost impossible to control democratically; its mere existence would trigger organized political competition for its levers, which would, in the current historical context, devolve into competition among preexisting political and ethnic collectivities—the very opposite of networked liberalism.

In short, we need to find ways to translate classical liberal rights and freedoms into a governance framework suitable for the global Internet. There can be no

cyber-liberty without a political movement to define, defend, and institutionalize individual rights and freedoms on a transnational scale.

# Democracy in Cyberspace: Self-Governing Netizens & a New, Global Form of Civic Virtue, Online

By David R. Johnson*

The Internet can be viewed as a set of wires, wireless "pipes" and servers, a set of protocols, or as a vast array of content and applications to which these lower layers of the stack provide access. None of those tangible and intangible things can be "governed." They may or may not be owned or manipulated. But it is the actions of the people involved in creating and using the Internet that are the proper subject of a question regarding "governance." Viewed with respect to the social and legal relationships among the people who are creating and using it, and who would be "governed," the Internet is a complex system—so making accurate predictions about its future state is impossible.

But it is possible to answer the question: "Who *could* and who *should* govern the Internet in 2020?" My answer is, in a word: netizens—the global polity of those who collaborate online, seek to use the new affordances of the Internet to improve the world, and care about protecting an Internet architecture that facilitates new forms of civic virtue.

## The Internet Governance Debate

The debate about "Internet Governance" has continued for more than fifteen years and settled into an unsatisfying rut. The established trope is that early visionaries (*e.g.*, John Perry Barlow[1]) claimed that cyberspace was a new realm of freedom, poised to escape from regulation by local governments. Then, later "realists" (*e.g.*, Jack Goldsmith and Tim Wu[2]) discovered that sovereign governments indeed had ways to regulate online speech and even use the Internet for surveillance and tyranny. Early idealists envisioned the Internet Corporation for Assigned Names and Numbers (charged with setting policy for

---

* David Johnson joined New York Law School's faculty in spring 2004 as a visiting professor of law. He is a faculty member of the Institute for Information Law and Policy.

1 *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), **https://projects.eff.org/~barlow/Declaration-Final.html** [hereinafter *A Declaration of the Independence of Cyberspace*]; John Perry Barlow, *Declaring Independence*, 4.06 *WIRED* 121-22 (June 1996), *available at* **http://www.wired.com/wired/archive/4.06/independence.html**.

2 *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006) [hereinafter WHO CONTROLS THE INTERNET?].

the domain name system and allocating blocks of IP numbers)[3] as a new democratic global institution constrained by consensus reached in a global community. Later, we observe an expensive bureaucracy imposing complex regulations—as one wag has put it: "recapitulating the FCC and doing it badly."[4] Internet Governance as an empowering and liberating democratic ideal is a total failure—or so it would seem.

This debate has missed a fundamental point by asking the wrong question. The key question is not "Who will govern the Internet?" Instead, it is "Will the global Internet affect the way in which we (the global polity) govern ourselves?" One way or another, we act through governments, NGOs, private corporations and many other types of groups to collectively set the rules by which we live our lives. We all strive for a world in which our own choices determine how we are governed. So the more salient way to put the real question at issue is: "Can the Internet make society more democratic?"

## The Vision of the Internet's Founders

The founders of the Internet (technologists, advocates, policy makers, and visionaries) saw its democratic potential. They were not (mostly) seeking to create a "lawless frontier." They were instead seizing a moment of flexibility during which new modes of association for community improvement might flourish. They opposed rigid regulation and unaccountable power, of course. But they also favored collaborative decision-making to establish rules, group effort to write empowering and constraining code, and respectful deliberation to forge new norms. They favored civility and civic virtue (good netizenship) as much as individual liberty.

We're not just talking about the founding technologists. Many individuals, nonprofit organizations and companies came together, in the late 1980s and throughout the 1990s, to create a technology and policy framework to enable a democratic Internet: open access, limitations on intermediaries' powers and liabilities, privacy protections for communications, limitations on centralized levers of power (like the control over the domain name system) and, at least in the United States, establishment of strong First Amendment rights (in contrast to regulation of the Internet as a form of mass media). To a considerable

---

[3] ICANN is generally accepted as the authority for decisions about what top level domains will be placed in the "root zone file." By establishing contractual conditions in connection with such additions, it can establish rules that flow down onto registries, registrars and registrants. For example, this capability has been used to require registrants in generic Top Level Domains to submit to a "Uniform Dispute Resolution Policy" that decides and takes action on disputes about "cybersquatting."

[4] Harold Feld, quoted in Jonathan Weinberg, *ICANN, "Internet Stability," and New Top Level Domains* 1 n. 1, **http://faculty.law.wayne.edu/Weinberg/icannetc.pdf**.

degree, from that perspective, the Internet's founders have, up to this point, succeeded.

I want to re-emphasize that, while the Internet relies on wires and protocols, it most fundamentally consists of connections among people. Local governments may control who has the right to provide access. Standard setting bodies may have some say in what protocols become widely adopted. Law plays a role—and the law of local governments does constrain the actions of people over whom they can assert jurisdiction. But the "governance" of the Internet is fundamentally a question about how we all constrain the manner in which we do whatever it is we do in groups online, including establishing new structures of society, new forms of social organization, and new roles and rules that incentivize our efforts and focus our minds. No government could even hope to make the rule set for a global web of relationships involving billions of people interacting in complex and ever evolving ways. The governance of the social layer of the Internet will be, perforce, decentralized.

## The Democratic Nature of the Internet

Thus, contrary to Larry Lessig's suggestion in *Code*,[5] I submit that the Internet of today has a nature: It is inherently democratic. Not inevitably so, in the sense that any global communications network would necessarily be democratic. And not necessarily so in the future. But historically so and by design—in the sense that *this* Internet, the one we have and the one that scaled globally in no time, was successful precisely because it was open, decentralized, tolerant of innovation and disagreement, voluntary, and empowering of anyone who cared to use it to join with others to improve the world. Every time we address an email, or establish a blog, or "agree" to some "terms of service," we are creating the rules for our online society.

From Wikipedia to PatientsLikeMe,[6] we are continuously learning how to use the Internet to come together to share knowledge, improve education, solve health care problems, and provide charitable assistance to those in need around the world. We use the Internet to participate in local politics and explore new ways to make global society energy efficient. In these and countless other ways, the Internet is an engine of democratic civic virtue.

---

5 *See* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (Basic Books 2006).

6 For example, PatientsLikeMe allows users to create profiles and then share, interact, and learn from the experience of other users on health and wellness issues.

## Self-Governance Online

As noted, and sometimes in defiance of repressive regulations, we choose many of the rules under which these collaborations occur simply by logging in to one website or platform rather than another. We can rise up together in protest when a site like Facebook changes its "terms of service" and "privacy policy" in ways we don't like. And we increasingly accept obligations to spend our attention and effort in support of groups we find online with whom we share a persistent purpose or goal.

Even an email listserv involves social duties (not always honored, of course) to fellow participants. Open source efforts have evolved complex, hierarchical, yet open and democratic (or meritocratic) self-governance structures. We are beginning to understand that, at least for those things that can happen online, the choices we make about which groups to join have as much impact on setting the terms of our relationships with others than any governmental laws or regulations.

Goldsmith and Wu and other "anti-exceptionalists" have cited the Yahoo! France case, Australia's imposition of its libel laws on a New Jersey-based publisher, and Italy's conviction of Google executives for the proposition that the Net cannot escape from the "real world" governance of sovereign states.[7] Their examples, rather than making a case for a bordered Internet, in fact prove the opposite: A world in which every local sovereign seeks to control the activities of netizens beyond its borders violates the true meaning of self-governance and democratic sovereignty.

## Attention Governance & Global Civic Virtue

Even though governments still have the guns and have not yet uniformly agreed to defer to self-governing online groups, "We the Netizens" are still mostly in control of what happens online. The everyday actions of millions of bloggers and tweeters (and re-tweeters) and senders of emails and instant messages draw the attention of the entire world to new and interesting (though not always important) developments every day. The distributed collaboration arising from ratings, rankings and reviews disclose and shame, or shine a flattering light on, every action of every author, seller, politician, organization and anyone else who wields any form of power. We are learning to use the Internet to engage in a decentralized form of democracy that might be called "attention governance."

Democracy is about decentralization and equalization of power—particularly the power to influence the rules under which we live our lives together. This

---

7 WHO CONTROLS THE INTERNET?, *supra* note 2.

requires the absence of centralized, unaccountable power—tyranny—whether exercised by government or corporations. It also requires that individuals participate in collective action and adopt a frame of mind that asks how to improve society rather than only how best to achieve their own private goals.

That frame of mind is called "civic virtue." It creates a feedback loop—showing us all ourselves in a mirror, thereby enhancing our ethical standards for both individual actions and the actions we take together in organizations and groups (including via the global corporations in which we invest, serve as employees or participate as customers). Perhaps the single most powerful contribution to the sovereignty of the people made by the Internet is its ability to direct our collective attention. At one time, mass media held that power. Now we all do, in potentially equal measure. While online anonymity may (sometimes unfortunately) give us the power to act without disclosing our identity, the Internet simultaneously makes it virtually impossible for groups of people to act together without being confronted with the consequences of their actions and the views of others regarding the moral and social value (or lack thereof) of those consequences.

Democracy is not just about how we organize political campaigns or governmental institutions. It is about how we self-organize all aspects of society—and what we can do in collaboration with others to improve the world. It is not just about freedom from arbitrary control by government (or corporate tyrants)—it is, rather, about the myriad ways in which we come together to construct society. The Internet has had a profound impact on political campaigns by making it much easier for individuals to contribute small amounts and get involved in local activities. And netizens could and should use their newfound collective voice to instruct their local governments to protect the Internet and its new freedoms, rather than using it to restrict our freedom. But the Internet has done even more to decentralize decision-making—about how we spend our attention and effort and how we organize our collaborative efforts. Today, anyone can form a purposeful group online on Facebook, Yahoo! Groups, Google Groups, Twitter, etc. and attract adherents to a cause or even start a new organization. When we can more easily act together, we become more powerful and more free—we enjoy what Tocqueville would have called "a new equality of condition."[8]

The interesting thing about attention is that, as long as you are awake, you have to spend it! It is a non-renewable resource. You can fritter it away on the entertainments of television or tweeting. You can give it away to an employer whose goals and ethics don't match your own. Or, after the basic necessities of life have been arranged for, you can apply a higher standard. Through the

---

8 ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA (1835).

Internet, you can join with others in groups that try to make the world a better place, and talk together about what that means.[9]

## Good Netizenship

Governing the Internet well fundamentally entails governing ourselves—making sure that more of our time, attention and effort is spent in roles that are defined in relation to social organizations and purposive groups that make society more productive, congruent, ethical, and, yes, interesting, complex and empowering for everyone. It involves defending the new civic religion of the Internet, including preservation of individual choice and deference to the self-governance of online groups. It is no light duty to be a good netizen.

Goldsmith and Wu have shown that open communications via the Internet can indeed be shut down by governments.[10] But they don't say anything about how to preserve and enhance democracy in the context of a global Internet. They postulate the extension of local and state power onto people who have no opportunity to participate in making these policies. But they fail to take account of the possibility that once We the Netizens understand the threat, we could refuse to allow that to happen.

How could we netizens prevent the tyranny of local governments or of corporate intermediaries with a new kind of power generated by network effects? It may be a struggle at times. But we use our minds online—we direct our attention and support to groups we value. It takes a very seriously repressive governmental regime to regulate minds rather than behavior. And not even governments, much less corporations, can stand forever in opposition to what large segments of the people they regulate *think*—especially when they are thinking, and talking, together. As Victor Hugo famously remarked, "One resists the invasion of armies; one simply cannot resist the invasion of ideas."[11]

Even those who purport to want to preserve civil civic dialogue and self-governance by the people sometimes suggest that the Internet has broken our existing (U.S.) democratic institutions—polarizing political factions, eliminating the possibility of political compromise, fostering hate speech and inciting the

---

9 As Tocqueville observed about America in the 1830s: "*In their political associations the Americans, of all conditions, minds, and ages, daily acquire a general taste for association and grow accustomed to the use of it.* There they meet together in large numbers, they converse, they listen to one another, and they are mutually stimulated to all sorts of undertakings. They afterwards *transfer to civil life the notions they have thus acquired and make them subservient to a thousand purposes*. Thus *it is by the enjoyment of a dangerous freedom that the Americans learn the art of rendering the dangers of freedom less formidable*." *Id.* (emphasis added).

10 WHO CONTROLS THE INTERNET?, *supra* note 2.

11 VICTOR HUGO, THE HISTORY OF A CRIME (1877).

mob.[12] Even those who favor civic virtue suggest that the Internet has led to a retreat into individualism, mindless narcissism, pornography, intellectual distraction and worse.[13]

The democratic potential of the Internet is under threat—as democracy always is. Some local sovereigns attempt to limit its freedoms. People lacking the requisite civic virtue may lapse into self-indulgent individualism. We might all decide to live under the benevolent dictatorship of search engines and online app stores that make our lives a little more convenient and secure. We might all decide it is too much trouble to help our fellow netizens in foreign countries who are fighting repressive local governments. Large corporations with monopolies born of network effects might gain enough power to become a new aristocracy, purporting to benefit the people, but ruling as they please and giving priority to profit. Bad actors might turn this new communications medium into a social nightmare. So any theory of the democratic potential (and actual achievement) of the Internet must include a view regarding how we can all use the Internet itself to preserve and enhance gains achieved up till now in popular sovereignty and civic collaboration.

## The Trajectory of Freedom

I have such a theory—one derived from reflecting on Tocqueville's views regarding the new democracy that he discovered in the America of 1830: *The Internet establishes a new equality of condition and enables us to exercise liberty to form associations to pursue new civic, social, and cultural goals.* Such a world can produce wonders simply because we become more powerful when we act together in groups. Moreover, to paraphrase Oliver Wendell Holmes, "Man's mind, once stretched to a new democratic practice, never regains its original dimensions."[14] The theory, then, is that having discovered and exercised new ways to improve the world, whatever they mean by "improve," netizens will collaborate in myriad ways to protect their newfound powers.

The actual state of society may, of course, periodically regress. Some groups will adopt definitions of "improvement" that are so intrusive upon and unacceptable to other groups that governmental and corporate powers will be rightly invited in to constrain such non-congruent actions. (For example, almost everyone agrees that the Internet should not provide a safe haven for child

---

12 *See, e.g.*, CASS SUNSTEIN, REPUBLIC.COM 2.0 (2007).

13 *See, e.g.*, NICHOLAS CARR, THE SHALLOWS: WHAT THE INTERNET IS DOING TO OUR BRAINS (2010).

14 The original quotation is as follows: "Man's mind, once stretched by a new idea, never regains its original dimensions." Oliver Wendell Holmes, *quoted in* H. JACKSON BROWN, JR., A FATHER'S BOOK OF WISDOM (1989).

pornography or terrorism and governmental powers will need to be used to address these problems.)

But the trajectory of freedom and even civic virtue has been, in broad terms, over time, constantly upward—because everyone who gets a chance to experience an increased level of democratic self-government—a new "equality of condition"—a new kind of power that comes from the ability to direct and control one's own attention and combine one's efforts with those of others—comes to share a desire to have a voice in shaping the world for the better (even when we don't all agree on what "better" means). And everyone has now tasted an empowering opportunity to join with others, online, to do so.

Acting together, the founding netizens created a global network, and thus, inevitably, a global economy, society and politics. The visionary founders of the Internet did not seek to liberate selfish individualism, frontier justice based on force, or mere wilderness escape. They were civically virtuous themselves and foresaw the creation of great schools and libraries, social services, cultural venues, and everything else a prosperous and democratic global township might want, online.[15] Perhaps they were naïve, a bit too optimistic that everyone else shared their civility. Perhaps they assumed that most online groups would make rules and take actions designed to benefit those who were affected by those rules and actions. Confronted with criminals or tyrants, these Internet optimists would be (and are) as quick as anyone to call for a "rule of law." But they can now envision a "law" consisting in part of globally applicable rule sets and globally accessible self-governing organizations that exist only because netizens have devoted their time, attention and effort to support or shun new online institutions.

Copyright law won't disappear, but we now also have Creative Commons. Laws against spam will survive, but we also have software filters. Local content regulation will persist, but we now have proxy servers. Banks will be regulated, but online currencies can also flourish. Governments will still regulate and tax the shipment of physical goods, but most long ago gave up trying to establish custom houses at their virtual border. Every netizen is still a citizen, subject to local regulation. But, increasingly, we can travel online to virtual places that have rules no local legislature would adopt. Land use in Second Life will not become a subject of any real world government's zoning laws. Topic moderation in an online discussion group is not likely to become a matter of local regulation.

---

15 *See, e.g.*, HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER (1993); FRED TURNER, FROM COUNTER CULTURE TO CYBERCULTURE: STEWARD BRAND, THE WHOLE EARTH NETWORK, AND THE RISE OF DIGITAL UTOPIANISM (2006); KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996).

Online schools will establish their own rules for participation in the classes they offer.

Where we congregate online, most of the relevant rules will originate with our shared support of the manner in which the proprietor (the owner of the server, the writer of constraining code, a moderator) "governs" that online space. Governments will, in general, defer to online spaces that are mostly minding their own business, rather than inflicting harms on outsiders. They have enough to do in securing our physical safety. So congruent rule sets voluntarily "adopted" by willing "users" will become most of the applicable "law" of online life. That new law will be fundamentally democratic in character, not because we elected representatives to a global legislature, but because we all have new powers to decide where to go online and to persuade others to join us.

Because global scale and interconnection make it easier to find each other, valuable online groups can exist even if there are very few who share the group's goals and interests. By the same token, online sites that no one visits lose social salience. An online source of destructive code or spam may still intrude upon our finite attention, but almost everyone agrees that we can and should get better at constraining the actions of those who use the Internet to inflict that kind of harm on others. ISPs provide centralized filters but these depend in part on user actions to flag spam and malicious code. This same dependence on our collective attention happens to apply to governments and corporations, the very real "legal fictions" that we call into existence by means of a shared act of imagination. They thrive only insofar as we allocate our own time, effort and attention to facilitate their purposes. If we refuse to play along, governments and corporations are doomed to lose (legitimate) power and cannot ultimately impose their will on an unwilling global polity.

In short, there was never any possibility, or dream, that global online society would be a society without some amount of order. Even the most idealistic Internet Exceptionalists, like John Perry Barlow, never denied that there might be problems in Cyberspace that needed to be solved, only that "We in Cyberspace" would solve them by "forming our own Social Contract."[16] The questions have always been: How much order? Where would it come from? And, if it came from the online community, how closely would its mechanisms approximate the democratic ideal of giving everyone at least a potentially equal say in what particular kind of order (rules, norms, incentives, roles) were to be established? Who gets to tell who else what they can and cannot do? Will the Internet preserve, or even enhance, the sovereignty of the people? Those were the key questions from the Internet's very beginning.

---

16 See *A Declaration of the Independence of Cyberspace*, *supra* note 1.

Wu, Goldsmith and others triumphantly declare the death of Internet Exceptionalism based on the reality that governments seek to regulate the Internet—and succeed in doing so to a much greater extent than some Internet Exceptionalists might have imagined possible. But this does not mean the Internet does not present profoundly new opportunities for self-government—a new potential form of democracy. It is up to us to seize that opportunity. If we do so, the Internet will have proved itself as exceptional as its founders hoped.

## Cosmopolitan Pluralism

Because people have many different values (ideas about the social good), the global online society will need to be pluralistic, cosmopolitan, and tolerant of diverse coexisting groups. As the Internet's founding netizens urged, online society could and should be based on the moral norm that all groups should be "conservative in what they send, liberal in what they accept."[17] Above all, they imagined (correctly, in my view) that such a global online society would become ever more complex—providing increasingly diverse roles for people to play while, simultaneously, preserving connections (causal and communicative) among all its parts and the whole—thereby creating vast new wealth (of all types) for all to share. All wealth ultimately comes from trade. And trade requires two people who value whatever they have to exchange differently—so that the bargain makes them both better off.[18] We *need* our differences. Democratic Internet governance can preserve them, by allowing us to tolerate diverse groups, rather than seeking to impose a single rule set on everyone.

If you think democracy is about voting, then the apogee of democratization is when everyone has an equal vote. That just doesn't scale globally. We will "vote" online with our clicks, not with ballots. If you think democracy is about deliberation and discussion, then the ideal would seem to be a continuous global town meeting, with everyone getting an equal turn at the microphone. *Please, spare us!*

If, however, you think that democracy is about equalization of (potential) power to have an influence on how society is structured, on how we will improve the world, then you have to ask: What is it that we all have in equal measure, the deployment of which *can* shape our world and its rules. The answer is attention and effort. That is why attention governance is inherently democratic. That is

---

17 The Internet Society, RFC 4677, *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force* 6 (Sept. 2006) (quoting Jon Postel), *available at* **http://tools.ietf.org/pdf/rfc4677.pdf**.

18 *See generally*, ERIC D. BEINHOCKER, THE ORIGIN OF WEALTH: EVOLUTION, COMPLEXITY, AND THE RADICAL REMAKING OF ECONOMICS (2006); DAVID WARSH, KNOWLEDGE AND THE WEALTH OF NATIONS: A STORY OF ECONOMIC DISCOVERY (2006).

how the Internet can make self-governance real in the context of a new global society of netizens.

Every social organization with power (including governments and corporations) depends critically on a collective act of imagination. We create our social institutions by going along together with the idea that they exist, adopting roles that constrain our time and attention in the service of their goals and investing our attention and effort in ways that further empower them. The Internet is, centrally, a way for us to deploy our attention and effort together, in a context in which we can see the resulting effects and correct or constrain social organizations that don't share our values. It makes us all citizens (and, indeed, global netizens) in a new way. It increases our power and, by doing so, our responsibilities.

## A New Sovereignty of the People

Internet governance will not be about voting, or complex governmental regulations, or even treaties among states. It will be more mundane, more pervasive, and more profoundly important than that. As long as some states create havens for freedom (whether the First Amendment and Section 230 of the Communications Decency Act[19] in the United States or the Icelandic protection of WikiLeaks[20]), netizens will find ways to exercise those freedoms. Insofar as some states create havens for wrongdoers (think Nigerian phishers, Russian botnets), governments, corporations and individuals will all respond, in their own ways, to avoid or suppress such evils. It would be folly to suggest that no organizations (and, therefore, people in organizational roles) will be more powerful than others, or that no one will use power for evil so widely condemned that it cannot and should not be "tolerated." But no collective action can persist online over the long term if it is not "tolerated" by those who decide where to direct their attention, what products to buy, what Terms of Service to accept, what jobs to take, what companies to invest in, and what local politicians to send packing.

America was founded on the idea of sovereignty of the people. The global Internet gives the people more tools to exercise that sovereignty and greater visibility on when and how and where to do so. Good netizenship isn't effortless. Civic virtue requires, well, virtue. It is about responsibilities, not rights. Whether the Internet will realize its democratic potential will ultimately depend, of course, on the character of the people—the new global polity.

---

19 47 U.S.C. § 230 (providing liability immunity for providers and users of an "interactive computer service" who publish third party information).

20 *See* Robert Mackey, *Victory for WikiLeaks in Iceland's Parliament*, *The Lede Blog*, N.Y. TIMES, June 17, 2010, *available at* **http://thelede.blogs.nytimes.com/2010/06/17/victory-for-wikileaks-in-icelands-parliament/**.

I'm optimistic about the prospects for enhanced self-governance by a global polity, for one simple reason: Most of us, whatever our nationality, *want* to be empowered. To communicate. To associate to make the world better for ourselves, our children and everyone else. We've had a taste of the new democracy of the Internet. We'll never willingly, or for long, go back. We certainly *shouldn't* turn away from this new opportunity, the Internet founders' shared dream of a more empowering, democratic, global society. If we remember the democratic visions of the founders, and commit to continue to act as good netizens, then we could and should *all* "govern the Internet," together, in 2020—and beyond.

# Who's Who in Internet Politics: A Taxonomy of Information Technology Policy & Politics

By Robert D. Atkinson*

Where's the Internet in the United States going to be in a decade? Given the important role of public policy in shaping a host of Internet issues, one way to answer this question is to understand the political constellation that now shapes U.S. and—to some extent—international Internet policy.

Debates have erupted over myriad information technology (IT) issues such as copyright protection, privacy, open source software procurement, cybersecurity, Internet taxation, media ownership, Internet governance, electronic voting, broadband deployment and adoption, anti-trust, spectrum reform, net neutrality, Internet censorship, and equality of access. These issues raise familiar legal and political questions in some unfamiliar contexts, and have given rise to a lively, increasingly shrill, and important digital politics. Today, interest groups of all kinds, including a host of single-issue advocacy organizations, routinely weigh in on a range of Internet and digital economy issues. Vexing policy conundrums arise constantly, with each new business model and Internet innovation creating a new wrinkle in the fabric of the debate.

How we resolve these issues will have important implications for what the Internet of 2020 looks like. The debate over IT policy issues does not take place in a vacuum or only in the corridors of Congress. From think tanks to trade associations to single-issue advocacy groups, a proliferation of organizations fights to shape digital policy debates. This essay is a field guide to help the reader understand the politics of IT.[1] It describes the major groups of players in the IT policy debate and discusses how they differ along two key

---

* Robert D. Atkinson is the founder and president of the **Information Technology and Innovation Foundation**, a Washington, DC-based technology policy think tank. He is also author of the State New Economy Index series and the book, THE PAST AND FUTURE OF AMERICA'S ECONOMY: LONG WAVES OF INNOVATION THAT POWER CYCLES OF GROWTH (Edward Elgar, 2005).

1 For other useful attempts at creating Internet policy typologies, *see* Adam Thierer & Berin Szoka, *Cyber-Libertarianism: The Case for Real Internet Freedom*, THE TECHNOLOGY LIBERATION FRONT, Aug. 12, 2009, **http://techliberation.com/2009/08/12/cyber-libertarianism-the-case-for-real-internet-freedom/**; and Adam Thierer, *Are You an Internet Optimist or Pessimist? The Great Debate over Technology's Impact on Society*, THE TECHNOLOGY LIBERATION FRONT, Jan. 31, 2010, **http://techliberation.com/2010/01/31/are-you-an-internet-optimist-or-pessimist-the-great-debate-over-technology%E2%80%99s-impact-on-society**.

dimensions shaping policy: individual empowerment vs. societal benefit; and laissez-faire vs. government regulation. It then uses four timely and important policy cases (privacy, taxation, copyright protection, and net neutrality) to illuminate how these politics play out today in the United States. While primarily focused on American digital politics, this framework is not entirely unique to the United States.

## The Major Players

The primary players in the IT policy debate fall into eight basic groups:

1. **Internet Exceptionalists**: These "Netizens" believe that they launched the Internet revolution. Typified by groups such as the Free Software Foundation and the Electronic Frontier Foundation, and dedicated readers of Wired magazine, they believe "information wants to be free"[2] and that all software should be open-source. They think technology itself can solve many problems that it might create (if users are only smart enough to program software to protect themselves), and that cyberspace should be governed by the informally enforced social mores (*i.e.*, "netiquette") that evolved among early users. Like John Perry Barlow in his 1996 **Declaration of Independence of Cyberspace**,[3] they deplore both government involvement in the Internet and its widespread commercialization. In their view, anyone who suggests that society, through its legitimately elected government leaders, might have a role to play in shaping the Internet, including defending copyright, "just doesn't get it." Internet exceptionalists believe the Internet should be governed by its users. Afraid your privacy is being violated? Technologically-empowered users are the best solution, as they set their Web browser to reject cookies, use anonymizer tools and encrypt their web traffic. Worried about the recording industry losing money from Internet piracy? Encourage artists to find a new business model, like selling T-shirts and putting on more concerts. Worried over lackluster IT industry competitiveness in the U.S.? Don't make waves, Government intervention generally makes things worse. After all, Silicon Valley didn't need Washington to get where it is.

2. **Social Engineers**: These liberals believe the Internet is empowering but they worry that its growth is having unintended and sometimes dire consequences for society—whether they invoke the so-called "Digital Divide " (between the "wired" and the "unwired") the purported loss of privacy, net neutrality, or concern that corporations are controlling the use

---

2 Stewart Brand, speaking at the first Hacker's Conference, 1984. Roger Clarke, *Information Wants to be Free*, **http://www.rogerclarke.com/II/IWtbF.html**.

3 John Perry Barlow, A Declaration of the Independence of Cyberspace, Feb. 8, 1996, **https://projects.eff.org/~barlow/Declaration-Final.html**.

of digital content. They mistrust both government and corporations, the latter especially—particularly large telecommunications companies and Internet companies making money from the use of consumer data (to, ironically, provide free content and services). A large array of groups and individuals carry this mantle, including the Benton Foundation, Center for Democracy and Technology (on some issues), Center for Digital Democracy, Civil Rights Forum on Communication Policy, Consumer Project on Technology, Electronic Privacy Information Center, Free Press, Media Access Project, and Public Knowledge, and scholars such as Columbia's Tim Wu and most of those hanging their hats at Harvard's Berkman Center (among them, Larry Lessig and Yochai Benkler). Social engineers tend to believe the Internet should serve mainly as an educational and communications tool. They fear that its empowering capabilities will be taken away by powerful multinational corporations and statist governments that will reshape it to serve their own narrow purposes (either to steal our privacy, limit our freedom on the Internet, spy on us, or all three). As such, they minimize the role of IT as an economic engine, and focus more on the impact of IT on social issues, such as privacy, community, access to information and content, and civil liberties.

3. **Free Marketers**: This group views the digital revolution as the great third wave of economic innovation in human history (after the agricultural and industrial revolutions). IT reduces transaction costs and facilitates the application of markets to many more areas of human activity. Free marketers envision a dramatically reduced role for government as the Internet empowers people, liberates entrepreneurs, and enables markets. Influenced by groups such as the Cato Institute, the Mercatus Center, the Pacific Research Institute, the Phoenix Center, The Progress & Freedom Foundation, and the Technology Policy Institute, they consider the emergence of the Internet as a vehicle for commerce (*e.g.*, exchanging goods, services, and information in the marketplace) and a liberating and progressive force. They are skeptical of the need for government involvement, even government partnering with industry to more rapidly digitize the economy.

4. **Moderates**: This group is staunchly and unabashedly pro-IT, seeing it as this era's driving force for both economic growth and social progress. While they view the Internet as a unique development to which old rules and laws may not apply, they believe appropriate guidelines must be developed if it is to reach its full potential. Likewise, they argue that while rules and regulations should not favor bricks-and-mortar companies (see #8 below) over Internet ones, neither should they favor Internet companies over bricks-and-mortars. Moreover, they argue that while government should "do no harm" to limit IT innovations, it should also "actively do good" by adopting policies to promote digital transformation in areas such

as broadband, the smart electric grid, health IT, intelligent transportation systems, mobile payments, digital signatures, and others. Examples of moderates include the Center for Advanced Studies in Science and Technology Policy, the Center for Strategic and International Studies, the Information Technology and Innovation Foundation (ITIF), and the Stilwell Center.

5. **Moral Conservatives**: This group sees the Internet as a dangerous place, a virtual den of iniquity, populated by pornographers, gamblers, child molesters, terrorists, and other degenerates. Unlike the free marketers, the moral conservatives have no qualms about enlisting governments to regulate the Internet. They have been the driving force behind the Communications Decency Act's censorship restrictions and Child Online Protection Act (both deemed unconstitutional), Internet filtering in libraries, and worked to push legislation to ban online gambling. They have also joined forces with the liberal social engineers (Group #2) in pushing for strong "net neutrality" regulations, fearing that Internet Service Providers (ISPs) will somehow discriminate against Christians online. This group argues that, because the Internet is a public space, some rules and laws are necessary to govern anti-social behavior. They do not believe that technology can solve all social problems—on the contrary, they believe that the Internet is generally furthering the decline of culture. Yet, in some instances they embrace the Internet as a tool, as evidenced by former Secretary of Education William Bennett's K-12 Internet-based home schooling project. In general, moral conservatives don't want individuals empowered to engage in antisocial behavior, nor do they want corporations to facilitate such behavior. Examples are groups like the Christian Coalition and Focus on the Family, and around the world with countries like Indonesia, Thailand, Saudi Arabia and other religiously conservative nations that seek to limit activity on the Internet.

6. **Old Economy Regulators**: This group believes that there is nothing inherently unique about the Internet and that it should be regulated in the same way that government regulates everything else, including past technologies. There is a certain sense of urgency among certain elected officials, government bureaucrats, and "public interest" advocates who believe that cyberspace is in a state of near-anarchy—a haven for criminals, con artists, and rapacious corporations. Exemplars of this group include, law enforcement officials seeking to limit use of encryption and other innovative technologies, veterans of the telecom regulatory wars that preceded the breakup of Ma Bell, legal analysts working for social engineering think tanks, as well as government officials seeking to impose restrictive regulatory frameworks on the broadband Internet. As far as old economy regulators are concerned, the 1934 Communications Act (or perhaps its 1996 update) answered all the questions that will ever arise

regarding the Internet. Moreover, European, Chinese and other old economy regulators overseas fear that, absent more regulation, their nations will be bypassed by the American Internet leviathan.

7. **Tech Companies & Trade Associations**: This group encompasses a range of organizations from the politically savvy hardware, software and communications giants to Internet start-ups. These businesses, from old stalwarts like IBM, AT&T, and Hewlett Packard to "teenagers" like Cisco Systems and Microsoft, and "youngsters" like Google and Facebook, understand that trade, tax, regulatory, and other public policy issues increasingly affect their bottom line and competitive position. While the players in this group (and in Bricks and Mortars) don't have the same level of ideological cohesion as the above groups, they share a certain set of interests which justifies their grouping. They realize that getting one's way in politics takes more than being right: It requires playing the game and making one's case persuasively. From time to time, some tech businesses may take the Internet exceptionalist position that the Internet should be left free from government intervention. Generally, they do so only to avoid regulation that might put them at a competitive disadvantage. On the whole, tech companies tend to believe that regulation can be both advantageous and detrimental; they do not fight against all regulations and are in favor of the right ones for them (and increasingly support the "wrong" ones for their competitors).[4] To some extent, they also advocate policies that are good for the technology industry or the economy as a whole. While communication companies, being in a traditionally regulated industry, have long recognized the importance of government, most IT companies have ignored government and policy issues, being too busy creating the technologies that drive the digital world. But as these companies have matured and become aware, often through painful experience, of how issues in Washington can affect their bottom line, many have evolved into political sophisticates. And while individual tech companies can have different views on different issues, these differences are largely rooted in business model interests, rather than ideological views about the market or government.

8. **Bricks-and-Mortars**: This group includes the companies, professional groups, and unions that gain their livelihood from old-economy, face-to-face business transactions. These include both producers (such as automobile manufacturers, record companies, and airlines) and distributors and middlemen (such as retailers, car dealers, wine wholesalers, pharmacies,

---

[4] For a discussion of how technology companies view public policy see ACT's *Understanding the IT Lobby: An Insider's Guide*, 2008, **http://actonline.org/publications/2008/08/05/understanding-the-it-lobby-an-insiders-guide/**.

optometrists, real estate agents, or unions representing workers in these industries). Many of them fear, often correctly, that the Internet is making them obsolete, while others have worked to transform their business models to take advantage of e-commerce. In recent years, there has been a widening rift between the bricks-and-mortar producers and the distributors and middlemen (and the unions that represent their workers). Producers have begun to realize that they can use the Internet to go directly to their consumers, bypassing (or at least minimizing) the role of bricks-and-mortar middlemen. The middlemen and unions, working actively to keep this from happening or at least to forestall the day of reckoning, are not shy about enlisting the aid of government to "level the playing field." Certainly, the long running battle over taxing Internet sales represented a fight between bricks-and-mortars and tech companies. Likewise, the grocery store workers' union in California has recently worked to pass legislation making it more difficult for stores to use self-service checkout systems.[5]

# The Dividing Lines

The above groups' attitudes about Internet policy can be placed along two axes:

## Individual Empowerment vs. Societal Benefit

This line separates groups on the basis of beliefs about the Internet's overriding purpose. In some ways this is a variant on the classic tension between liberty and equality. However, it goes beyond this to represent the tension between individualism and communitarianism, with the former being a focus on individual rights, and the latter invoking community benefits like economic growth, security, and improved quality of life.

Those in the individual empowerment category believe that IT's chief function is to liberate individuals from control by, or dependence on, big organizations. For them the Internet is a vast, open global communications medium designed principally to enable individuals to freely communicate and access information. When debating any issue, they examine it principally through the lens of how it affects individuals, not society as a whole. Thus, the issue of net neutrality is seen in terms of its effect on individual freedom to act in any way desired on broadband networks. Such groups want to put the little guy on the same playing field as the big boys, whether this means supporting small ISPs, small media outlets, or individual open source coders.

Those belonging in the societal benefit camp believe IT and the Internet's main job is to increase economic productivity, promote government responsiveness

---

5 Robert D. Atkinson, *Innovation and Its Army of Opponents*, BUSINESSWEEK, Sept. 23, 2010, **http://search.businessweek.com/Search?searchTerm=innovation+and+its+army+of+opponents&resultsPerPage=20**.

and efficiency, and enable the development new and better services for consumers as a societal whole. They tend to examine individual IT policy issues through the lens of how they affect the communitarian interest and are willing to accept tradeoffs to individual liberty or freedom if they boost overall economic or societal well-being. For example, they see the actions of ISPs to manage their broadband networks as being necessary to help the majority of the users, even if it means that a few "bandwidth hogs" have to wait a minute or two longer to download their pirated copy of *Lord of the Rings*. They also believe that both government and corporations can serve as proxies for community interests, and that what's good for, say, Cisco, AT&T, Microsoft or Google or the federal government can be good for America as whole. Some groups fall in between the two extremes and argue that tradeoffs between particular individual's benefit (or harm) and community interests are inevitable.

Internet exceptionalists and social engineers generally believe the Internet is all about individual empowerment. The former resent its commercialization and view empowerment as inevitable. The latter, as stated earlier, believe the Internet should mainly be an educational and social networking tool and fear its empowering capabilities will be taken away by powerful multinational corporations and statist governments that will reshape the Internet to serve their own narrow purposes (profit in the former, control in the latter). Both see hackers and pirates as lone champions standing tall against greedy corporate and inept government leviathans.

Bricks-and-mortars and old economy regulators see IT in instrumental terms as designed for commerce and, by extension, for the community benefit. They just don't like how the Internet has evolved, whether it's competition from Dot-Coms or the spread of strong encryption that frustrates government surveillance, censorship, and other control. Tech companies also see IT in more instrumental terms, arguing that its rules should facilitate robust commerce. Moral conservatives don't want individuals empowered, since this will just enable even more antisocial behavior, and they also don't want corporations to facilitate such behavior.

Moderates and free marketers occupy the middle ground. They believe that the digitization of the economy holds great promise for boosting productivity and improving society. At the same time, they see the Internet as creating communities, boosting education, and giving people more control over their lives. Free marketers don't believe that individual interests should necessarily trump corporate interests—they see corporations as persons under the law.

## Laissez-Faire vs. Government Regulation

The groups divide along this line over the degree to which the government should impose formal rules on IT and the Internet.

Internet exceptionalists, and to a lesser degree free marketers, believe the Internet should be governed by its users. These groups lie on the *laissez-faire* side of the dividing line. They consider the Internet unique and capable of creating spontaneous order, a model for how the rest of society should be organized. Free marketers believe the Internet is what allows Coase's vision of a society with low transaction costs and ubiquitous markets to become a reality.[6]

At the other extreme are groups on the government regulation side of the line, who see the Internet as a new "Wild West" calling for a man with a badge to protect vulnerable citizens against intrusive governments and profit-hungry corporations. Moral conservatives, social engineers, and old economy regulators tend to hold this view, arguing for an array of government actions to limit what companies can do. So do bricks-and-mortars, although less as a matter of principle than as a way of clinging to their ever-weakening economic position.

Moderates and tech companies occupy the middle ground. They believe the Internet is unique and generally requires a light regulatory touch if IT innovation is to thrive. But in some key areas such as cybersecurity and copyright protection, they believe that the Internet needs stronger rules, especially to enable law enforcement to go after bad actors. In still other areas, such as the privacy of non-sensitive data and net neutrality, they believe that self-regulating government/business partnerships are the best way to protect consumers while giving companies needed flexibility.

ITIF was formed to advance a set of pragmatic solutions to the growing number of technology-related policy problems. We believe the growth of the digital economy and society depends on a synthesis of these views: the correct position will tend to lie at the intersection of the two axes. The dichotomy between individual empowerment and institutional efficiency is not a zero-sum game. Individuals benefit both socially and economically when governments and corporations work more efficiently and effectively, and institutions benefit when individuals are informed and able to make choices. A light touch on regulation is important to maintain the flexibility required to operate in this high-speed economy, but government action is also necessary to give businesses and consumers confidence that the Internet is not a den of thieves or a market tilted against fair competition, and to help speed digital transformation (*e.g.*, the ubiquitous use of IT throughout the economy and society).

---

6 Economist Ronald Coase postulated that high transaction costs engendered large organizations. *See, e.g.*, RONALD COASE, THE FIRM, THE MARKET AND THE LAW (1988).

# Ongoing Policy Debates

Of course, the above typology is imperfect—with many individuals and organizations falling into more than one group or no group at all. But as one looks at the central political fights about the future of information technology, the influence of these competing factions is clear. As case studies, we consider the recent debates over four key issues: privacy, taxation, copyright protection, and net neutrality.

## Privacy

While the recent flaps over Facebook and Google Street View are the most visible examples, the collection and use of personal information about Internet users by corporations and government is the source of many heated and emotional debates. Old economy regulators and social engineers want to impose sweeping regulations that would give individuals control over "their" personal data. And while they tolerate, grudgingly, advertising as the one true business model for Internet content and services (they oppose ISPs allowing content or application companies to voluntarily pay for prioritized service) they want to limit the effectiveness of online advertising, and the revenue it can raise, because of privacy fears.

Many tech companies want complete freedom to collect personal data, provided they comply with privacy policies they write themselves. And while some tech companies have supported moderate "notice and choice" legislation, most companies remain wary of any federal regulation of privacy, even as they recognize the need for federal laws to preempt increasingly antsy state legislators from passing a patchwork of different Internet privacy bills.

Internet exceptionalists expect technology to solve the problem. As far as they're concerned, users should take responsibility for their own privacy and apply the tools available to protect their personal data.

Free marketers reject the need for privacy legislation, asserting that the harms from regulation would far outweigh the benefits, and that government regulation is likely to be an imposition on individual liberty and choice, including basic rights of free speech. While moderates worry that overly-strict privacy laws would stifle innovation and increase costs for consumers, they also believe that, absent any rules, users will not develop the trust needed for the digital economy and society to flourish.

The recent furor over Facebook is a perfect example of how these issues play out. This social network company announced two new features in 2010: instant personalization, which allows users to share data from their Facebook profile with partner websites, and social plug-ins for third party websites, which allow

users to more easily share web pages they like with their social network outside of Facebook.[7]

Social engineers howled in protest, demanding restrictive government regulations to bar such practices. Some, like Danah Boyd, a fellow at Harvard's Berkman Center for Internet and Society, went so far as to claim that Facebook functioned as a public utility and should be regulated like one.[8]

Facebook was slow to react, initially focusing more on highlighting the benefits of its innovative new tools. However, it quickly responded more appropriately, rolling out a much more user-friendly and transparent system of user privacy controls.

ITIF and other moderates as well as free marketers argue that government control over the privacy policies of social networks is not necessary to protect consumers and moreover, would be harmful to future innovation. In the heated political environment of the privacy debate, government intervention would probably become regulatory overkill. At the same time, moderates argue that legitimate privacy concerns about personally identifiable data and sensitive data (financial or medical information, for example) need to be addressed through comprehensive industry-wide codes of self-regulation, enforceable by government action (*e.g.*, FTC action against companies that do not live up to their own privacy policies for unfair and deceptive trade practices).

When it comes to the collection and use of data by government, the coalitions reconfigure. Here the Internet exceptionalists, social engineers, and free marketers make common cause in their crusade against "Big Brother." It largely does not matter whether the goal is to crack down on deadbeat dads, catch red light runners, or prevent terrorist attacks: If it involves the government collecting more information or using existing information for new purposes, these groups will generally oppose it. In protesting against the growing practice of cities installing red light cameras, former Republican House majority leader Dick Armey railed: "This is a full-scale surveillance system. Do we really want a society where one cannot walk down the street without Big Brother tracking our every move?"[9]

---

7 For more see: Daniel Castro, Information Technology and Innovation Foundation, *The Right to Privacy is Not a Right to Facebook*, April 2010), **http://itif.org/publications/facebook-not-right**; and Daniel Castro, Information Technology and Innovation Foundation, *Facebook is Not the Enemy*, 2010, **http://itif.org/publications/facebook-not-enemy**.

8 Danah Boyd, *Facebook is a utility; utilities get regulated*, APOPHENIA, May 15, 2010, **http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html**.

9 Thomas C. Greene, *Cops Using High-Tech Surveillance in Florida*, THE REGISTER, July 2, 2001, **http://www.theregister.co.uk/2001/07/02/cops_using_hightech_surveillance/**.

High-tech companies have engaged in the debate over government use of and access to data based in large part on their business interests. Technology companies with direct business interests in providing government technologies to collect information (*e.g.*, smart card and biometrics companies) have been strong supporters of particular initiatives. Other technology companies, worrying that government access to data can restrict commerce or reduce consumer trust in the Internet (*e.g.*, in cloud computing applications where consumer data is remotely stored) have called for limitations or procedural safeguards on government access to data.

Whether a middle position in the debate can be found remains an ongoing question. Moderates support the adoption of new technologies by government, if it is clearly demonstrated that they fulfill an important public mission and if potential privacy problems are effectively addressed, especially by designing privacy protections into systems. At the same time, they support putting into place adequate rules and protections governing the access to that data by government.

## Internet Sales Taxes

Tax policy is controversial in any setting, but perhaps particularly so with regard to the Internet. The collection of state and local sales taxes for Internet transactions is so controversial that 15 years after it was first raised, the issue continues to be debated. Old economy regulators want sales taxes to be collected on Internet purchases and want high taxes on telecommunications services to maintain their revenue. The state of Colorado has gone so far as to require Internet retailers to share the names and purchase information of Colorado residents with the state government (so the state can collect a "use" tax from Internet shoppers). Bricks and mortar companies want sales taxes imposed to maintain their competitive position against pure-play Internet retailers. Some social engineers favor not only sales tax collection, but also special taxes on broadband use to subsidize access for low-income and rural households.

By contrast, the tech companies involved in selling over the Internet do not want the burden of collecting taxes over thousands of jurisdictions, and they do not want to lose their price advantage. Likewise, they do not want broadband or telephone service unfairly taxed at higher rates. Others—like many free marketers and Internet exceptionalists—oppose Internet sales taxes on principle. They believe "the fewer taxes the better," especially when it comes to promoting the new digital economy.

Internet exceptionalists, tech companies, and free marketers will likely continue to oppose giving states the right to tax Internet sales to their residents from companies outside their borders. State governments will press hard for the right, citing their large budget shortfalls. And pragmatists will likely favor state sales

taxes, particularly if they are tied to a *quid pro quo* deal forcing states to rescind laws and regulations that discriminate against e-commerce sellers, and if taxation is administered in ways that minimize administrative burden. For now, however, the debate continues, with states legally unable to collect sales taxes and most states imposing high, discriminatory taxes on telecommunications services.

## Copyright Protection

As virtually all media have become digital, protecting copyrights has become a nightmare. The controversy over the file sharing system Napster almost a decade ago was just the beginning. The ubiquity of file-sharing technologies, coupled with computers that can rip digital files from CDs or DVDs, and high-speed broadband networks that can quickly transfer large files, has meant that "digital piracy" has grown like wildfire. Internet exceptionalists argue that the Internet Age marks the end of intellectual property rights because enforcing copyright protections on digital media is too difficult (hence their mantra "information wants to be free.") These advocates claim that non-commercial file "sharing" of copyrighted media is a form of fair use, which they assert is legal under copyright law. For example, the Electronic Freedom Forum's "Let the Music Play" campaign protests the music and film industries' prosecution of file copiers. In their ideal world, some rich dot-com entrepreneur would establish a separate country on a desert island, linked to the rest of the world by high speed fiber-optic cable and hosting a massive computer with a cornucopia of pirated digital content, all beyond the reach of national copyright laws.

Many social engineers side with the Internet exceptionalists, though for very different reasons. They fear that technology will let copyright holders exact such strict control on content that traditional notions of fair use will become obsolete. And they fear that digital rights management (DRM) technologies will become so stringent that activities consumers have long enjoyed (like the ability to play music files on more than one device) will be prohibited. Both argue strongly against any efforts to better control digital copyright theft that may impinge on individual liberty or individual rights like free speech (*e.g.*, permitting ISPs to filter for illegal content or crafting international treaties like ACTA to strengthen and harmonize anti-piracy efforts). And both would love to see the Digital Millennium Copyright Act (DMCA) enter the dust bin of IT policy history, particularly the academics and engineers who feel the DMCA restricts their ability to hack DRM technology in the name of research.[10]

Because of their emphasis on property rights, most free marketers tend to strongly support efforts to limit digital copyright theft. But with their focus on freedom, a few come all the way around to the left, arguing that because liberty

---

[10] Michele Boldrin, Against Intellectual Monopoly, Nov. 10, 2008, **http://www.cato.org/event.php?eventid=5362**.

trumps property, the grant of intellectual property rights by government amounts to the provision of a state-sanctioned monopoly.[11] In their view, individuals should be free to use digital content in ways they want and content owners—not others such as digital intermediaries—should be responsible for policing the use of their content.

Moderates also support efforts to limit digital copyright theft, believing that such theft is wrong, and that a robust digital ecosystem requires economic incentives to produce often expensive digital content. At the same time, however, they are not absolutists, and in particular seek to balance the costs and benefits of copyright defense, especially through fair use.

The bricks and mortar companies—including the Recording Industry Association of America—initially worked to block the development of new technologies that facilitate playing downloaded and possibly pirated music. But more than a decade later the content industries are not so much fighting against such technologies as they are working to develop and use technologies that can counter copyright theft, and going after organizations that enable widespread digital content theft (*e.g.*, the Swedish Pirate Bay).[12] And even as they have struggled to cope with music and movie piracy, content producers have largely come to terms with the realities of the digital era: They have begun providing legal, affordable, and consumer-friendly means for consumers to buy or view copyright-protected digital content, with Apple's iTunes music store and Hulu being the most prominent examples.

Although generally sympathetic to the content providers' copyright concerns, many high-tech companies (*e.g.*, ISPs, search engines, social networks) fear that the federal government will require them to adjust their businesses to become copyright enforcers, either by having to take action against their customers or by building in expensive content protection technologies. Once again, the question is whether a compromise can be found, ensuring that content holders have the legal protections and economic incentives they need to continue producing copyrighted materials without imposing overly-large burdens on technology companies, and by extension their customers.

---

11 *See, e.g.,* Cato Institute, *Against Intellectual Monopoly*, 2008, **http://www.cato.org/event.php?eventid=5362**.

12 Eric Pfanner, *Music Industry Counts the Cost of Piracy*, THE NEW YORK TIMES, Jan. 21, 2010, **http://www.nytimes.com/2010/01/22/business/global/22music.html?ref=recording_industry_association_of_america**; Eamonn Forde, *From Peer to Eternity: Will Jumping the Legal Divide Solve Anything?*, THE MUSIC NETWORK, Dec. 6, 2010, **http://www.themusicnetwork.com/music-features/industry/2010/12/06/from-peer-to-eternity-will-jumping-the-legal-divide-solve-anything/**.

## Net Neutrality

What has become a highly contentious issue, net neutrality, refers to the idea that the individual networks collectively forming the Internet be controlled by users rather than by their owners and operators. While network operators are in a unique position to manage their resources, proponents of net neutrality believe they cannot be trusted to utilize their knowledge for the good of the Internet user community.

Social engineers are the most passionate about net neutrality, but they make common cause with the veterans of the old economy regulator group and Internet exceptionalists. Indeed, social engineer Tim Wu coined the still-mystifying term "net neutrality."[13] These groups fear that the Internet's unique nature is under threat by the forces of incumbent telecommunications and cable companies providing broadband service. If "Big Broadband" gets its way, neutralists fear the Internet will go the way of cable TV, the "vast wasteland"[14] where elitist programming such as *The Wire* competes with advertising-supported, populist programming such as *American Idol.*

Free marketers see net neutrality as one more attack by big government regulators on the Internet, the last bastion of freedom from regulation. They argue that market forces and consumer choice will always discipline any anti-consumer violations of net neutrality, while antitrust or tort law will serve as a handy tool to remedy any anti-business violations.

Tech companies are split on the issue, largely around which side of the network they are on. Those tech companies providing network services (*e.g.*, ISPs and major equipment makers) are generally against strong regulations in support of network neutrality (at least with regard to the network itself) while companies whose business model depends on using the network to gain access to customers (*e.g.*, content & service providers like Google) are either neutral or in favor of a stronger regulatory regime (at least with regard to the infrastructure layers, as opposed to other parts of the Internet "stack," such as applications.)

---

13 Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 JOURNAL OF TELECOMMUNICATIONS AND HIGH TECHNOLOGY LAW 141 (2003), **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863**.

14 On May 9, 1961, in a speech to the National Association of Broadcasters, newly-appointed FCC chairman Newton N. Minow referred to television as a "vast wasteland." Newton N. Minow, "Television and the Public Interest," address to the National Association of Broadcasters, Washington, D.C., May 9, 1961.

However, these differences have begun to blur somewhat, as evidenced by the October 2009 joint statement on net neutrality issued by Google and Verizon.[15]

Moderates generally see the Internet as a work-in-progress. Moderates believe it is good that network equipment producers are improving the Internet and recognize operators as possessing the highly specialized knowledge needed to provide equitable access to the Internet's pool of resources. But moderates realize that competition doesn't operate as efficiently in some network markets as it does in the markets for general-purpose consumer goods and services. In other words, some network markets are under-competitive (because network effects create market power), so markets alone aren't sufficient to guarantee an open Internet for everyone.[16] The role of government in Internet regulation is to ensure that all consumers enjoy the fruits of investment and innovation, but only in ways that don't limit continued investment and innovation.

As these and other issues continue to be fought in legislatures and communities around the country, government officials should seek solutions that balance the needs of individuals with those of society, and that offer the security of codified laws when necessary and the flexibility of informal rules when appropriate. As the technology policy debates go on and the various factions push for the solutions that fit their ideologies and interests, the policies that promote the growth and vitality of the digital economy will not be found at the extremes, but instead in the vital center.

## The Future of Digital Politics

Some might argue that these issues are transitory and will recede in importance as the digital economy matures. But there is good reason to believe otherwise: The debates that pit online consumers against resistant middlemen are likely to continue as new forms of online distribution evolve. The emergence of much faster and ubiquitous wired and wireless broadband networks will mean more Americans using these networks and more business models developing to take advantage of them. Data generated by emerging new technologies such as wireless location systems, digital signature systems, intelligent transportation systems, the smart electric grid, health IT, and radio frequency identification (RFID) devices—some used by government, others by the private sector—will drive new privacy concerns among social engineers and their fellow travelers. In some ways, the digital revolution has been so successful that many previously

---

15 Lowell McAdam, CEO Verizon Wireless & Eric Schmidt, CEO Google, Finding Common Ground on an Open Internet, Verizon PolicyBlog, Oct. 21, 2009, **http://policyblog.verizon.com/BlogPost/675/FindingCommonGroundonanOpenInternet.aspx**.

16 Richard Bennett, Information Technology and Innovation Foundation, *ITIF Comments on FCC Broadband Reclassifying*, August 10, 2010, **http://www.itif.org/publications/itif-comments-fcc-broadband-reclassifying**.

analog political issues have become digital issues; on the other hand, the political issues of the future remain unformed, precisely because the technologies are changing so quickly.

The public policy issues surrounding the IT revolution are no longer sideshows or mere theoretical discussions for a handful of technologically savvy people, nor are they the royal road to a utopia of untold wealth and perfect freedom. The battle lines have been drawn, and the issues are both serious and complex. Digital politics, if not the great issue of our age, will be central to the life of our nation in the decade ahead—and well beyond.

# PART II

## ISSUES & APPLICATIONS

# CHAPTER 6

## SHOULD ONLINE INTERMEDIARIES BE REQUIRED TO POLICE MORE?

# Trusting (and Verifying) Online Intermediaries' Policing

By Frank Pasquale*

## Introduction

Internet Service Providers (ISPs) and search engines have mapped the Web, accelerated e-commerce, and empowered new communities. They can also enable intellectual property infringement, harassment, stealth marketing, and frightening levels of surveillance. As a result, individuals are rapidly losing the ability to control their own image on the web, or even to know what data others are presented with regarding them. When Web users attempt to find information or entertainment, they have little assurance that a carrier or search engine is not subtly biasing the presentation of results in accordance with its own commercial interests.[1]

None of these problems is readily susceptible to swift legal intervention. Instead, intermediaries themselves have begun policing their own virtual premises. eBay makes it easy for intellectual property owners to report infringing merchandise. A carrier like Comcast has the technical power to slow or block traffic to and from a site like BitTorrent, which is often accused of infringement.[2] Google's StopBadware program tries to alert searchers about malware-ridden websites,[3] and YouTube employs an indeterminate number of people to police copyright infringement, illegal obscenity, and even many grotesque or humiliating videos.[4] Reputable social networks do the same for their own content.

---

* Professor of Law, Seton Hall Law School; Visiting Fellow, Princeton Center for Information Technology Policy.

1 Benjamin Edelman, *Hard-Coding Bias in Google "Algorithmic" Search Results*, Nov. 15, 2010, available at **http://www.benedelman.org/hardcoding/** ("I present categories of searches for which available evidence indicates Google has "hard-coded" its own links to appear at the top of algorithmic search results, and I offer a **methodology** for detecting certain kinds of tampering by comparing Google results for similar searches. I compare Google's hard-coded results with Google's public **statements** and promises, including a dozen denials but at least one admission.").

2 *See, e.g.*, Comcast Corp. v. FCC, No. 08-1291, 2010 U.S. App. LEXIS 7039 (D.C. Cir. April 6, 2010).

3 For more information, visit **http://stopbadware.org/**.

4 YouTube, *YouTube Community Guidelines*, **http://www.youtube.com/t/community_guidelines** ("YouTube staff review flagged

Yet all is not well in the land of online self-regulation. However competently they police their sites, nagging questions will remain about their fairness and objectivity in doing so. Is Comcast blocking BitTorrent to stop infringement, or to decrease access to content that competes with its own for viewers? How much digital due process does Google need to give a site it accuses of harboring malware? If Facebook eliminates a video of war carnage, is that a token of respect for the wounded or one more reflexive effort of a major company to ingratiate itself with a Washington establishment currently committed to indefinite military engagement in the Middle East?

Questions like these will persist, and erode the legitimacy of intermediary self-policing, as long as key operations of leading companies are shrouded in secrecy. Administrators must develop an institutional competence for continually monitoring rapidly-changing business practices. A trusted advisory council charged with assisting the Federal Trade Commission (FTC) and Federal Communications Commission (FCC) could help courts and agencies adjudicate controversies concerning intermediary practices. An Internet Intermediary Regulatory Council (IIRC) would spur the development of what Christopher Kelty calls a "recursive public"—one that is "vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its own existence as a public."[5] Questioning the power of a dominant intermediary is not just a preoccupation of the anxious. Rather, monitoring is a prerequisite for assuring a level playing field online.

## Understanding Intermediaries' Power

Internet intermediaries govern online life.[6] ISPs and search engines are particularly central to the web's ecology. Users rely on search services to map the web for them and use ISPs to connect to one another. Economic sociologist David Stark has observed that "search is the watchword of the information age."[7] ISPs are often called "carriers" to reflect the parallel

---

videos 24 hours a day, seven days a week to determine whether they violate our Community Guidelines. When they do, we remove them.")

5 CHRISTOPHER M. KELTY, TWO BITS: THE CULTURAL SIGNIFICANCE OF FREE SOFTWARE 3 (Duke Univ. Press 2007).

6 For a definition of intermediary, *see* Thomas F. Cotter, *Some Observations on the Law and Economics of Intermediaries*, 2006 MICH. ST. L. REV. 67, 68–71 ("[A]n 'intermediary' can be any entity that enables the communication of information from one party to another. On the basis of this definition, any provider of communications services (including telephone companies, cable companies, and Internet service providers) qualify as intermediaries.").

7 DAVID STARK, THE SENSE OF DISSONANCE: ACCOUNTS OF WORTH IN ECONOMIC LIFE 1 (Princeton Univ. Press 2009) ("Among the many new information technologies that are reshaping work and daily life, perhaps none are more empowering than the new technologies of search.").

between their own services in the new economy and transportation infrastructure. Online intermediaries organize and control access to an extraordinary variety of digitized content. Content providers aim to be at the top of Google Search or Google News results.[8] Services like iTunes, Hulu, and YouTube offer audio and video content. Social networks are extending their reach into each of these areas. Cable-based ISPs like Comcast have their own relationships with content providers.[9]

When an Internet connection is dropped, or a search engine fails to produce a result the searcher knows exists somewhere on the web, such failures are obvious. However, most web experiences do not unfold in such a binary, pass–fail manner. An ISP or search engine can slow down the speed or reduce the ranking of a website in ways that are very hard for users to detect. Moreover, there are many points of control, or layers, of the Web.[10] Even when users' experience with one layer causes suspicion, it can blame others for the problem.

The new power of intermediaries over reputation and visibility implicates several traditional concerns of the American legal system.[11] Unfortunately, Internet intermediaries are presently bound only by weak and inadequate enforcement of consumer protection and false advertising statutes, which were designed for very different digital infrastructures.

---

8 *See* Deborah Fallows & Lee Rainie, Pew Internet & Am. Life Project, *Data Memo: The Popularity and Importance of Search Engines* 2 (Aug. 2004), **http://www.pewinternet.org/pdfs/PIP_Data_Memo_Searchengines.pdf** ("The average visitor scrolled through 1.8 result pages during a typical search."); Leslie Marable, *False Oracles: Consumer Reaction to Learning the Truth About How Search Engines Work: Results of an Ethnographic Study*, CONSUMER WEBWATCH, June 30, 2003, at 5, *available at* **http://www.consumerwebwatch.org/pdfs/false-oracles.pdf** ("The majority of participants never clicked beyond the first page of search results. They trusted search engines to present only the best or most accurate, unbiased results on the first page.").

9 ROBERT W. MCCHESNEY, RICH MEDIA, POOR DEMOCRACY: COMMUNICATION POLITICS IN DUBIOUS TIMES 123 (2000) (describing how convergence of digital technology "eliminates the traditional distinctions between media and communications sectors").

10 JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 67 (2008) (describing a physical layer, the "actual wires or airwaves over which data will flow;" an application layer, "representing the tasks people might want to perform on the network;" a content layer, "containing actual information exchanged among the network's users;" and a social layer, "where new behaviors and interactions among people are enabled by the technologies underneath").

11 Yochai Benkler, *Communications Infrastructure Regulation and the Distribution of Control over Content*, 22 TELECOMM. POL'Y 183, 185–86 (1998) (describing the power of intermediaries over information flow: "technology, institutional framework, and organizational adaptation … determine … who can produce information, and who may or must consume, what type of information, under what conditions, and to what effect"); Cotter, *supra* note 6, at 69–71 (discussing some of the functions of technological intermediaries, including their control of information flow from suppliers to consumers).

In the space of a brief essay, I cannot survey the entire range of intermediary policing practices. But it is worthwhile to drill down a bit into the tough questions raised by one intermediary—the dominant search engine, Google—as it decides what is and is not an acceptable practice for search engine optimizers who want their clients' sites to appear higher in the rankings for given queries.

Search engineers tend to divide the search engine optimization (SEO) business into "good guys" and "bad guys," often calling the former "white hat SEO" and the latter "black hat SEO."[12] Some degree of transparency regarding the search engine's algorithm is required to permit white hat SEO. These rules are generally agreed upon as practices that "make the web better;" *i.e.*, have fresh content, don't sell links, don't "stuff metatags" with extraneous information just to get attention. However, if there were complete transparency, "black hat" SEOs could unfairly elevate the visibility of their clients' sites—and even if this were only done temporarily, the resulting churn and chaos could severely reduce the utility of search results. Moreover, a search engine's competitors could use the trade secrets to enhance its own services.

This secrecy has led to a growing gray zone of Internet practices with uncertain effect on sites' rankings. Consider some of the distinctions below, based on search engine optimization literature:

| **White Hat** (acceptable)[13] | **Gray Area** (unclear how these are treated)[14] | **Black Hat** (unacceptable; can lead to down-ranking in Google results or even the "Google Death Penalty" of De-Indexing) |
|---|---|---|
| Asking blogs you like to link to you, or engaging in reciprocal linking between your site and other sites in a legitimate dialogue.[15] | Paying a blogger or site to link to your blog in order to boost search results and not just to increase traffic. | Creating a "link farm" of spam blogs (splogs) to link to you, or linking between multiple sites you created (known as link farms) to boost search results.[16] |

12 Elizabeth van Couvering, *Is Relevance Relevant?*, **http://jcmc.indiana.edu/vol12/issue3/vancouvering.html** (search engineers' "animosity towards the … guerilla fighters of spamming and hacking, is more direct" than their hostility toward direct business competitors); Aaron Wall, *Google Thinks YOU Are a Black Hat SEO. Should You Trust Them?*, SEOBOOK, Apr. 17, 2008, **http://www.seobook.com/to-google-you-are-a-spammer** (claiming that Google discriminates against self-identified SEOs).

13 Phil Craven, 'Ethical' Search Engine Optimization Exposed!, WebWorkshop, **http://www.webworkshop.net/ethical-search-engine-optimization.html** (last visited Jun. 8, 2009).

14 Grey Hat SEO, **http://greyhatseo.com/** (last visited Jun. 5, 2006) (claiming a Grey Hat SEO is someone who uses black hat techniques in an ethical way.)

15 *Link Schemes*, GOOGLE WEBMASTER CENTRAL, **http://www.google.com/support/webmasters/bin/answer.py?answer=66356** ("The

| **White Hat** (acceptable)[13] | **Gray Area** (unclear how these are treated)[14] | **Black Hat** (unacceptable; can lead to down-ranking in Google results or even the "Google Death Penalty" of De-Indexing) |
|---|---|---|
| Running human-conducted tests of search inquiries with permission from the search engine. | Doing a few queries to do elementary reverse engineering. (This may not be permitted under the Terms of Service). | Using computer programs to send automated search queries to gauge the page rank generated from various search terms (Terms of Service prohibit this)[17] |
| Creating non-intentional duplicate content (through printer-friendly versions, pages aimed at mobile devices, *etc.*)[18] | Intentionally creating permitted duplicate content to boost search results | Intentionally creating unnecessary duplicate content on many pages and domains to boost results |
| Generating a coherent site with original and informative material aimed at the user | Creating content or additional pages that walk the line between useful information and "doorway pages" | Creating "doorway pages" that are geared towards popular keywords but that redirect to a largely unrelated main site.[19] |

---

best way to get other sites to create relevant links to yours is to create unique, relevant content that can quickly gain popularity in the Internet community. The more useful content you have, the greater the chances someone else will find that content valuable to their readers and link to it.").

16 Duncan Riley, *Google Declares Jihad On Blog Link Farms*, TECHCRUNCH, Oct. 24, 2007, **http://www.techcrunch.com/2007/10/24/google-declares-jihad-on-blog-link-farms/**.

17 *Automated Queries*, GOOGLE WEBMASTER CENTRAL, **http://www.google.com/support/webmasters/bin/answer.py?answer=66357** ("Google's Terms of Service do not allow the sending of automated queries of any sort to our system without express permission in advance from Google."); Google Terms of Service: Use of the Services by you, **http://www.google.com/accounts/TOS** (last visited Jun. 4, 2009) ("You agree not to access (or attempt to access) any of the Services by any means other than through the interface that is provided by Google, unless you have been specifically allowed to do so in a separate agreement with Google.").

18 *Duplicate Content*, GOOGLE WEBMASTER CENTRAL, **http://www.google.com/support/webmasters/bin/answer.py?answer=66359** ("Examples of non-malicious duplicate content could include: Discussion forums that can generate both regular and stripped-down pages targeted at mobile devices, Store items shown or linked via multiple distinct URLs, Printer-only versions of web pages").

19 Google Blogoscoped, *German BMW Banned From Google*, Feb. 4, 2006, **http://blogoscoped.com/archive/2006-02-04-n60.html**; Matt Cutts, *Ramping up on International Webspam*, MATT CUTTS: GADGETS, GOOGLE, AND SEO, Feb. 4, 2006, **http://www.mattcutts.com/blog/ramping-up-on-international-webspam/** (Google employee confirming BMW's ban).

| **White Hat** (acceptable)[13] | **Gray Area** (unclear how these are treated)[14] | **Black Hat** (unacceptable; can lead to down-ranking in Google results or even the "Google Death Penalty" of De-Indexing) |
|---|---|---|
| Targeting an appreciative audience[20] | Putting random references to salacious or celebrity topics on a blog primarily devoted to discussing current affairs[21] | Distracting an involuntary audience with completely misleading indexed content (akin to "initial interest confusion" in Internet trademark law)[22] |
| Influencing search engine by making pages easier to scan by automated bots[23] | Creating "hidden pages" when there may be a logical reason to show one page to search engine bots and another page to users who type in the page's URL | Using "hidden pages" to show a misleading page to search engine bots, and another page to users who type in the page's URL |

As these practices show, search engines are referees in the millions of contests for attention that take place on the web each day. There are hundreds of entities that want to be the top result in response to a query like "sneakers," "restaurant in New York City," or "best employer to work for." Any academic who writes on an obscure subject wants to be the "go-to" authority when it is Googled—and for consultants, a top or tenth-ranked result could be the

---

20 *Webmaster Guidelines: Design and content guidelines*, GOOGLE WEBMASTER CENTRAL, **http://www.google.com/support/webmasters/bin/answer.py?answer=35769** (last visited Jun. 4, 2009) ("Think about the words users would type to find your pages, and make sure that your site actually includes those words within it.").

21 Daniel Solove, *Thanks, Jennifer Aniston (or the Manifold Ways to Do the Same Search),* CONCURRING OPINIONS, ***http://www.concurringopinions.com/archives/2006/01/thanks_jennifer.html*** ("One of my more popular posts is one entitled ***Jennifer Aniston Nude Photos and the Anti-Paparazzi Act***. It seems to be getting a lot of readers interested in learning about the workings of the Anti-Paparazzi Act and the law of information privacy. It sure is surprising that so many readers are eager to understand this rather technical statute. Anyway, for the small part that Jennifer Aniston plays in this, we thank her for the traffic."); Dan Filler, *Coffee Or Nude Celebrity Photos: A Tale Of Two Evergreen Posts*, THE FACULTY LOUNGE, **http://www.thefacultylounge.org/2008/04/coffee-or-nude.html** ("significant amounts of traffic arrived in the form of web surfers seeking out pictures of Jennifer Aniston").

22 Jason Preston, *Google punishes Squidoo for having too much Spam*, BLOG BUSINESS SUMMIT, Jul. 11, 2007, **http://blogbusinesssummit.com/2007/07/google-punishes-squidoo-for-having-too-much-spam.htm**.

23 *Webmaster Guidelines: Design and Content Guidelines*, GOOGLE WEBMASTER CENTRAL, **http://www.google.com/support/webmasters/bin/answer.py?answer=35769** (last visited Jun. 4, 2009) ("Create a useful, information-rich site, and write pages that clearly and accurately describe your content."); *Id.* ("Try to use text instead of images to display important names, content, or links. The Google crawler doesn't recognize text contained in images.").

difference between lucrative gigs and obscurity. The top and right hand sides of many search engine pages are open for paid placement; but even there the highest bidder may not get a prime spot because a good search engine strives to keep even these sections very relevant to searchers.[24] The organic results are determined by search engines' proprietary algorithms, and preliminary evidence indicates that searchers (and particularly educated searchers) concentrate attention there. Businesses can grow reliant on good Google rankings as a way of attracting and keeping customers.

For example, John Battelle tells the story of the owner of 2bigfeet.com (a seller of large-sized men's shoes), whose site was knocked off the first page of Google's results for terms like "big shoes" by a sudden algorithm shift in November 2003, right before the Christmas shopping season. The owner attempted to contact Google several times, but said he "never got a response." Google claimed the owner may have hired a search engine optimizer who ran afoul of its rules—but it would not say precisely what those rules were.[25] Like the IRS's unwillingness to disclose all of its "audit flags," the company did not

---

[24] Steven Levy, *Secret of Googlenomics: Data-Fueled Recipe Brews Profitability*, WIRED, May 2, 2009, **http://www.wired.com/culture/culturereviews/magazine/17-06/nep_googlenomics** (in Google's AdWords program,"The bids themselves are only a part of what ultimately determines the auction winners. The other major determinant is something called **the quality score**. This metric strives to ensure that the ads Google shows on its results page are true, high-caliber matches for what users are querying. If they aren't, the whole system suffers and Google makes less money."); *see also* Google, *What is the Quality Score and How is it Calculated*, **http://adwords.google.com/support/aw/bin/answer.py?hl=en&answer=10215** (last visited Sept. 1, 2009) ("The AdWords system works best for everybody—advertisers, users, publishers, and Google too—when the ads we display match our users' needs as closely as possible.").

[25] JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE (Portfolio Trade 2005). *See also* Joe Nocera, *Stuck in Google's Doghouse*, N.Y. TIMES, Sept. 13, 2008, **http://www.nytimes.com/2008/09/13/technology/13nocera.html** ("In the summer of 2006 … Google pulled the rug out from under [web business owner Dan Savage, who had come to rely on its referrals to his page, Sourcetool]… . When Mr. Savage asked Google executives what the problem was, he was told that Sourcetool's "landing page quality" was low. Google had recently changed the algorithm for choosing advertisements for prominent positions on Google search pages, and Mr. Savage's site had been identified as one that didn't meet the algorithm's new standards… . Although the company never told Mr. Savage what, precisely, was wrong with his landing page quality, it offered some suggestions for improvement, including running fewer AdSense ads and manually typing in the addresses and phone numbers of the 600,000 companies in his directory, even though their Web sites were just a click away. At a cost of several hundred thousand dollars, he made some of the changes Google suggested. No improvement."). Savage filed suit against Google on an antitrust theory, which was dismissed in March 2010. *See* TradeComet, LLC v. Google, Inc., 2010 U.S. Dist. LEXIS 20154 (S.D. N.Y. March 5, 2010), **http://www.courthousenews.com/2010/03/08/Google%20opinion.pdf**.

want to permit manipulators to gain too great an understanding of how it detected their tactics.

So far, claims like 2bigfeet.com's have not been fully examined in the judicial system, largely because Google has successfully deflected them by claiming that its search results embody opinions protected by the First Amendment. Several articles have questioned whether blanket First Amendment protection covers all search engine actions, and that conclusion has not yet been embraced on the appellate level in the United States.[26] The FTC's guidance to search engines, promoting the clear separation of organic and paid results, suggests that search engines' First Amendment shield is not insurmountable.[27] While a creative or opportunistic litigant could conceivably advance a First Amendment right to promote products or positions without indicating that the promotion has been paid for, such a challenge has not yet eliminated false advertising law, and even political speakers have been required to reveal their funding sources.[28]

## Qualified Transparency for Carrier & Search Engine Practices

Both search engines' ranking practices and carriers' network management should be transparent to some entity capable of detecting biased policing by these intermediaries.[29] There are some institutional precedents for the kind of monitoring that would be necessary to accomplish these goals. For example, the French Commission Nationale De L'Informatique et des Libertes (CNIL) has several prerogatives designed to protect the privacy and reputation of

---

26 Frank Pasquale, *Rankings, Reductionism, and Responsibility*, CLEVELAND ST. L. REV. (2006); Frank Pasquale & Oren Bracha, *Federal Search Commission*, 93 CORNELL L. REV. 1149 (2008); Jennifer A. Chandler, *A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet*, 35 HOFSTRA L. REV. 1095, 1109 (2007).

27 *See* Bracha & Pasquale, *Federal Search Commission*, *supra* note 26 (discussing the implications of Ellen Goodman's work on "stealth marketing" for search engines, and how the Hippsley Letter of 2002 inadequately addressed such concerns in the industry.).

28 In early cases alleging an array of unfair competition and business torts claims against search engines, the First Amendment has proven a formidable shield against liability. Search engines characterize their results as opinion, and lower courts have been reluctant to penalize them for these forms of expression. In other work, I have described why this First Amendment barrier to accountability should not be insurmountable. Search engines take advantage of a web of governmental immunities that they would be loath to surrender. *FAIR v. Rumsfeld*, 547 U.S. 47 (2006) and cognate cases stand for the proposition that such immunities can be conditioned on agreement to certain conditions on an entity's speech. Whatever the federal government's will, it is within its power to regulate ranking and rating entities in some way when they are so deeply dependent on governmental action. Frank Pasquale, *Asterisk Revisited*, 3 J. BUS. & TECH. LAW 61 (2008).

29 I mean partial in two senses of the word—unduly self-interested, or only partly solving problems they claim to be solving.

French citizens, and to enforce standards of fair data practices.[30] CNIL "ensure[s] that citizens are in a position to exercise their rights through information" by requiring data controllers to "ensure data security and confidentiality," to "accept on-site inspections by the CNIL," and to "reply to any request for information."[31] CNIL also grants individual persons the right to obtain information about the digital dossiers kept on them and the use of this information. For example, CNIL explains that French law provides that:

> Every person may, on simple request addressed to the organisation in question, have free access to all the information concerning him in clear language.
>
> Every person may directly require from an organisation holding information about him that the data be corrected (if they are wrong), completed or clarified (if they are incomplete or equivocal), or erased (if this information could not legally be collected).

---

30 Law No. 78-17 of January 6, 1978, J.C.P. 1978, III, No. 44692. English translation of law as amended by law of August 6, 2004, and by Law of May 12, 2009, **http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf**; French language text modified through Law No. 2009-526 of May 12, 2009, J.O., May 13, 2009, **http://www.cnil.fr/la-cnil/qui-sommes-nous/**; French language consolidated version as of May 14, 2009, **http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&fastPos=1&fastReqId=826368234&categorieLien=cid&oldAction=rechTexte**. Commission Nationale de l'Informatique et des Libertés (CNIL), founded by Law No. 78-17 of January 6, 1978, *supra*, is an independent administrative French authority protecting privacy and personal data held by government agencies and private entities. Specifically, CNIL's general mission consists of ensuring that the development of information technology remains at the service of citizens and does not breach human identity, human rights, privacy, or personal or public liberties.

31 CNIL, *Rights and Obligations*, **http://www.cnil.fr/english/the-cnil/rights-and-obligations/** (last visited Mar. 12, 2010). Specifically, Chapter 6, Article 44, of the CNIL-creating Act provides:

> The members of the "Commission nationale de l'informatique et des libertés" as well as those officers of the Commission's operational services accredited in accordance with the conditions defined by the last paragraph of Article 19 (accreditation by the commission), have access, from 6 a.m to 9 p.m, for the exercise of their functions, to the places, premises, surroundings, equipment or buildings used for the processing of personal data for professional purposes, with the exception of the parts of the places, premises, surroundings, equipment or buildings used for private purposes.

Law No. 78-17 of January 6, 1978, J.C.P. 1978, III, No. 44692, ch. 6, art. 44, at 30, **http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf**.

> Every person may oppose that information about him is used for advertising purposes or for commercial purposes.[32]

While the United States does not have the same tradition of protecting privacy prevalent in Europe,[33] CNIL's aims and commitments could prove worthwhile models for U.S. agencies.

U.S. policymakers may also continue to experiment with public–private partnerships to monitor problematic behavior at search engines and carriers. For instance, the National Advertising Division (NAD) of the Council of Better Business Bureaus is a "voluntary, self-regulating body" that fields complaints about allegedly untruthful advertising.[34] The vast majority of companies investigated by NAD comply with its recommendations, but can also resist its authority and resolve the dispute before the FTC.[35] Rather than overwhelming the agency with adjudications, the NAD process provides an initial forum for advertisers and their critics to contest the validity of statements.[36] NAD is part of a larger association called the National Advertising Review Council (NARC), which promulgates procedures for NAD, the Children's Advertising Review Unit (CARU), and the National Advertising Review Board (NARB).[37]

---

32 CNIL, Rights and Obligations, *supra* note 31.

33 James Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1155 (2004) (comparing U.S. and European privacy law).

34 Seth Stevenson, *How New Is New? How Improved Is Improved? The People Who Keep Advertisers Honest*, SLATE, July 13, 2009, **http://www.slate.com/id/2221968**.

35 *Id.* ("When an ad is brought to their attention, the NAD's lawyers review the specific claims at issue. The rule is that the advertiser must have substantiated any claims before the ad was put on the air, so the NAD will first ask for any substantiating materials the advertiser can provide. If the NAD lawyers determine that the claims aren't valid, they'll recommend that the ad be altered. The compliance rate on this is more than 95 percent. But if the advertiser refuses to modify the ad (this is a voluntary, self-regulating body, not a court of law), the NAD will refer the matter to the Federal Trade Commission. One such FTC referral resulted in an $83 million judgment against a weight-loss company.").

36 *Id.*

37 NATIONAL ADVERTISING REVIEW COUNCIL, THE ADVERTISING INDUSTRY'S PROCESS OF VOLUNTARY SELF-REGULATION: POLICIES AND PROCEDURES § 2.1(a) (July 27, 2009) ("The National Advertising Division of the Council of Better Business Bureaus (hereinafter NAD), and the Children's Advertising Review Unit (CARU), shall be responsible for receiving or initiating, evaluating, investigating, analyzing (in conjunction with outside experts, if warranted, and upon notice to the parties), and holding negotiations with an advertiser, and resolving complaints or questions from any source involving the truth or accuracy of national advertising."). Though billed as "self-regulation," it is difficult to see how the policy would have teeth were it not self-regulation in the shadow of an FTC empowered by the Lanham Act to aggressively police false advertising. The FTC has several mechanisms by which to regulate unfair business practices in commerce. *See, e.g.*, 15 U.S.C. § 45(b) (2006)

Instead of an "Innovation Environment Protection Agency (iEPA)" (the agency Lawrence Lessig proposed to supplant the FCC), I would recommend the formation of an Internet Intermediary Regulatory Council (IIRC), which would assist both the FCC and FTC in carrying out their present missions.[38] Like the NARC, the IIRC would follow up on complaints made by competitors, the public, or when it determines that a practice deserves investigation. If the self-regulatory council failed to reconcile conflicting claims, it could refer complaints to the FTC (in the case of search engines, which implicate the FTC's extant expertise in both privacy and advertising) or the FCC (in the case of carriers). In either context, an IIRC would need not only lawyers, but also engineers and programmers who could fully understand the technology affecting data, ranking, and traffic management practices.

An IIRC would research and issue reports on suspect practices by Internet intermediaries, while respecting the intellectual property of the companies it investigated. An IIRC could generate official and even public understanding of intermediary practices, while keeping crucial proprietary information under the control of the companies it monitors. An IIRC could develop a detailed description of safeguards for trade secrets, which would prevent anyone outside its offices from accessing the information.[39] Another option would be to allow IIRC agents to inspect such information without actually obtaining it. An IIRC could create "reading rooms" for use by its experts, just as some courts allow restrictive protective orders to govern discovery in disputes involving trade secrets. The experts would review the information in a group setting (possibly during a period of days) to determine whether a given intermediary had engaged in practices that could constitute a violation of privacy or consumer protection laws. Such review would not require any outside access to sensitive information.

I prefer not to specify at this time whether an IIRC would be a private or public entity. Either approach would have distinct costs and benefits explored (in part) by a well-developed literature on the role of private entities in Internet

---

(giving the commission the authority to register an official complaint against an entity engaged in unfair business methods).

38 It could include a search engine division, an ISP division focusing on carriers, and eventually divisions related to social networks or auction sites if their practices begin to raise commensurate concerns.

39 This is the way that the NAD proceeds. It provides specific procedures under which the participants can request that certain sensitive information be protected. *See* NAT'L ADVERTISING REVIEW COUNCIL, THE ADVERTISING INDUSTRY'S PROCESS OF VOLUNTARY SELF-REGULATION § 2.4(d)–(e), at 4–5 (2009), **http://www.nadreview.org/07_Procedures.pdf** (discussing procedure for confidential submission of trade secrets).

governance.[40] Regardless of whether monitoring is done by a governmental entity (like CNIL) or an NGO (like NARC), we must begin developing the institutional capacity to permit a more rapid understanding of intermediary actions than traditional litigation permits.[41]

It is not merely markets and antitrust enforcement that are insufficient to constrain problematic intermediary behavior—the common law is also likely to fall short. It is hard to imagine any but the wealthiest and most sophisticated plaintiffs' attorneys attempting to understand the tweaks to the Google algorithm that might have unfairly diminished their clients' sites' salience. Trade secrets have been deployed in the context of other litigation to frustrate investigations of black box algorithms.[42] Examination of Google's algorithms subject to very restrictive protective orders would amount to a similar barrier to accountability. Given its recent string of litigation victories, it is hard to imagine rational litigants continuing to take on that risk. Moreover, it makes little sense for a court to start from scratch in understanding the complex practices of intermediaries when an entity like the IIRC could develop lasting expertise in interpreting their actions.

A status quo of unmonitored intermediary operations is a veritable "ring of Gyges,"[43] tempting them to push the envelope with policing practices which

---

40 *See, e.g.*, Philip J. Weiser, *Internet Governance, Standard Setting, and Self-Regulation*, 28 N. KY. L. REV. 822, 822 (2001) (examining "in particular the nature and limits of a key private regulator of the Internet: standard-setting organizations and their institution of open, interoperable standards").

41 Google has already recognized the need for some kind of due process in response to complaints about its labeling of certain websites as "harmful" (due to the presence of viruses or other security threats at the sites) via the StopBadware program. *See* ZITTRAIN, FUTURE OF THE INTERNET, *supra* note 10, at 171 ("Requests for review—which included pleas for help in understanding the problem to begin with—inundated StopBadware researchers, who found themselves overwhelmed in a matter of days by appeals from thousands of Web sites listed. Until StopBadware could check each site and verify it had been cleaned of bad code, the warning page stayed up."). Google's cooperation with the Harvard Berkman Center for Internet Research to run the StopBadware program could prefigure future intermediary cooperation with NGOs to provide "rough justice" to those disadvantaged by certain intermediary practices.

42 *See* Jessica Ring Amunson & Sam Hirsch, *The Case of the Disappearing Votes: Lessons from the Jennings v. Buchanan Congressional Election Contest*, 17 WM. & MARY BILL RTS. J. 397, 397–98 (2008) ("[T]he litigation ultimately was utterly inconclusive as to the reason for the 18,000 electronic undervotes because discovery targeting the defective voting system was thwarted when the voting machines' manufacturer successfully invoked the trade-secret privilege to block any investigation of the machines or their software by the litigants.").

43 "The Ring of Gyges is a mythical magical artifact mentioned by the philosopher Plato in book 2 of his Republic (2.359a–2.360d). It granted its owner the power to become invisible at will. Through the story of the ring, Republic discusses whether a typical person would be moral if he did not have to fear the consequences of his actions." Wikipedia, *Ring of Gyges*, **http://en.wikipedia.org/wiki/Ring_of_Gyges** (last accessed Dec. 1, 2010).

cannot be scrutinized or challenged. Distortions of the public sphere are also likely. While a commercially-influenced "fast-tracking" or "up-ranking" of some content past others might raise suspicions among its direct (but dispersed) victims, the real issues it raises are far broader. If an online ecology of information that purports to be based on one mode of ordering is actually based on another, it sets an unfair playing field whose biases are largely undetectable by lay observers. Stealth marketing generates serious negative externalities that menace personal autonomy and cultural authenticity. Moreover, the degree of expertise necessary to recognize these externalities in the new online environment is likely to be possessed by only the most committed observers.

This potent combination of expertise and externalities is a classic rationale for regulation. As Danny Weitzner's proposal for "extreme factfinding" (in the context of the Google–DoubleClick merger review) recognized, only a dedicated group of engineers, social scientists, attorneys, and computer scientists are likely to be adept enough at understanding search engine decisions as a whole to understand particular complaints about them.[44] Someone needs to be able to examine the finer details of the publicly undisclosed operation of culturally significant automated ranking systems—that is, to watch those who watch and influence us.[45]

---

[44] *See generally*, Danny Weitzner, *What to Do About Google and Doubleclick? Hold Google to It's Word With Some Extreme Factfinding About Privacy Practices*, GOOGLE OPEN INTERNET POLICY BLOG, Oct. 8, 2007, **http://dig.csail.mit.edu/breadcrumbs/node/203**:

> In the 1990s, the FTC under Christine Varney's leadership pushed operators of commercial websites to post policies stating how they handle personal information. That was an innovative idea at the time, but the power of personal information processing has swamped the ability of a static statement to capture the privacy impact of sophisticated services, and the level of generality at which these policies tend to be written often obscure the real privacy impact of the practices described. It's time for regulators to take the next step and assure that both individuals and policy makers have information they need.

Weitzner proposes that "[r]egulators should appoint an independent panel of technical, legal and business experts to help them review, on an ongoing basis the privacy practices of Google." *Id.* The panel would be "made up of those with technical, legal and business expertise from around the world." *Id.* It would hold "public hearings at which Google technical experts are available to answer questions about operational details of personal data handling." *Id.* There would be "staff support for the panel from participating regulatory agencies," "real-time publication of questions and answers," and "[a]n annual report summarizing what the panel has learned." *Id.*

[45] In the meantime, Google has been developing a tool that would help consumers detect if their Internet service provider was "running afoul of Net neutrality principles." Stephanie Condon, *Google-Backed Tool Detects Net Filtering, Blocking*, CNET NEWS, Jan. 28, 2009, **http://news.cnet.com/8301-13578_3-10152117-38.html** ("[The tool, M-Lab,] is running three diagnostic tools for consumers: one to determine whether BitTorrent is being blocked or throttled, one to diagnose problems that affect last-mile broadband networks, and one to

## Why Dominant Search Engines & Carriers Deserve More Scrutiny than Dominant Auction Sites & Social Networks

Those skeptical of the administrative state may find this proposal to "watch the watchers" problematic. They think of intermediaries as primarily market actors, to be disciplined by market constraints. However, the development of dominant Web 2.0 intermediaries was itself a product of particular legal choices about the extent of intellectual property rights and the responsibilities of intermediaries made in legislative and judicial decisions in the 1990s. As intermediaries gained power, various entities tried to bring them to heel—including content providers, search engine optimizers, trademark owners, and consumer advocates. In traditional information law, claims under trademark, defamation, and copyright law might have posed serious worries for intermediaries. However, revisions of communications and intellectual property law in the late 1990s provided safe harbors that can trump legal claims sounding in each of these other areas.[46] Some basic reporting responsibilities are a small price to pay for continuing enjoyment of such immunities.

An argument for treating internet intermediaries more like regulated entities owes much to the trail-blazing work of legal realists. Among these, Robert Hale's work on utilities remains especially inspirational.[47] Hale developed many of the theoretical foundations of the New Deal, focusing on the ways in which the common law became inadequate as large business entities began ordering

---

diagnose problems limiting speeds."). It remains to be seen whether Google itself would submit to a similar inspection to determine whether it was engaging in stealth marketing or other problematic practices.

46 17 U.S.C. § 512(d) (2000) (Digital Millennium Copyright Act of 1998 safe harbor); 47 U.S.C. § 230(c)(1) (2000) (Communications Decency Act of 1997 safe harbor for intermediaries). For critical commentary on the latter, *see* Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 371 (2005) ("An activist judiciary, however, has radically expanded § 230 by conferring immunity on distributors. Section 230(c)(1) has been interpreted to preclude all tort lawsuits against ISPs, websites, and search engines. Courts have … haphazardly lump[ed] together web hosts, websites, search engines, and content creators into this amorphous category.").

47 Ilana Waxman, Note, *Hale's Legacy: Why Private Property is Not a Synonym for Liberty*, 57 HASTINGS L.J. 1009, 1019 ("Hale's most fundamental insight was that the coercive power exerted by private property owners is itself a creature of state power… . By protecting the owner's property right … 'the government's function of protecting property serves to delegate power to the owners' over non-owners, so that 'when the owners are in a position to require non-owners to accept conditions as the price of obtaining permission to use the property in question, it is the state that is enforcing compliance, by threatening to forbid the use of the property unless the owner's terms are met.' … .[A]ll property essentially constitutes a delegation of state power to the property owner…). For a powerful application of these ideas to Internet law, *see* Julie Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of 'Rights Management,'* 97 MICH. L. REV. 462 (1998).

increasing proportions of the national economy.[48] Hale's crucial insight was that many of the leading businesses of his day were not extraordinary innovators that "deserved" all the profits they made; rather, their success was dependent on a network of laws and regulation that could easily shift favor from one corporate player to another.[49] Hale focused his theoretical work on the utilities of his time, expounding an economic and philosophical justification for imposing public service obligations on them. Regulatory bodies like state utility commissions and the FCC all learned from his work, which showed the inadequacy of private law for handling disputes over infrastructural utilities.

Market advocates may worry that monitoring of search engines and carriers will lead to more extensive surveillance of the affairs of other intermediaries, like social networks and auction platforms. They may feel that competition is working in each of those areas, and should be the foundation of all intermediary policy. However, competition is only one of many tools we can use to encourage responsible and useful intermediaries. We should rely on competition-promotion via markets and antitrust only to the extent that (a) the intermediary in question is an economic (as opposed to cultural or political) force; (b) the "voice" of the intermediary's user community is strong;[50] and (c) competition is likely to be genuine and not contrived. These criteria help us map older debates about platforms onto newer entities.

For search engines and carriers, each of these factors strongly militates in favor of regulatory intervention. Broadband competition has failed to materialize beyond duopoly service for most Americans. There are several reasons to suspect that Google's dominance of the general purpose search market will continue to grow.[51] Just as past policymakers recognized the need for common

---

48 Duncan Kennedy, ***The Stakes of Law, or, Hale and Foucault***, 15 LEGAL STUDIES FORUM (4) (1991).

49 BARBARA FRIED, THE PROGRESSIVE ASSAULT ON LAISSEZ FAIRE: ROBERT HALE AND THE FIRST LAW AND ECONOMICS MOVEMENT (1998), available at **http://www.hup.harvard.edu/catalog/FRIPRA.html**.

50 Competition is designed to provide users an "exit" option; regulation is designed to give them more of a "voice" in its governance. Hirschman ALBERT O. HIRSCHMAN, *Exit and Voice: An Expanding Sphere of Influence*, *in* RIVAL VIEWS OF MARKET SOCIETY AND OTHER RECENT ESSAYS 78–80 (1986) (describing "exit" and "voice" as two classic options of reform or protest). To the extent exit is unavailable, voice (influence) within the relevant intermediary becomes less necessary; to the extent voice is available, exit becomes less necessary.

51 Bracha & Pasquale, *Federal Search Commission*, *supra* note 26, at 1179. Section III of the article, "Why Can't Non-Regulatory Alternatives Solve the Problem?," addresses the many factors impeding competition in the search market. Present dominance entrenches future dominance as the leading search engine's expertise on user habits grows to the extent that no competitor can match its understanding of how to target ads well. *Id.* Since that article was published, Harvard Business School Professor Ben Edelman has investigated another self-reinforcing aspect of Google's market power: the non-portability of AdSense data, which

carrier obligations for concentrated communications industries, present ones will need to recognize carriers' and search engines' status as increasingly essential facilities for researchers, advertisers, and media outlets.[52]

The parallel is apt because, to use the three dimensions discussed above, carriers and dominant general-purpose search engines a) are just as important to culture and politics as they are to economic life, b) conceal key aspects of their operations, and are essentially credence goods, vitiating user community influence, and c) do not presently face many strong competitors, and are unlikely to do so in the immediate future. The first point—regarding cultural power—should lead scholars away from merely considering economies of scale and scope and network effects in evaluating search engines. We need to consider all dimensions of network power—the full range of cultural, political, and social obstacles to competition that a dominant standard can generate.[53] Moreover, policymakers must acknowledge that competition itself can drive practices with many negative externalities. The bottom line here is that someone needs to be able to "look under the hood" of culturally significant automated ranking systems.

What about auction platforms, another important online intermediary?[54] Here, a purely economic, antitrust-driven approach to possible problems is more appropriate. To use the criteria mentioned above: (a) a site like eBay is a very important online marketplace, but has little cultural or political impact and (b) the user community at eBay understands its reputation rankings very well, and has shown remarkable capacities for cohesion and self-organization to protest

---

makes it difficult for Google customers to apply what they have learned about their Internet customers to ad campaigns designed for other search engines. Ben Edelman, *PPC Platform Competition and Google's 'May Not Copy' Restriction*, June 27, 2008, **http://www.benedelman.org/news/062708-1.html**. As Edelman shows, Google has tried to make the data it gathers for companies "sticky," inextricable from its own proprietary data structures.

52 TIM WU, THE MASTER SWITCH (Knopf, 2010) (promoting "separations principle" in the digital landscape.).

53 DAVID GREWAL, NETWORK POWER: THE SOCIAL DYNAMICS OF GLOBALIZATION 45 (Yale Univ. Press 2008) ("[T]he network power of English isn't the result of any intrinsic features of English (for example, 'it's easy to learn'): it's purely a result of the number of other people and other networks you can use it to reach… . The idea of network power … explains how the convergence on a set of common global standards is driven by the accretion of individual choices that are free and forced at the same time.").

54 David S. Evans, *Antitrust Issues Raised by the Emerging Global Internet Economy,* 102 NW. U. L. REV. COLLOQUY 285, 291 (2008) ("European Community law and decisional practice … impose special obligations and significant scrutiny on firms that have market shares as low as 40 percent."). Evans compiles data demonstrating that some leading auction platforms (such as eBay) are well above this market share in Europe and the U.S. *Id.* (citing comScore, *MyMetrix qSearch 2.0 Key Measures Report,* Dec. 2007, **http://www.comscore.com/method/method.asp**).

(and occasionally overturn) policies it dislikes. These factors overwhelm the possibility that (c) competition in the general auction market (as opposed to niche auctions) may be unlikely to develop. If real competitors fail to materialize due to illicit monopolization, antitrust judgments against Microsoft (and parallel requirements of some forms of "operating system neutrality") can guide future litigants seeking online auction platform neutrality. While eBay's user community successfully pressured Disney to end its 2000 special-preference deal with eBay, in the future antitrust judgments or settlements might require the full disclosure of (and perhaps put conditions on) such deals.[55]

In social networks, another area where tipping can quickly lead to one or a few players' dominance,[56] the situation is more mixed. While Rebecca Mackinnon and danah boyd have compared Facebook to a utility, the famously market-oriented Economist magazine has compared it to a country, possibly in need of a constitution and formal input from users. Social networks are closer to search engines than auction sites with respect to factor a: they are becoming crucial hubs of social interactions, cultural distribution and promotion, and political organizing.[57]

On the other hand, social networks provide a some leverage to their members to police bad behavior, opening up "voice" options, with respect to factor b, far more potent than those available to the scattered searchers of Google. A group named "Facebook: Stop Invading My Privacy" became very popular within Facebook itself, catalyzing opposition to some proposed features of its Beacon program in 2008.[58] Facebook's privacy snafus in early 2009 led the company to organize formal user community input on future alterations to the company's terms of service. On the final factor, competitive dynamics, it appears that competition is more likely to develop in the social network space than in the broadband, search engine, or auction platform industries. There is a more

---

55 In 2000, eBay granted special perks to Disney on a platform within its auction site. After protest from "the eBay community," the perks ceased. eBay CEO Meg Whitman said of the special Disney deal: "We've concluded that eBay has to be a level playing field. That is a core part of our DNA, and it has to be going forward." ADAM COHEN, THE PERFECT STORE: INSIDE EBAY 292 (Back Bay Books 2006).

56 In early 2008, 98% of Brazilian social networkers used Google's Orkut; 97% of South Korean social networkers used CyWorld, and 83% of American social networkers used MySpace or Facebook. Evans, *supra* note *54* at 292.

57 James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 52-59 (2009), **http://works.bepress.com/james_grimmelmann/20/**.

58 William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 ILL. L. REV. 1105, 1120 (2009), **http://www.law.uiuc.edu/lrev/publications/2000s/2009/2009_4/McGeveran.pdf**.

diverse playing field here than in the carrier or search space, with more than 4,000 social networks in the United States.[59]

Any policy analysis of dominant intermediaries should recognize the sensitive cultural and political issues raised by them. The cultural, communal, and competitive dynamics surrounding dominant search engines and carriers defy easy or stereotyped responses. Qualified transparency will assist policymakers and courts that seek to address the cultural, reputational, and political impact of dominant intermediaries.

## Conclusion

As David Brin predicted in The Transparent Society, further disclosure from corporate entities needs to accompany the scrutiny we all increasingly suffer as individuals.[60] While the FTC and the FCC have articulated principles for protecting privacy, they have not engaged in the monitoring necessary to enforce these guidelines. This essay promotes institutions designed to develop better agency understanding of privacy-eroding practices. Whether public or private, such institutions would respect legitimate needs for business confidentiality while promoting individuals' capacity to understand how their reputations are shaped by dominant intermediaries.

---

59 Evans, *supra* note 54, at 290.

60 DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (Basic Books 1999).

# Online Liability for Payment Systems

By Mark MacCarthy*

## Introduction

U.S. policy toward the liability of Internet intermediaries for online harms was set in the late 1990s. It consisted of two parts. The first part was Section 230 of the 1996 Telecommunications Act, providing a safe harbor from indirect liability for online service providers.[1] This safe harbor is an exception from a range of normal liabilities that would apply to traditional providers of media content such as broadcasters and newspapers. It does not apply to all intermediaries or platform providers, but to what might be called "pure" Internet intermediaries. That is, it covers intermediaries to the extent they are providing services that are somehow intrinsic to the Internet. Under its terms, except for requirements of contract law, criminal law, and intellectual property law, online entities are not responsible for the content of the material that is found on their systems as long as it has been provided by another information content provider.

The second part of the U.S. policy toward Internet intermediary liability was set out in 1998 with the Digital Millennium Copyright Act.[2] DMCA allows a complete exemption from copyright liability for entities involved in pure transmission activities. It also creates a notice-and-takedown regime for web hosts and other online service providers. It also allows recipients of these notices to challenge them. Upon receipt of a response, the online service providers are required to reinstate the allegedly infringing material unless the rights holder has filed a legal infringement action. Online service providers are exempt from liability for good faith removal of material following a notice. It also provides for penalties if a rights holder files a notification that knowingly

---

* Mark MacCarthy is Adjunct Professor in the Communications Culture and Technology Program at Georgetown University. Formerly, he was Senior Vice President for Public Policy at Visa Inc. Substantial portions of this essay were originally published as Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECHNOLOGY LAW JOURNAL 1039 (2010).

1 47 U.S.C. § 230(c)(1) (2006) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."). The interpretation of this provision is quite broad. *See*, *e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 330-31 (4th Cir. 1997) (finding that plaintiff's tort claims of defamation were preempted by § 230). The immunity does not extend to criminal law, contract law, or intellectual property law. 47 U.S.C. § 230(e)(1)-(4) (2006).

2 17 U.S.C. § 512 avaiable at **http://www4.law.cornell.edu/uscode/17/512.html**.

misrepresents that the material is infringing. DMCA also requires online service providers to have in place some procedures to respond to "repeat infringers," including termination of accounts in appropriate circumstances.[3]

Many commentators think that DMCA represents a balanced compromise.[4] However, controversy persists. Content providers have successfully lobbied for laws imposing more robust responsibilities for stopping copyright infringement on Internet service providers (ISPs). France and the United Kingdom, for example, have adopted "graduated response" mechanisms.[5] These liability regimes require ISPs to forward copyright infringement notices to alleged infringers, and to disconnect alleged repeat infringers.

On the other hand, defenders of civil liberties and the First Amendment think DMCA notice-and-takedown requirements are too strong, arguing that a large proportion of the complaints filed under the law are improper,[6] and that they contains an inherent imbalance toward takedown, even when First Amendment values are implicated.[7]

In another essay in this collection, Brian Holland strongly defends Section 230 as a modified version of Internet exceptionalism,[8] and as providing the basis for the development of innovation on the Internet.[9] However, it, too, has been

---

3 17 U.S.C. § 512(i) conditions the eligibility of the safe harbor. It applies only if the service provider "has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." Intermediaries such as Google, YouTube and AT&T appear to have established termination policies for copyright infringement.

4 See, for example, "United States and Canada Overview," in RONALD DEIBERT, JOHN PALFREY, RAFAL ROHOZINSKI, AND JONATHAN ZITTRAIN, ACCESS CONTROLLED 378 ( 2010) and JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 119 (2008).

5 Eric Pfanner, *U.K. Approves Crackdown on Internet Pirates*, NEW YORK TIMES, April 8, 2010 at **http://www.nytimes.com/2010/04/09/technology/09piracy.html?scp=1&sq=digital%20economy%20bill%20uk&st=cse**. Eric Pfanner, *France Approves Wide Crackdown on Net Piracy*, NEW YORK TIMES, Oct. 22, 2009, **http://www.nytimes.com/2009/10/23/technology/23net.html?_r=1**.

6 Jennifer M. Urban & Laura Quilter, *Efficient Process or 'Chilling Effects'? Take-down Notices Under Section 512 of the Digital. Millennium Copyright Act*, 22 SANTA CLARA HIGH TECH LJ 621 (2006).

7 Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, BERKMAN CENTER RESEARCH PUBLICATION NO. 2010-3, p. 16, March 2010, available at **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1577785**.

8 *See* chapter 3, *see also* H. Brian Holland, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 U. KAN. L. REV. 369, 397 (2007).

9 Remarks by Lawrence Strickling, Assistant Secretary of Commerce for Communications and Information, to Internet Society's INET Series: *Internet 2020: The Next Billion Users*, *April 29,*

controversial. Some argue that it allows ISPs to avoid making socially-desirable investments necessary to provide security on their networks.[10] Others think it allows hosting sites to escape their responsibility for defamation and other harms caused by people who use their sites to spread false and damaging information.[11]

Commentary on the controversies involved in these two pillars of the U.S. policy toward online liability is growing.[12] Work on whether to revise the consensus position on intermediary liability is underway.[13]

This essay attempts to contribute to this debate by looking at what payment systems have been doing about online liability. This will provide an illuminating perspective on the debate for a very straightforward reason: Payment systems have operated outside this framework for online liability. They are not covered by Section 230 and they are not subject to the notice-and-takedown provisions of the DMCA. How have they handled issues relating to the use of payment systems for illegal activity online? This essay explores this question through an examination of two cases in which they have been called upon to take steps to control illegal activity involving their payment systems: Internet gambling and copyright infringement.

Some have argued that payment systems should have legal responsibility for keeping their systems free of illegal online activity.[14] Payment systems can keep track of those who use their system online – both merchants and cardholders have contracts with financial. The online transactions using payment systems can be tracked electronically by type. Governments and aggrieved parties might not be able to find wrong-doers who use payment systems for illegal online activity, but the payment system providers can. They are the "least-cost"

---

*2010, available at*
**http://www.ntia.doc.gov/presentations/2010/InternetSociety_04292010.html**.

10 Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 U. CHI. SUP. CT. ECON. REV. 221 (2006).

11 JOHN PALFREY AND URS GASSER, BORN DIGITAL 106 (2008), and DANIEL SOLOVE, THE FUTURE OF REPUTATION 125-160 (2007).

12 See, Adam Thierer, *Dialogue: The Future of Online Obscenity and Social Networks*, ARS TECHNICA, March 5, 2009, **http://arstechnica.com/tech-policy/news/2009/03/a-friendly-exchange-about-the-future-of-online-liability.ars**.

13 See, for instance, Organization for Economic Cooperation and Development, *The Economic and Social Role of Internet Intermediaries*, April 2010, **http://www.oecd.org/dataoecd/49/4/44949023.pdf**.

14 Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 249-50 (2005), available at **http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1225&context=wmlr**.

avoider of the damage done by this illegal online activity and so should bear the burden of controlling it.

This perspective seems wrong to me. Still, payment system practices toward illegal online activity on their systems suggest several lessons. First, regardless of the precise legal liabilities, intermediaries have a general responsibility to keep their systems free of illegal transactions and they are taking steps to satisfy that obligation. Second, the decision to impose legal responsibilities on intermediaries should not be based on the least cost avoider principle. Assessments of intermediary liability must take into account market failures, as well as an analysis of costs, benefits and equities. Third, if intermediaries are shouldered with responsibilities to control illegal online activity, these responsibilities needed to be clearly spelled out. Fourth, if governments are going to use intermediaries to enforce local laws, they must harmonize these local laws.

Part II of this essay outlines a framework for the analysis of intermediary liability. This framework calls for a thorough analysis, including an assessment of market failure and an analysis of the costs, benefits, and equities involved in imposing intermediary liability. Part III applies this framework to the policies and practices of payment intermediaries in the areas of Internet gambling and online copyright infringement. Part IV draws some conclusions from these experiences.

## Indirect Intermediary Liability Regimes

Most legal regimes hold parties liable for their own misconduct. In contrast, an indirect liability regime holds a person responsible for the wrongs committed by another. There are usually several parties involved in an indirect liability regime: the bad actor, the wronged party and a third party. The bad actor is the person directly involved in causing the harm to the wronged party. A third party, neither the bad actor nor the wronged party, is assigned responsibility in an attempt to prevent the harmful conduct of the bad actor or to compensate the wronged party for the harm. In the case of copyright infringement, for example, the bad actor would be the infringer, the wronged party would be the record company that owned the music copyrights, and the third party would be an ISP or a payment system that facilitates the infringement. Indirect liability can be imposed through a variety of legal mechanisms.[15]

---

15 *See, e.g.*, Douglas Lichtman, *Holding Internet Service Providers Accountable*, 27 REG. 54, 59 (2004) (proposing that ISP liability for cyber security issues could be established in a regime of "negligence or strict liability, whether it is best implemented by statute or via gradual common law development"); Mann & Belzley, *supra* note 14, at 269-72 (suggesting three possible regimes: traditional tort regime, a takedown requirement, and a hot list).

## A Framework for Analysis

Indirect liability holds a party responsible for wrongs committed by another person. Why should there be any such rule? Why not simply hold the bad actor responsible? The economic analysis of indirect liability attempts to answer this question using some standard economic tools and concepts.[16] A standard economic framework considers issues of market failure, costs and benefits, and equity to assess the need for an indirect liability regime in specific cases.[17]

### Market Failure Analysis

Before imposing an indirect liability regime, economic analysis asks whether there is really any market failure. If there is no market failure, there is no need for an indirect liability rule. In particular, there need not be an indirect liability rule when the law or the wronged party can effectively reach the bad actor directly[18] and transaction costs are not significant.

Even if the wronged party cannot easily reach a bad actor that a third party can reach, it is still not necessary to impose liability on the third party. When the wronged party and the intermediary can easily negotiate an arrangement, efficiency will guide the third party to undertake enforcement efforts on behalf of the wronged party. This is a key aspect of a market failure analysis. Unless transaction costs interfere with contracting, affected parties can allocate liability efficiently through contractual design.[19]

---

16 *See generally* Lichtman & Posner, *supra* note 10 (summarizing this perspective); Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395, 396-99 (2003).

17 *See* Lichtman & Posner, *supra* note 10, at 228-33.

18 The effective reach condition is evaluated prior to an assessment of the ability of a third party to effectively control the bad activity. *See id.* at 230-31. If the law or the wronged party can easily reach the bad actor, then why even consider whether to impose a duty on a third party? Of course, the bad actors are never totally out of reach of the law or wronged parties. With some finite expenditure of resources, perhaps very large, the direct bad actors could be brought to justice or harms could be prevented. The real economic question is whether those costs are larger than the costs of assigning that enforcement role to a third party. And this means that the effective reach condition collapses into the control factor discussed, infra. Landes and Lichtman put the comparative point accurately, applied to the specific case of contributory copyright liability: "Holding all else equal, contributory liability is more attractive … the greater the extent to which indirect liability reduces the costs of copyright enforcement as—compared to a system that allows only direct liability." Lichtman & Landes, *supra* note 16, at 398.

19 Lichtman & Posner, *supra* note 10, at 235. Lichtman and Posner also focus on what the parties might do: "The right thought experiment is to imagine that all the relevant entities and all the victims and all the bad actors can efficiently contract one to another and then to ask how the parties would in that situation allocate responsibility for detecting and deterring bad acts." *Id.* at 257. But there is no need to conduct this thought experiment in the abstract. Free, equal, and rational parties can bargain to allocate responsibility and so we can answer

## Cost Benefit Analysis

Some arguments for indirect liability follow a least cost analysis. A "least cost" perspective puts the burden of enforcing the law on the party that can stop the illegal transactions at the lowest cost. Focusing on costs is desirable in order to create an efficient enforcement regime. In a "least cost" framework, the cost to the intermediary itself and to the direct customers of the intermediary must be taken into account. If ISPs or payment systems have to incur costs to monitor their system for illegal content, those costs will be passed down to their direct customers. With the price increase, some customers stop using the service or reduce their usage of it. If the service provided is a network service, then the external network effects on other users of the service from an overall reduction in use also have to be counted.[20]According to the least cost idea, when these costs are less than the cost of enforcement activity by the wronged party or by enforcement officials, then liability rests with the intermediary.

This least-cost analysis is limited. It ignores the size of the harms that can be avoided by intermediary action. The mistake is to think that if efforts by third parties provide more enforcement than efforts by the wronged parties then it must be worthwhile for the third parties to take these enforcement steps. Similarly, it is sometimes thought that if third parties can more easily reach bad actors than the wronged parties, then they should be required to do so. But this is wrong. It is almost always possible to spend more on enforcement and obtain some return. From an economic point of view, the question is whether that extra spending provides commensurate reductions in damages. Therefore, the least cost rule is not the right decision rule, even in a strictly economic analysis. Instead, a full cost-benefit analysis is more appropriate.[21]

---

the question of what the parties would do in this thought experiment by looking at what they actually do. The relevant inquiry is whether the bargaining situation is free of significant transaction costs or other obstacles to reaching an agreement.

20 If there are fewer Internet subscribers then the service is less valuable to e-commerce merchants as well since there are fewer potential customers. *See* Matthew Schruers, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 250-52 (2002); *see also* Lichtman & Posner, *supra* note 10, at 241-43 (seeming to minimize the importance of these external, network effects in assessing liability regimes: "Immunizing ISPs from liability is not the correct mechanism for encouraging them to provide positive externalities." *Id.* at 243). However, the loss of the ISP-generated external benefits is a potential cost of assigning liability that has to be taken into account when assessing whether to assign liability. Mann and Belzley's article gets the overall point right, noting: "To the extent the regulation affects conduct with positive social value, as is likely in at least some of the contexts this essay discusses, the direct and indirect effects on that conduct must be counted as costs of any regulatory initiative." Mann & Belzley, *supra* note 14, at 274.

21 The least-cost analysis seems to function like a cost effectiveness analysis, where a given level of enforcement is assumed and the question is how that goal can be reached at the lowest cost. *See* Mann & Belzley, *supra* note 14, at 250 (adopting that perspective as "a mature scheme of regulation that limits the social costs of illegal Internet conduct in the

There is a difference between the costs and benefits to private parties involved and the costs and benefits to society. The costs and benefits of third party enforcement efforts fall on different parties. A wronged party benefits from third party enforcement efforts and the third party pays the costs. The wronged party has a natural incentive to have the third party do as much as possible in the way of enforcement—even past the point where there is a corresponding reduction in damages—because the wronged party appropriates the damage reduction but pays no costs. From an economic efficiency point of view, enforcement efforts that do not yield a commensurate reduction in damages are wasted. Private benefits may not be worth it from a social point of view when balanced against the costs to other parties.

## Equity Analysis

The cost benefit framework just described lacks a normative dimension. It does not take into account questions of fairness, rights, and justice. And it does not consider who deserves the benefit of protection from harm or who is at fault or blameworthy for failing to take preventive measures.

The view that an economic efficiency standard, by itself, is sufficient to create indirect liability is too strong. The focus on parties who had no part in creating the problem and who are not responsible for the illegal activity puts a burden on people who are innocent of any wrong-doing. Burdening innocent people seems unfair, and arguments that justify this approach on grounds that it is good for society as a whole violate widely accepted moral principles and are unlikely to withstand public scrutiny.[22]

We should require a person to right the wrongs committed by others only if we think that person is somehow responsible for those wrongs. Determining who is responsible for righting wrongs committed by others is controversial in both moral and political philosophy.[23] Libertarians generally maintain that people need to fix only the problems that they themselves directly created.[24] Without

---

most cost-effective manner"). But a full cost-benefit analysis gives up the assumption of a fixed benefit goal and takes the value of benefits into account as well.

22 *See, e.g.*, JONATHAN WOLFF, AN INTRODUCTION TO POLITICAL PHILOSOPHY 57 (1996) (stating that "utilitarianism will permit enormous injustice in the pursuit of the general happiness"). A more sophisticated indirect or rule utilitarian approach can attempt to meet this difficulty, but that approach is subject to difficulties of its own. *See generally* JOHN RAWLS, A THEORY OF JUSTICE (1971) (critiquing utilitarianism). The underlying intuition behind this alternative account of social justice is that "[e]ach person possesses an inviolability founded on justice that even the welfare of society as a whole cannot override." *Id.* at 3

23 *See infra* notes 24-27 and accompanying text.

24 *See* Jim Harper, *Against ISP Liability*, 28 REG. 30, 30-31 (2005) (arguing that ISPs should be liable for harms to third parties only if they have a duty to these parties and that "efficiency" considerations do not override the lack of such a duty founded on justice). Libertarians

this limitation, it is hard not to slide into a doctrine that requires all actors to stop misconduct whenever they can.[25] Others think that one has a duty to correct injustices to the extent that one participates in an institutional framework which produces injustice.[26] Still others believe in general positive duties to eliminate harms even when one has no direct role in causing them.[27]

Ultimately, the analysis of indirect liability cannot avoid considerations of fairness, rights, and justice. The key factors in this assessment will be those that have been used traditionally: directness of the involvement by third parties in activities that lead to harm to another person, an assessment of the degree of harm involved, the knowledge that third parties have or should have about the specific harm involved, what their intentions are, whether they are consciously acting in furtherance of a crime or other illegal act, and other similar considerations.[28] These complicated normative and empirical questions cannot be avoided by a single principle that purports to look at costs and benefits alone. [29]

---

generally reject the idea that we have positive duties to ameliorate harms we did not cause. *E.g.*, *id.*

25 Mann & Belzley, *supra* note 14, at 272 (noting that the principle that liability should be assigned regardless of blameworthiness "easily could shade into judicial doctrines that would obligate all actors to stop all misconduct whenever possible" and thinking that this "unbounded principle" is "unduly disruptive"). But it is hard to see how their proposal to implement indirect liability through regulation whenever it would be less expensive than leaving liability with the wronged party would be less disruptive.

26 *See, e.g.*, THOMAS W. POGGE, WORLD POVERTY AND HUMAN RIGHTS 172 (2002) (arguing that those involved in an institutional order that authorizes and upholds slavery have a duty to protect slaves or to promote institutional reform, even if they do not own slaves themselves).

27 *See, e.g.*, David Luban, *Just War and Human Rights*, *in* INTERNATIONAL ETHICS 195, 209 (Charles R. Beitz et al. eds., 1985) (stating that "all humans in a position to effect" a human right have an obligation to do so).

28 Mann and Belzley criticize the "myopic focus on the idea that the inherent passivity of Internet intermediaries makes it normatively inappropriate to impose responsibility on them for the conduct of primary malfeasors." Mann & Belzley, *supra* note 14, at 261-62. But passivity is relevant to the knowledge and control factors needed to assess liability from an equity point of view. Lichtman and Landes seem to criticize the focus of current law on "knowledge, control, the extent of any non-infringing uses, and other factors" because they are not "particularly clear as to why those issues are central." Lichtman & Landes, *supra* note 16, at 405. But these factors are crucial because they relate to the way in which the equity issues can be resolved.

29 These equity considerations can interact with the cost analysis. Consider the following: suppose transaction costs make it impossible for the wronged parties to negotiate enforcement deals with a third party–they are too numerous or lack the resources to compensate the third party. Suppose further it is possible that the cost savings involved in assigning liability to a third party are substantial. And finally stipulate that the third party's involvement in the harm is so remote that assigning blame is a mistake. We might in that

An economic framework, broadly construed and supplemented with suitable considerations of equity, can be a useful way to assess the need for indirect liability for intermediaries in specific cases. The elements of the framework are as follows:

- **Market Failure Analysis**: Are there substantial transaction costs? Can enforcement be achieved without an indirect liability rule? Can private parties work out enforcement arrangements among themselves? Can third parties effectively work with law enforcement without an indirect liability mandate?
- **Cost-Benefit Analysis**: Does the burden on the wronged party or on law enforcement to take enforcement steps exceed the burden on the third parties? Are the costs of enforcement efforts reasonable in light of the reduction in harm? Are there longer-term or dynamic considerations to take into account?
- **Equity Analysis**: Do third parties exercise such close control over the harm that they should be held responsible for its mitigation or elimination? Are they blameworthy for not taking steps against it? Is the harm particularly egregious?

## Applying the Framework to Payment Intermediaries

Payment intermediaries have developed and refined policies and practices to deal with illegal Internet transactions in their payment networks. Two general conclusions can be drawn from an analysis of these policies and practices.

The first is that payment intermediary action has been effective. As the following discussions demonstrate, Internet gambling websites have been denied access to the U.S. market, and their current and projected revenues are in decline. As a result of the payment system action in the *Allofmp3.com* copyright infringement case, Allofmp3.com was confined to a domestic market and experienced a dramatic reduction in the volume of activity at its website.

The second conclusion is that the widespread assumption that payment system action in this area is simple and almost cost-free deserves more careful consideration.[30] The discussion of payment intermediaries' activities to control

---

circumstance nevertheless assign liability to the third party. The gains to the rest of us are just too great. However, should we not compensate the third party for taking the enforcement steps he is required to take? Assigning indirect liability when there is not this level of control or fault to justify blameworthiness might be so efficient under a cost analysis that it is worth considering, but in that case the use of compensation mechanisms should also be considered.

30 *See, e.g.*, *Perfect 10*, 494 F.3d at 824 (Kozinski, J., dissenting).

illegal activity on their systems reveals substantial costs that should give policy makers pause before moving ahead with the imposition of an indirect liability scheme for payment providers. These include:

- The cost to maintain and enforce an Internet gambling coding and blocking scheme that is entirely manual and cannot be automated;
- The cost from over-blocking legal transactions;
- The cost to screen and check the business activity of merchants participating in the payment systems;
- The cost to monitor the use of payment systems for specific illegal activity, where the payment systems are in no better position than anyone else to conduct this monitoring activity;
- The cost to assess complaints of illegality, where the intermediary has no special expertise and is often less familiar with the legal and factual issues than the wronged party and the allegedly bad actor;
- The cost to defend against legal challenges to enforcement actions, where the challenge typically comes in an off-shore jurisdiction; and
- Longer-term costs to the United States from taking unilateral action in this area, including the encouragement of copycat regimes in other areas of law and in other jurisdictions.

The reasonableness of these costs in light of the benefits achieved has not yet been seriously studied. Instead, it seems to be assumed that small compliance costs are justified by large enforcement benefits. Although precision in the estimates of costs and benefits is unlikely in this area, a more disciplined qualitative analysis is required.

## Internet Gambling Legislation

The development of the Internet as a commercial medium presented a challenge to local gambling laws. With access to the Internet, individuals could reach gambling services from their homes, without the need to travel to a gambling merchant's physical operation. The Internet provided a way for gambling merchants who were legal in their own jurisdictions to provide service to customers in different jurisdictions where gambling was not allowed.

The United States Congress began its consideration of how to react to illegal Internet gambling in the late 1990s.[31] One early proposal was to put an

---

31 *See* General Accounting Office, *Internet Gambling, An Overview of the Issues*, Dec. 2002, **http://www.gao.gov/new.items/d0389.pdf**. Many state laws made Internet gambling illegal and Federal law also appeared to outlaw at least some forms of it in interstate commerce. But the legal situation was ambiguous with respect to some forms of Internet gambling. The Interstate Wire Act of 1961 applied to Internet gambling and appeared to prohibit the use of the Internet for the "placing of bets or wages on any sporting event or contest." *See* The Interstate Wire Act (18 U.S.C. § 1084) at

enforcement burden on ISPs. It would have required ISPs to terminate domestic Internet gambling merchants and to block foreign Internet gambling merchants upon request of law enforcement.[32] This initial effort failed to pass, in part because of concerns about the effectiveness and appropriateness of putting an enforcement burden on ISPs.[33]

In 2006, Congress passed the Unlawful Internet Gambling Enforcement Act (UIGEA), which imposed a system of indirect liability on financial institutions for the purpose of preventing illegal Internet gambling transactions.[34] Prior to the passage of UIGEA, payment card networks devised a coding and blocking system in order to manage the risks of Internet gambling.[35] Each merchant in the payment system is normally required to identify its major line of business and to include a four digit "merchant category code" in each authorization message.[36] For gambling, this merchant category code was 7995.[37] In addition, merchants were required to use an electronic commerce indicator when an Internet transaction was involved.[38] Together, these two pieces of information

---

**http://www.law.cornell.edu/uscode/18/usc_sec_18_00001084----000-.html**. The U.S. Fifth Circuit Court of Appeals ruled in 2002 that the Wire Act applied only to sports betting and not to other types of online gambling. See In re MasterCard, 313 F.3d 257 (5th Cir. 2002). The status of horseracing was similarly unclear. The Interstate Horse Racing Act appeared to allow the electronic transmission of interstate bets. It was amended in December 2000 to explicitly include wagers through the telephone or other electronic media. See the Interstate Horse Racing Act (15 U.S.C. §§ 3001-3007) at **http://www.law.cornell.edu/uscode/15/usc_sup_01_15_10_57.html**. These statutes appeared to allow the Internet to be used for both non-sports gambling and for gambling on horse races. The U.S. Department of Justice, however, thought, and still thinks, that existing statutes bar all forms of Internet gambling. *See* Letter from William E. Moschella, Assistant Attorney General to Rep. John Conyers Jr., July 14, 2003 at **http://www.igamingnews.com/articles/files/DOJ_letter-031714.pdf** ("The Department of Justice believes that current federal law, including 18 U.S.C. §§ 1084, 1952, and 1955, prohibits all types of gambling over the Internet.").

32 H.R. 3125 at **http://thomas.loc.gov/cgi-bin/query/D?c106:2:./temp/~c106mktqmw**

33 *See* the floor debate on H.R. 3125, CR H6057-6068, July 17, 2000, **http://thomas.loc.gov/cgi-bin/query/R?r106:FLD001:H56058**.

34 Unlawful Internet Gambling Enforcement Act of 2006, Pub. L. No. 109–347, 120 Stat. 1884 (codified at 31 U.S.C. §§ 5361–5367 (2006)).

35 Financial Aspects of Internet Gaming: Good Gamble or Bad Bet?: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Financial Servs., 107th Cong. 25-27, 34-35 (2001) [*hereinafter* Financial Aspects of Internet Gaming Hearing] (statement and testimony of Mark MacCarthy, Senior Vice President, Public Policy, Visa, U.S.A., Inc.) (describing this system of coding and blocking Internet gambling transactions); U.S. GEN. ACCOUNTING OFFICE, supra note 31, at 20-25.

36 U.S. GEN. ACCOUNTING OFFICE, *supra* note 31, at 22.

37 VISA MERCHANT CATEGORY CLASSIFICATION (MCC) CODES DIRECTORY, *available at* **http://www.da.usda.gov/procurement/card/card_x/mcc.pdf**.

38 U.S. GEN. ACCOUNTING OFFICE, *supra* note 31, at 22.

in the authorization message allowed payment networks or issuing banks to identify transactions involving Internet gambling merchants.[39]

Given this system, it was entirely feasible for the issuing bank or the payment network to block Internet gambling transactions. The system could accommodate conflicting laws in different jurisdictions in the following way: If it was illegal in one country, such as the United States, for cardholders to engage in Internet gambling, then the issuing banks based in that country could decline authorization requests for all properly coded Internet gambling transactions. This would effectively block these transactions. However, the banks in other countries who permit Internet gambling, such as the United Kingdom, could allow the use of their cards for Internet gambling by not declining properly coded Internet gambling transactions.

The system was limited in detecting nuances in illegal versus legal Internet gambling. If a jurisdiction recognized some Internet gambling transactions as legal and others as illegal, the system would not detect it.[40] The merchant category code described a type of business, not the legal status of the transaction involved.[41] If a particular jurisdiction allowed casino gambling, but not sports betting, both transactions would nevertheless be labeled 7995. And if the system was set up to block these coded transactions, then both transactions, legal and illegal, would be blocked.[42]

Another weakness in the system was enforcement. If an Internet gambling merchant realized that his transactions would be blocked in a large jurisdiction such as the United States, then he would have every incentive to hide.[43] Instead of describing itself as a gambling merchant, it would just code itself as a T-shirt sales site or some other legal merchant. Without the proper merchant category code, the system was blind and could not effectively block the merchant's transactions.[44]

The payment networks addressed this enforcement issue with a special program to verify that Internet gambling merchants coded their transactions correctly.[45]

---

39 *Id.*

40 U.S. GEN. ACCOUNTING OFFICE, *supra* note 31, at 22.

41 *See* VISA MERCHANT CATEGORY CLASSIFICATION (MCC) CODES DIRECTORY, *supra* note 37 (listing all the MCC codes by "merchant type").

42 U.S. GEN. ACCOUNTING OFFICE, *supra* note 31, at 22.

43 *Id.* at 26.

44 *Id.*

45 *Id.* at 31-32. The fines for incorrectly identifying authorization requests for online gambling transactions are set out at page 557 of the Visa International Operating Regulations. VISA, VISA INTERNATIONAL OPERATING REGULATIONS (April 2010),

Payment network personnel would test transactions at popular Internet gambling sites. They would enter a transaction at the web site and track the transaction through the payment system. They would be able to tell whether the transaction was coded properly or not after they identified the transaction in the system. If the transaction was not properly coded, the network would contact the bank that worked with the merchant and tell the bank that its merchant was out of compliance with the coding rule. The payment network would ask the bank to take steps to bring the merchant into compliance. Finally, the network would retest the site for proper coding. [46]

The UIGEA required payment systems to have policies and procedures reasonably designed to stop illegal Internet gambling transactions.[47] The statute creates a safe harbor for payment systems that adopt a coding and blocking scheme.[48] The Federal Reserve Board and the Department of the Treasury implemented this safe harbor with a non-exclusive description of one way in which a payment system can demonstrate that its policies and practices are reasonably designed to stop illegal Internet gambling transactions.[49] This non-exclusive description tracked the existing industry practices.

---

**http://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf#557**. In addition, Visa requires online gambling merchants to post certain notices: "a Website for an Online Gambling Merchant must contain … [t]he statement ' Internet Gambling may be illegal in the jurisdiction in which you are located; if so, you are not authorized to use your payment card to complete this transaction.'" *Id.* at 594.

46 U.S GEN. ACCOUNTING OFFICE, *supra* note 31, at 32.

47 Unlawful Internet Gambling Enforcement Act of 2006, Pub. L. No. 109–347, 120 Stat. 1884 (codified at 31 U.S.C. §§ 5361–5367 (2006)).

48 12 C.F.R. § 233.6(d)(1)(ii) (2009).

49 The code's relevant section reads:

> (ii) Implementation of a code system, such as transaction codes and merchant/business category codes, that are required to accompany the authorization request for a transaction, including—
>
> (A) The operational functionality to enable the card system operator or the card issuer to reasonably identify and deny authorization for a transaction that the coding procedure indicates may be a restricted transaction; and
>
> (B) Procedures for ongoing monitoring or testing by the card system operator to detect potential restricted transactions, including—
>
> (*1*) Conducting testing to ascertain whether transaction authorization requests are coded correctly; and
>
> (*2*) Monitoring and analyzing payment patterns to detect suspicious payment volumes from a merchant customer … .

*Id.*

## Implementation Challenges with the Internet Gambling Act

UIGEA defines illegal Internet gambling as whatever is illegal under current U.S. state and Federal law. It therefore continues the uncertainty regarding the illegality of some Internet gambling activities.[50] Financial intermediaries have the discretion to block or not block these transactions based upon their own judgment and the strength of the legal arguments presented to them. UIGEA also provides them with protection from liability if they over-block Internet gambling sites that turn out to be legal. The current law thereby allows substantial over-blocking and puts substantial discretion in the hands of the payment companies.

### Impact of UIGEA

A large percentage of non-U.S. companies that derived extensive revenues from their operations in the United States left the market after the passage of UIGEA. All European companies that had been active in the U.S. market left it after the passage of UIGEA.[51] By December 2008, all the publicly-trade online gambling firms had left the U.S. market, even though most of the private firms remained.[52]

Three major European online gambling merchants lost $3 billion in 2006 from this withdrawal from the U.S market.[53] Measured traffic at particular sites declined as well. In September 2006, Party Poker, for example, which derived much of its traffic from the United States, had an average of about 12,000 active players. By November 2006, that number had dropped to about 4,000.[54]

---

50 These uncertainties affect several types of gambling, including horse racing, state lotteries, Indian gaming, and games of skill.

51 European Commission Directorate-General for Trade, *Examination Procedure Concerning an Obstacle to Trade, Within the Meaning of Council Regulation (EC) No 3286/94, Consisting of Measures Adopted by the United States of America Affecting Trade in Remote Gambling Services Complaint, Report to the Trade Barriers Regulation Committee (Commission Staff Working Paper)* 59, June 10, 2009, available at **http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143405.pdf** [hereinafter EC Gambling Report].

52 Casino City, *Online Gambling in the United States Jurisdiction*, 2009, **http://online.casinocity.com/jurisdictions/united-states/**.

53 *See EC Gambling Report*, supra note 51, at 79 ("the direct losses in revenue due to the loss of the US market for just these three companies were above $3 billion in 2006.").

54 *See* WhichPoker.com, *UIEGA Effects*, **http://www.whichpoker.com/stats/UIGEAEffects** (last accessed Oct. 18, 2010). WhichPoker attributes the departure of the biggest publicly-traded online poker sites from the US market to stock market rules.

Shortly after UIGEA was signed into law in October 2006 analysts estimated that the value of British Internet gambling stocks declined by $7.6 billion.[55] In the 9 months between January 1, 2006 and November 1, 2006, just after the passage of UIGEA, three major European online gambling firms lost an estimated 75% of their value, totaling approximately 8.3 billion euros.[56]

An estimate by the European Commission of the likely evolution of the U.S. market in the absence of the specific restrictions imposed in 2006, based on an assumption of a 3% yearly growth, show U.S. Internet gambling accounting for about $5.8 billion per year in gross revenue in 2006, and reaching almost $14.5 billion in 2012. Following the passage of UIGEA, the annual figure declined to about $4.0 billion in 2006, and by 2012 was estimated to be at only $4.6 billion.[57] UIGEA reduced thus the size of the U.S. market well below what it would otherwise have been.

## Internet Gambling Assessment

On equity grounds, it seems that the payment system connection to Internet gambling is too passive to justify imposing legal responsibility for blocking illegal Internet gambling. Payment intermediaries are not to blame when others use their system for Internet gambling because these intermediaries have no specific connection to the activity other than operating a general purpose payment system. They do not reap extra profits through special arrangements with the Internet gambling merchants. Internet gambling transactions are no different from any other payment card transaction. On pure equity grounds alone, then, there is no reason to single out these transactions and impose special legal responsibilities.

A market analysis indicates that there are still some feasible enforcement arrangements that were not established prior to the passage of the UIGEA. Although intermediaries may not be responsible for their customers' gambling, many of them are concerned about the social ills connected with the activity and want to reduce its prevalence.[58] U.S. financial intermediaries had already refused to sign up domestic Internet merchants because these merchants were not

---

55 Eric Pfanner and Heather Timmons, *U.K. Seeks Global Rules for Online Gambling*, INTERNATIONAL HERALD TRIBUNE, Nov. 2, 2006, at 14, available at **http://www.nytimes.com/iht/2006/11/02/technology/IHT-02gamble.html**. The basis for this decline in share value was the withdrawal of these firms from the lucrative US market and the perception that they would not be able to recover the revenue lost from non-U.S. customers.

56 EC *Gambling Report*, supra note 51, at 83.

57 *Id.* at 19.

58 *See Financial Aspects of Internet Gaming Hearing, supra* note 39, at 25-26 (statement of Mark MacCarthy, Senior Vice President, Public Policy, Visa U.S.A., Inc.).

authorized to act legally in the United States.[59] Some state attorneys general requested the intermediaries to block offshore gambling activities, and many cooperated.[60] These agreements did not extend to all financial institutions and did not cover all states, but they could have been extended without imposing a legislative requirement.

A cost-benefit analysis of the UIGEA starts with an estimate of its effect on the amount of illegal Internet gambling activity. As we have seen, the legislation did not eliminate Internet gambling in the United States, but it did reduce it substantially below what it would otherwise have been.

The costs associated with the payment systems' compliance with the legislation include the costs of maintaining and enforcing an Internet gambling coding and blocking scheme, which is entirely manual and cannot be automated, as noted above.

Another cost is the over-blocking problem created by the way in which payment intermediaries comply with UIGEA. Perfectly legal transactions will likely be blocked because payment intermediaries cannot distinguish them from illegal transactions. This example illustrates that intermediaries are usually better than others at monitoring their own systems for business activity of a certain type, but not at detecting the illegality of activity on their systems.[61] The point arises in Internet gambling because the codes used by financial institutions reflect the business activity of gambling, not its status as legal or illegal. As a result, the payment systems' policies and procedures, which were adopted to comply with the Act and which have been accepted by the implementing regulations, over-block and prevent perfectly legal activity from taking place.[62]

---

59 *Id.* at 26; U.S. GEN. ACCOUNTING OFFICE, *supra* note 31, at 20.

60 *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 82 (2006) (discussing Spitzer's efforts "to convince every major American credit card provider and online payment system to stop honoring web gambling transactions.").

61 *See* Mann & Belzley, *supra* note 14, at 278 ("Surely eBay is more adept at searching and monitoring its marketplace than Tiffany & Co., while eBay probably is not as effective as Tiffany & Co. in distinguishing bona fide Tiffany products from counterfeits."); *see also* Schruers, *supra* note 20, at 252 ("[T]he ISP is not the least-cost avoider when it comes to discovering [illegal] content; it is only well suited for cost avoidance after it is apprized of the problem."). Schruers adds that in this case, the wronged party may be better suited to the task of locating the offending content. *Id.* at 252.

62 Mann & Belzley, *supra* note 14, at 294. Mann and Belzley have a useful discussion of this over-blocking issue:

> [A] risk always exists that imposing additional burdens on intermediaries will chill the provision of valuable goods and services. That will be especially problematic in cases where considerable risk of chilling legal conduct that is

### Alternatives to UIGEA

In light of this difficulty, there might be more effective ways of assigning liability. The new law creates unnecessary confusion by failing to define the term "unlawful Internet gambling." Congressman Barney Frank has introduced legislation to license and regulate Internet gambling merchants.[63] The lack of clarity about which merchants are legal would be resolved through a licensing process. At best, the system would rely on a list of approved gambling entities that the payment networks could check before approving gambling transactions from particular Internet merchants.[64]

The new licensing regime proposed in Congressman Frank's legislation would be an improvement over the existing system in the short term. But over time, the only way payment systems can operate is through a reduction in the diversity of the laws they must accommodate. The U.S. government must either find other ways to enforce its laws abroad or begin harmonizing its laws with those of other countries. One solution is an international agreement that would recognize licensing arrangements in different countries as long as they satisfied certain agreed-upon minimum standards.

---

> adjacent to the targeted conduct exists. As discussed below, that might tend to make the use of intermediaries less plausible in file-sharing contexts where determining whether any particular act of file-sharing is illegal is difficult, and much more plausible in the gambling context where in many cases substantially all traffic to a particular site likely involves illegal conduct. Requiring intermediaries to make those kind [sic] of subjective decisions imposes costs not only on the intermediaries (that must make those decisions), but also on the underlying actors whose conduct might be filtered incorrectly.

*Id.* at 274. The Internet gambling case illustrates that determining when a website is engaged in illegal gambling is not a simple task. It is fraught with the kind of "subjective decisions" that Mann and Belzley are properly concerned about. Payment systems faced with this difficulty do not to make these subjective decisions, instead blocking *all* gambling activity, including legal gambling transactions.

63 Internet Gambling Regulation, Consumer Protection, and Enforcement Act, H.R. 2267, 111th Cong. (2009).

64 See text of H.R. 2267 and discussion at **http://financialservices.house.gov/press/PRArticle.aspx?NewsID=495**. The House Financial Services Committee approved the measure on July 29, 2010. See Sewell Chan, *Congress Rethinks its Ban on Internet Gambling*, NEW YORK TIMES, July 29, 2010 available at **http://www.nytimes.com/2010/07/29/us/politics/29gamble.html**. The revised legislation contains a ban on the use of credit cards for any Internet gambling, even the newly-legalized merchants, but debit cards can be used at the licensed sites. The text of the revised legislation is available at **http://financialservices.house.gov/Media/file/markups/7_28_2010/Amendments--HR%202267/Frank12.pdf**

## Online Copyright Infringement

The ideal copyright enforcement mechanism would be for content owners to sue direct infringers. But often, direct infringers are too ubiquitous, too small, and too difficult to find. The result is well-developed notions of secondary liability for copyright infringement that involve intermediaries—as Paul Szynol dicusses in another essay in this collection. These doctrines of secondary liability have evolved substantially over the past decades.

### Legal Context for Intermediary Liability in Copyright Infringement

Court cases and federal statute define some indirect responsibilities of intermediaries regarding copyright. The 1984 Supreme Court decision in *Sony Corp. of America v. Universal City Studios, Inc.*[65] established a standard for assessing third party liability. Providers of a technology that can be used for infringing activities are not liable when there are "substantial non-infringing uses" of the technology.[66] The Digital Millennium Copyright Act of 1998 enabled copyright owners to enforce their existing rights in the Internet context by enlisting the help of Internet intermediaries.[67] The key mechanism for gaining the cooperation of intermediaries is a safe harbor from secondary liability. ISPs are given an exemption from secondary liability so long as they act as a pure conduit, providing only transitory communications and system caching.[68] Web hosts and search engines also receive a safe harbor, provided they comply with a specific notice-and-takedown procedure.[69] Upon receiving notification of claimed infringement, the provider must expeditiously take down or block access to the material.[70]

Successful litigation against peer-to-peer networks in the digital music area also increased the ability of copyright owners to use third parties to combat copyright infringement where the third party is affirmatively involved in fostering the infringement. In an early file-sharing case, the Ninth Circuit found that the peer-to-peer service Napster was liable for secondary infringement based on its control and facilitation of its users' infringement of music copyrights;[71] The company subsequently went out of business in its original

---

65 464 U.S. 417 (1984).

66 *Id.* at 442.

67 17 U.S.C. § 512 (2006).

68 17 U.S.C. § 512(a).

69 17 U.S.C. § 512(b).

70 *Id.*

71 A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

form.[72] More recently, the Supreme Court found that another peer-to-peer service, Grokster, violated federal copyright law when it took "affirmative steps taken to foster infringement … by third parties," such as advertising an infringing use or instructing how to engage in an infringing use.[73]

Against this background arose a question regarding payment systems: Are they liable for secondary infringement when they are used for direct infringement? In *Perfect 10 v. Visa International Service Ass'n*,[74] a subscription-based adult content website alleged that numerous websites based in several countries had stolen its proprietary images, altered them, and illegally offered them for sale online.[75] In response to complaints, Visa did not deny payment services to the allegedly infringing sites, and Perfect 10 brought a contributory and vicarious infringement action against Visa. The Ninth Circuit affirmed the district court's rejection of liability for Visa.[76]

In *Perfect 10*, the Ninth Circuit dismissed the charge of contributory infringement by focusing on whether the credit card companies "materially contributed" to the infringement.[77] The court said the credit card companies did not materially contribute to the infringement because they had no "direct connection" to the infringement.[78] To have direct connection to the infringement they would have had to reproduce, display, or distribute the allegedly infringing works, which they did not do.[79] Payment services might make it more profitable to infringe, but they are too far removed in the causal

---

72 Benny Evangelista, *Napster Runs Out of Lives – Judge Rules Against Sale*, S.F. CHRONICLE, Sept. 4, 2002, at B1.

73 MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 919 (2005).

74 494 F.3d 788 (9th Cir. 2007); *see* Jonathan Band, *The Perfect 10 Trilogy*, 5 COMPUTER L. REV. INT'L 142 (2007) (discussing *Perfect 10 v. Visa International Service Ass'n* and its relationship to similar secondary liability cases). Band summarizes the Visa case:

> Here the Ninth Circuit rejected what would have represented a significant expansion of secondary liability to actors far removed from the infringing activity. However, unlike the other cases, this case provoked a strong dissent by respected jurist Alex Kozinski. This dissent suggests that the outer edges of secondary liability remain to be defined.

*Id.* at 14. Judge Kozinski's dissent is indeed stinging, but it also underestimates the burden that secondary liability would place on intermediaries. *Id.*

75 *Perfect 10*, 494 F.3d at 793.

76 *Id.*

77 *Id.* at 796.

78 *Id.*

79 *Id.*

chain that leads to the actual infringing acts for them to be described as making a material contribution.[80]

The court made a similar point about vicarious liability, finding that the card companies had no practical ability or right to prevent the infringing activity.[81] While credit card services can exert financial pressure on the infringing websites, they cannot stop the actual reproduction or distribution of the infringing images.[82]

In his dissent, Judge Kozinski rejected both arguments.[83] According to Judge Kozinski, the card companies were directly connected to the infringement because they provided payment services.[84] Without these payment services there would be no infringement.[85] The card companies had the contractual right to terminate illegal activity on their systems, as well as the practical ability to exert financial pressure to stop or limit the infringing activity.[86]

This dissent apparently played a role in a more recent case in which a district court found payment processors liable for trademark infringement for failing to take down allegedly infringing content. A key element in this case was the knowledge imputed to the payment processor of infringing activity that should have been apparent from an analysis of chargeback claims.[87]

## Payment System Complaint Program

Even though payment intermediaries may not be required to take steps against online copyright infringement, they have chosen to do so.[88] Payment systems cannot monitor their networks for copyright law violations. They do not have the factual basis to conclude that a particular sale of a product is a violation of

---

80 *Id.* at 797.

81 *Id.* at 803.

82 *Id.* at 804.

83 *Id.* at 810-11 (Kozinski, J., dissenting).

84 *Id.* at 811-12.

85 *Id.*

86 *Id.* at 816-17.

87 Gucci v. Frontline No. 9 Civ.6925 (HB) U.S. District Court for the Southern District, June 23, 2010

88 See generally International Piracy: The Challenges of Protecting Intellectual Property in the 21st Century: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary, 110th Cong. 73-82 (2007) [hereinafter International Piracy Hearing] (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.) (providing this account of payment intermediaries and intellectual property).

someone's copyright.[89] Many music downloads are perfectly legal transactions, but some are not. Distinguishing the two is often a complex factual and legal question which payment intermediaries do not have the expertise or ability to resolve.

The payment systems have no way of knowing whether a transaction involves copyright infringement without a complaint. The payment networks have thus developed policies and procedures to handle these complaints.[90]

The complaint process starts when a business entity approaches a payment system with clear, documented evidence of illegal activity and adequately identifies the infringing Internet merchant.[91] The business entity must provide substantiation that the activity is illegal and documentation that payment cards are actually being used for this illegal activity.[92]

The next step is to assess legality, which can be complex in cross-border situations.[93] After wrestling with these issues, the payment networks developed a policy for cross-border transactions: If a transaction would be illegal in either the jurisdiction of the merchant or the jurisdiction of the cardholder, the transactions should not be in the payment system.[94] In cases like copyright infringement, this means that merchants are responsible for making sure that the transactions they submit to the payment system are legal in both their operating jurisdiction and the jurisdiction in which their customer is located.

This assessment of legality requires the payment network to determine whether the type of transaction would be illegal in either jurisdiction.[95] Since the facts and law involved are often complex, the payment networks are willing to take on only the clearest cases of copyright violation. Once they determine illegality, the payment providers do what they reasonably can to assist the complaining party. Since payment networks do not work directly with merchants, they typically try to locate the bank that has the merchant account and provide the complaint to the bank involved, which usually resolves the issue.[96] In most cases, either the bank does not want the business and terminates the merchant

---

89 *Id.* at 76.

90 *Id.* at 77.

91 This Section describes the process at Visa, but other payment networks use a similar process. *See id.* at 85.

92 *Id.*

93 *Id.* at 77-78.

94 *Id.* at 78.

95 *Id.*

96 *Id.*

or takes other action to bring the merchant into compliance.[97] If the bank does not take action, the payment networks can take further enforcement action against the bank.[98]

## Allofmp3.com

In some instances, the merchant resists the enforcement efforts of payment systems, insists on the legality of the underlying activity, and goes to a local court to vindicate its perceived rights under local law. This is what occurred in the Allofmp3.com case.

In 2005, Visa received a documented complaint from International Federation of the Phonographic Industry (IFPI), which represents copyright owners based in more than seventy countries.[99] The complaint alleged that Allofmp3.com, a website located in Russia, was infringing on the copyrights of IFPI's members by allowing unauthorized downloads of music.[100] Visa assessed the legal situation, in part by obtaining a review by outside counsel, and concluded that the transactions were illegal under local Russian law.[101] They were also illegal under the laws of the vast majority of the merchant's customers who were located primarily in the United Kingdom and the United States.[102] In October 2005, the Italian authorities shut down a localized version of Allofmp3.com, allofmp3.it, and began a criminal investigation of the Italian site.[103] In addition,

---

97 *Id.*

98 *Id.* Payment systems have a voluntary program such as this in place for counterfeiting complaints as well. This program includes include having a process in place to respond to complaints of the use of a payment brand for sales of counterfeit goods. Trademark owners would provide information such as a description of the allegedly counterfeit transaction and evidence that the payment system brand was involved, and the payment system would look into the allegation and take action in according with a publicly stated policy, which could include suspension of the merchant involved. Trademark owners would agree to indemnify payment systems for steps taken and for legal risk. This system is described by INTA in "Addressing the Sale of Counterfeits on the Internet," September 2009 available as attachment 3 in the INTA Submission On The Request For Public Comment Regarding The Joint Strategic Plan For IP Enforcement**,** for the Office of the Intellectual Property Enforcement Coordinator (IPEC) through the Office of Management and Budget *,* March 24, 2010 available at **http://www.whitehouse.gov/omb/IPEC/frn_comments/InternationalTrademarkAssociation.pdf**

99 *Id.*

100 *Id.* (discussing IFPI's role); Nate Anderson, *Music Industry Encouraged Visa to Pull the Plug on AllofMP3.com*, ARSTECHNICA, Oct. 19, 2006, **http://arstechnica.com/business/news/2006/10/8029.ars**.

101 *International Piracy Hearing*, *supra* note 88, at 79 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

102 *Id.*

the United States Trade Representative intervened with the Russian government to urge them to shut down Allofmp3.com.[104]

At the beginning of September 2006, after appropriate notice, the Russian bank working with Allofmp3.com stopped processing Visa transactions for Allofmp3.com.[105] At the end of September 2006, the bank also stopped processing transactions from an affiliated site called allTunes.[106] After these Visa transactions ended, further confirmation of the site's illegality was forthcoming; a Danish court ordered the Internet provider Tele2 to block its subscribers' access to allofmp3.com, thereby making it harder for potential customers in Denmark to access the site.[107] MasterCard also cut off payment services to allofmp3.com.[108] By May of 2007, the site's popularity had plummeted.[109]

The company was all but out of business, but the legal process was just starting. The owner of allTunes sued the bank that had stopped processing its Visa transactions in a Russian court.[110] Visa was a party to that litigation on the side of the bank.[111] In June 2007, the owner won a judgment that the bank had violated its contract with the merchant, and the judgment required the bank to continue to provide processing services.[112] In response to the bank's claim that the merchant was acting illegally, the court determined that there were no rulings in Russia establishing that allTunes was making illegal use of exclusive rights belonging to rights holders.[113]

---

103 Press Release, IFPI, *Allofmp3.com: Setting the Record Straight*, June 2, 2006, **http://www.ifpi.org/content/section_news/20060601.html**.

104 *See International Piracy Hearing*, *supra* note 88, at 26 (testimony of Victoria A. Espinel, Assistant U.S. Rep. for Intellectual Property and Innovation, Office of the U.S. Trade Rep.) ("We will continue to press Russia to shut down and prosecute the operators of illegal Web sites operating in Russia, including the successors to the infamous AllOfMP3.com.").

105 *Id.* at 79 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

106 *Id.*

107 Press Release, IFPI, *New Court Setback for Allofmp3.com*, Oct. 26, 2006, **http://www.ifpi.org/content/section_news/20061026.html**.

108 BBC News, *MP3 site's voucher system closes*, May 21, 2007, **http://news.bbc.co.uk/2/hi/entertainment/6677265.stm**.

109 IFPI reported in May 2007 that Allofmp3 "rated outside the top 2000 websites." Press Release, IFPI, *Police Dawn Raid Stops Allofmp3.com Pirate Vouchers Scheme*, May 21, 2007, **http://www.ifpi.org/content/section_news/20070521.html**.

110 Arbitration Court of Moscow 2007, A40-70411/06-67-500.

111 *Id.* at 1.

112 *Id.* at 5.

113 *Id.* The court stated:

In August 2007, another Russian court issued a ruling in a different case, relating to criminal copyright infringement initiated by IFPI against the owner of Allofmp3.com.[114] This ruling stated that there had not been sufficient confirmation of any illegal activity by the site's owner.[115] Even though the copyright owners had not given permission to distribute their recorded material, a Russian collective rights society (the Russian Multimedia and Internet Society, or ROMS by its initials in Russian) was deemed to be operating legitimately under Russian law.[116] The court implied that Allofmp3.com and similar sites would be in compliance with Russian law to the extent that they paid for rights from this Russian collective rights society.[117]

These court cases created a challenge for Visa because the payment system had responded to a documented complaint of copyright infringement.[118] Despite an outside review that seemed to establish illegality in the local jurisdiction, a local court ordered a local bank to continue to provide payment services.[119] Yet these transactions would still be illegal in virtually every other country in the world. To preserve its cross-border policy, Visa decided to allow the local bank to provide only domestic service to the site involved in the court case.[120] Transactions from customers in other countries would not be allowed.[121]

---

> According to Article 49 of the Russian Federation Law "On Copyright and Allied Rights," it is only the Court that can execute actions in connection with illegal use of copyrights and allied rights, if there is a lawsuit filed by exclusive right holders, which the Defendants, VISA and IFPI are not, while in this case there are no court rulings with the force of *res judicata* establishing the Plaintiff's illegal use of exclusive rights belonging to some right holders.

*Id.* The Defendant was Rosbank, the Russian financial institution licensed by Visa to authorize merchants in Russia to accept Visa. *Id.*

114 Cheremushkinsky [District Court of Moscow], 2007, No. 1-151-07.

115 *Id.* at 4.

116 *Id.* at 5.

117 *Id.*; *see also International Piracy Hearing*, *supra* note 88, at 99 (testimony of Victoria A. Espinel, Assistant U.S. Rep. for Intellectual Property and Innovation, Office of the U.S. Trade Rep.) ("My understanding of the case is that Media Services, the company that operated allTunes, was able to successfully argue in Russian court that it was not acting illegally because it was paying royalties to collecting societies, collecting societies that were not authorized by the rights holders.").

118 *Id.* at 80 (statement of Mark MacCarthy, Senior Vice President for Global Public Policy, Visa Inc.).

119 *Id.* at 80-81.

120 *Id.*

121 *Id.* at 81.

## Assessment of Payment System Actions on Online Copyright Infringement

Are payment systems doing enough on their own to respond to online copyright infringement? Does there need to be a system of legal liability for them to control online copyright infringement using their payment systems?

First, *Perfect 10* properly rejected indirect liability for payment intermediaries.[122] The involvement of payment networks in copyright violations is attenuated and entirely passive. On control grounds, there is simply no way to draw a line between payment network involvement in allegedly infringing transactions and involvement in a wide range of other potentially illegal activities. If they are liable in this case, why wouldn't they be liable for all cases of illegal activity on their payment systems? Unintentionally, Judge Kozinski's dissent brought out this implication.[123]

But the actual experience of payment intermediaries reveals that things are never as simple as removing infringing material. At best, there is a well-documented assertion of infringement under the laws of a particular jurisdiction. Judge Kozinski appears to favor a notice-and-takedown approach, so that payment intermediaries are not responsible for illegal conduct of which they are unaware.[124] But as Visa found in *Allofmp3.com*, payment card services and their associated financial service partners can be liable for wrongful termination of services in those jurisdictions if they react to an allegation of infringement by "kick[ing] the pirates off their payment networks."[125]

---

122 Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 798 (9th Cir. 2007). For analysis, see Band, *supra* note 74.

123 *See id.* at 824 (Kozinski, J., dissenting) ("Credit cards already have the tools to police the activities of their merchants, which is why we don't see credit card sales of illegal drugs or child pornography."). Of course, card companies use different tools in the case of illegal drugs and child pornography, namely, proactive monitoring, but it is hard to see on Kozinski's analysis why card companies shouldn't use whatever tools they can to stop illegal activity in all cases. *See id.* ("Plaintiff is not asking for a huge change in the way credit cards do business; they ask only that defendants abide by their own rules and stop doing business with crooks. Granting plaintiff the relief it seeks would not … be the end of Capitalism as we know it."). But it might be the end of payment systems as we know them if indirect liability for them means an obligation to stop doing business with everyone who might be involved with illegality anywhere. Kozinski attempts to limit his analysis to those cases where there are special arrangements between bad actors and the payment system, *id.* at 819-20, but nothing in his analysis turns on these special arrangements. These special arrangements turn out to be risk-based pricing for adult content websites. Would he really have voted with the majority if the price that adult content merchants face for accepting cards was the same as the price set for less risky merchants?

124 *Perfect 10*, 494 F.3d at 824 (Kozinski, J., dissenting).

125 *Id.* at 817.

Second, there is no market failure in this situation that would justify imposing intermediary liability on payment systems. There are available arrangements between payment intermediaries and copyright owners that can reduce the amount of copyright infringement on the Internet. These arrangements are informal, but expanding. They rely on complaints by copyright owners, followed by investigation and action by intermediaries. They seem to strike a cost-based balance by putting the burden of discovering infringement on the copyright owner and triggering action by the third party only after notification. The arrangements may involve compensating payment intermediaries for performing enforcement services, but if this enables copyright owners to reduce the harm of copyright infringement, they might very well pay. If there are extra efforts, above and beyond standard practices, that a particular copyright owner would like payment intermediaries to make, those efforts should be open to negotiation. There do not seem to be any transaction costs that would prevent the parties from negotiating adjustments to these arrangements over time. And there appears to be no market failure that would justify not relying on private sector enforcement arrangements.

Third, given the legal risks involved, copyright owners should be willing to indemnify payment intermediaries for damages resulting from enforcement actions against alleged infringers. *Allofmp3.com* indicates that these legal risks are not hypothetical. If the copyright owner believes in the legal soundness of his case, he should be prepared to assume the risk. It might be one way to assure that only strong complaints are brought to the attention of the payment intermediary. An additional mechanism might be to require the presence of a court or governmental agency that holds that the activity involved is infringing.

A statute could potentially help provide legal immunity to payment intermediaries when they take good-faith action against alleged infringers. But U.S. law cannot provide immunity in other jurisdictions, which is where the aid of global payment intermediaries is needed.

Fourth, this case illustrates the need for greater clarity in the legal environment in which intermediaries operate. Intermediaries cannot be in the position of creating new global law through their own interpretation of current statutes. Again *Allofmp3.com* suggests the need for even greater harmonization of local laws that intermediaries are expected to enforce.

In sum, the experience of payment intermediaries indicates that some efforts on their part to respond to legitimate complaints would be justified. It is not appropriate to do nothing in response to allegations of copyright infringement. The current complaint procedure and case-by-case response is reasonable. It could be improved through further discussions among the parties, further recourse to court judgments of infringement, and harmonization of current international standards.

## Conclusion

The question remains: Should the government place an enforcement burden on payment intermediaries? The standard least cost analysis suggests that the advantages of government intervention sometimes appear to be substantial, but nothing in the analysis suggests that Internet intermediaries are always the best vehicle for government control. The costs, benefits and equities involved in specific cases have not been adequately assessed. Intermediaries are often in a position to voluntarily police their own communities and have taken steps to do this without explicit government requirements. The equities set out in current law establish a regime that works tolerably well. Even when government requirements are explicit, as in the case of Internet gambling, they are often crafted to fit the architecture and structure of the intermediaries themselves. While some adjustments would improve these legal regimes, nothing suggests that more liability imposed unilaterally by local governments would be an improvement.

Greater government coordination on the rules that intermediaries must follow on the Internet would be an improvement. To avoid legal liability and to comply with local laws, payment intermediaries are moving toward accepting the laws of all jurisdictions. They also have wide discretion on what activities to allow on their systems. But this situation is problematic. Intermediaries are not the best- situated to decide which rules to follow. Also, no laws are self-interpreting. They often apply to particular situations in obscure and heavily fact-dependent ways. Intermediaries' flexibility in adjudication leaves room for private, strategic, and unaccountable decisions that affect the shape and direction of online activity. Coordinated government rules are best for an additional reason: The intermediary role does not scale well in a world of multiple, overlapping, and conflicting rules. If governments are going to use intermediaries to regulate the Internet, they need to coordinate their own laws to make that role possible.

# Fuzzy Boundaries: The Potential Impact of Vague Secondary Liability Doctrines on Technology Innovation

By Paul Szynol*

Last year, Ninth Circuit Judge Alex Kozinski, with Josh Goldfoot from the Department of Justice's Criminal Division, published an article in the Columbia Journal of Law and the Arts entitled "A Declaration of the Dependence of Cyberspace." Its title is a play on the title of John Perry Barlow's 1996 "A Declaration of the Independence of Cyberspace"; its content, as the title suggests, is something of an attack on Barlow's philosophies, and, more generally, on the idea that the Internet is a unique entity that requires custom legal treatment. The authors make several key claims about the law's relationship to the internet, but the central argument focuses on secondary liability—the copyright doctrine that makes makers of multi-use technologies legally liable for other people's infringing uses of their technology.

Broadly stated, the rationale at the heart of the secondary liability doctrine is this: An entity that knowingly helps to facilitate the commission of an illegal act (such as copyright infringement, for example) should be penalized for its contribution to the illegal activity.[1] If a technology company induces its customers to use its product for infringing purposes, for instance, both the users *and* the company should be liable for such infringement—the users for direct infringement and the company for contributory infringement, which is a species of secondary liability.

The doctrine is appealing as a practical solution to widespread infringement because it targets the entities that enable illegal behavior—*e.g.*, the Napsters and Groksters of the world—and thus eradicates the distribution mechanism that enables infringement in the first place. Judge Kozinski and Mr. Goldfoot (I'll generally refer to them as "the authors" from here on), like the movie and music industries, certainly believe that the doctrine of secondary liability should be readily used as a handy and effective tool for weeding out copyright

---

* Paul Szynol graduated from Columbia University, where he studied history and philosophy, and Yale University, where he studied intellectual property law.

1 The specific theories of secondary liability have more nuanced elements, such as the requirements of materiality for contributory infringement and direct financial benefit for vicarious infringement. Since these elements are not critical to the essay's main thesis, I've avoided spelling them out in detail.

infringement. According to the authors, people "who provide powerful tools that can be used for good or evil have some responsibility to make sure that those tools are used responsibly." Put more bluntly, however, if you outlaw the tool, you needn't chase after the users, so in practice it's less a question of ethics and more a question of convenience and efficiency.

One of the principal problems with this approach, however, is the fact that the boundaries of secondary liability are not precisely set, and, short of extreme cases, it is not at all clear under what circumstances a product manufacturer will be liable for secondary infringement. Such wholesale endorsement for secondary liability doctrines should therefore give us some pause. For example, at what point does a software company that develops a peer-to-peer application utilized by end users to exchange copyrighted materials begin to "contribute" to the infringement and become secondarily liable? Does the company contribute simply by writing software that is merely capable of infringing uses?[2] Or does the company contribute only if the software's primary use is, by design, infringing? Or, further yet, does the company contribute only if a substantial portion of the end-users utilize the technology for infringing purposes? If so, how much of the user base must engage in infringing activity for it to be a substantial portion? [3] Or, as yet another option, does the company "contribute" only if it promotes infringing uses of its software? And, if that's the case, how much promotion is too much promotion? For example, is the advertising slogan "Rip. Mix. Burn." too much of an inducement to make infringing copies of music?[4]

These are fundamental, starting-point questions about the secondary liability doctrine, and one would expect that case law or legislation provides a clear answer to each. Yet the law is ambiguous (and the authors are altogether silent) on these points. Outside of extreme cases, no one knows with certainty—including lawyers, judges, company officers, engineers and academics—when secondary liability might attach to a product that facilitates the transmission of copyrighted materials. The legal system's failure to provide clear guidelines is

---

2 An argument that the Supreme Court famously rejected in its 1984 "Betamax" decision. *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

3 See, for example, the Napster litigation. According to the District Court's opinion, 87% of the content on Napster was copyrighted, and "virtually all Napster users" transferred copyrighted content. *A & M Records, Inc. v. Napster*, Inc., 114 F. Supp. 2d 896 (N.D.Ca. 2000). A decade later, a critical question remains essentially unanswered: How much lower would those percentages have to be for a manufacturer to be safe from secondary liability?

4 The standard introduced in *Grokster* is "clear expression", which is not much of a lodestar for someone seeking to gauge risk with any degree of precision. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 914 (2005). One could persuasively argue that Apple's very large, very prominent and very ubiquitous "Rip. Mix. Burn." billboards amounted to "clear expression."

the equivalent of posting a sign on a freeway that says "obey the speed limit" without giving an actual speed.

The effect is potentially detrimental to the entire technology sector. A clear rule is a predictable rule, and a predictable rule is one on which innovators can rely when developing a product. Without clear guidance from the legal system, tech companies are forced to engage in a "fingers crossed" product design process, and, subsequently, face a market that can be an explosive landmine of infringement liability. The potential economic damage to a company found guilty of secondary liability can be substantial, to say the least. Since statutory damages for copyright infringement range from $750 to $150,000 per infringement, a maker of a multi-use technology may confront liabilities on a scale that can threaten the viability of even the wealthiest corporations. The risk is further exacerbated by the recent trend of unpredictable and often very bloated damage awards granted to copyright plaintiffs. Such risk can dissuade even the most resolute investors from marketing their invention—and it can literally bankrupt the braver among them. The loss of a robust distribution tool harms the content sector, too, since a powerful method for distributing content to end users will not be brought to market.

Judge Kozinski and Mr. Goldfoot are not concerned with the chilling effect that the legal system's ambiguity can have on technology innovation. In fact, they reject the proposition, and confidently point to the pharmaceutical and auto industries as counter-examples: Both industries have to comply with legal regulation yet manufacturers in both industries nevertheless innovate.

It's not a very persuasive comparison. First, the auto industry is hardly a hotbed of innovation. We might really like power windows and power steering, but, as advancements over prior art, these innovations are an order of magnitude smaller than the innovation we've seen on the internet. Second, the players in the auto and pharmaceutical industries are frequently different from the players in the technology sector. It is rare, after all, if not unheard of, that a single person invents valuable medicine—the medical R&D process takes place in the laboratories of some of the wealthiest companies under the sun. In addition, medical innovation is subject to review and approval by government regulatory agencies, so by the time a medicine reaches the market, it has already been approved by the government. Innovation in information technology, in contrast, is often the result of the proverbial garage inventor who releases the technology entirely on its own. Think of eBay, Napster, Apple, Google and Microsoft, each of which had a modest start in someone's home or garage at the hands of one or two people (and many subsequently acquired similarly independent garage innovations). The distinction between a multinational company and a garage inventor is critical. First, there is no government imprimatur for multi-use technologies. Second, in contrast to wealthy companies that can afford sophisticated legal teams, garage inventors typically

lack the economic resources necessary to pay for a comprehensive legal review of product design prior to the product's release. That inability increases the likelihood that the garage inventor will—unwittingly—design its product in a way that leads to legal liability, or the likelihood that, after releasing the product and receiving angry threats of litigation, the garage inventor will have to backtrack and redesign the product in order to avoid liability. These are very expensive measures. If the inventor can afford them, the inventor will have spent money that it would have saved had the law simply been clearer in the first place; if the inventor cannot afford them, the outcome is even worse: the start-up will simply fold, thus wasting its investment costs, while consumers will miss out on the product altogether.

That outcome is bad enough, but it's the third reason for the comparison's inadequacy that should give all of us some pause: Because the legal landscape around copyright secondary liability is so unclear, even if the would-be inventor did have the resources to hire outside counsel, lack of clarity in the law means that, unless the product clearly crosses a line, lawyers—no matter how high their hourly rates—won't be able to confidently provide the inventor with a legal imprimatur. In other words, no matter how much a company tries, lack of clear standards means that its lawyers might "get it wrong," and the company may face infringement liability if it releases the product, or incur the costs of post-release redesign, or both. That is a very expensive proposition, and its corollary is clear: Faced with potential liability exposure and potential redesign costs, each of which could figure in the millions or even billions of dollars,[5] some would-be inventors and investors will, as rational economic actors, forego the whole enterprise—not because they analyzed the risk and found it potentially too costly, but because the law's ambiguity meant they simply *couldn't* properly analyze the risk in the first place. Notably, the foregoing outcome will apply to garage inventors and big companies alike. The garage inventor whose coffers won't be able to withstand the potential cost will retreat to the sound of a distant death knell; the big company will retreat because it knows that its deep pockets makes it an attractive target for a lawsuit and therefore may well decide that the potential litigation and licensing costs, even if not fatal, just aren't worth it. Again, consumers will miss out on a new product.

An ambiguous secondary liability doctrine also disadvantages American products in a global market: U.S. companies will have to worry about drowning in the unpredictable and poorly charted quicksand of secondary liability, while their international competitors will have clear legal rules to guide them. The

---

[5] It's worth emphasizing that the billion dollar figure is not hyperbole—just ask SAP, which recently lost its legal dispute with Oracle and was ordered to pay $1.3 billion in damages. See Sam Diaz, *Jury: SAP Owes Oracle $1.3 Billion for Copyright Infringement*, ZDNET, Nov. 23, 2010. The facts of that case are quite different from the examples given here, of course, but the award is a very conspicuous reminder that such astronomical damage awards are a startling reality of present day copyright litigation.

domestic market suffers as well: By creating barriers to entry (high and unreliable due diligence costs as well as post-release redesign costs), the ambiguity favors entrenched entities over newcomers. Advocating secondary liability without removing the ambiguity also contradicts the authors' claim that the same set of laws should apply to offline and online worlds: The fuzzy secondary liability doctrine which they so strongly espouse in connection with technology wouldn't fly in the physical world. For example, should a car company be held liable for drivers who speed? After all, it would be easy enough to add a "speed limit compliance chip." Yet auto manufacturers are not forced to pay any portion of a speeding driver's ticket. Offline, in other words, bad actors—the *users* of technology—are punished for their own transgressions. Online, however, the law chases the manufacturers—and applies ad-hoc, ambiguous standards to their products. It would seem that the authors want Internet-specific laws after all.

None of this sounds like wise intellectual property policy. The legal system has a constitutional imperative to incentivize inventors, after all, and it achieves this objective in part by providing both content producers[6] *and* innovators with a stable and predictable legal climate, such as the "bright line" rule devised by the Supreme Court in its 1984 *Sony* ruling.[7] In its current state, the law threatens to punish rather than reward those who have the courage to release an innovative technology if that technology may be misused by its adopters and if that technology has yet to be contemplated and cleared by the judiciary or legislature. That is not an environment that encourages innovation. If the intent of the judiciary and the Department of Justice is indeed to mightily wield the secondary liability sword across the technology sector, the doctrine must be clearly defined, so that the rules of engagement are clearly stated and U.S. innovators can design their products with confidence—not in fear.

---

6 In *Community for Creative Non-Violence v. Reid*, the Supreme Court acknowledged "Congress' paramount goal in revising the 1976 Act of enhancing predictability and certainty of copyright ownership." 490 U.S. 730, 749 (1989).

7 *Sony v. Universal City Studios*, *supra* note 2.

# CHAPTER 7

## IS SEARCH NOW AN "ESSENTIAL FACILITY?"

# Dominant Search Engines: An Essential Cultural & Political Facility

By Frank Pasquale*

Many worry about search engines' growing power. How are worldviews being biased by them? Do search engines have an interest in getting certain information prioritized or occluded?[1] Dominant search engines ("DSEs")[2] are a key hub of Internet traffic. They provide an ever-expanding array of services. Google, for instance, just announced its intention to go into travel shopping. As they amass information about their users, calls for regulation have focused on the threats to privacy they generate. Some of these efforts have been successful; others look more doubtful. One thing is certain: They are only the beginning of a struggle over the rights and responsibilities of key intermediaries. Some hope that competition law—and particularly the doctrine of "essential facilities"—will lead policymakers to scrutinize search engines actions.

When American lawyers talk about "essential facilities," they are referring to antitrust doctrine that has tried, at various points, to make certain "bottlenecks" in the economy provide access on fair and nondiscriminatory terms to all comers. As robust American competition law fades into a secluded corner of legal history,[3] "essential facilities" doctrine still remains, for some scholars, a ray of hope for intermediary responsibility.[4] Oren Bracha and I helped fuel this

---

* Professor of Law, Seton Hall Law School; Visiting Fellow, Princeton Center for Information Technology Policy.

1 ALEX HALAVAIS, SEARCH ENGINE SOCIETY 85 (Polity 2008) ("In the process of ranking results, search engines effectively create winners and losers on the web as a whole. Now that search engines are moving into other realms, this often opaque technology of ranking becomes kingmaker in new venues."); Chi-Chu Tschang, *The Squeeze at China's Baidu*, BUSINESSWEEK, Dec. 31, 2008, at **www.businessweek.com/magazine/content/09_02/b4115021710265.htm** ("Salespeople working for Baidu drop sites from results to bully companies into buying sponsored links [a form of paid advertising], say some who have been approached.").

2 We can provisionally define a dominant search engine ("DSE") as one with more than 40 percent market share. Google clearly satisfies this criterion in the United States and Europe. *See* David S. Evans, *Antitrust Issues Raised by the Emerging Global Internet Economy*, 102 NW. U. L. REV. COLLOQUY 285 (2008) (reporting market shares for leading internet intermediaries).

3 BARRY LYNN, CORNERED: THE NEW MONOPOLY CAPITALISM AND THE ECONOMICS OF DESTRUCTION (John Wiley & Sons, Inc. 2010) (describing the declining impact of American antitrust law).

4 Brett Frischmann & Spencer Weber Waller, *Revitalizing Essential Facilities*, 75 ANTITRUST L.J. 1, 2 (2008) ("infrastructure subject to substantial access and nondiscrimination norms [has] … been heavily regulated.").

hope in our 2008 article *Federal Search Commission*, which compared dominant search engines to railroads and common carriers in the hope that they would be recognized as infrastructural foundations of the information economy.[5] But I now see that *Federal Search Commission,* like many other parts of the search engine accountability literature, tried too hard to shoehorn a wide variety of social concerns about search engines into the economic language of antitrust policy.[6] It is now time for scholars and activists to move beyond the crabbed vocabulary of competition law to develop a richer normative critique of search engine dominance.

This will not be an easy sell in cyberlaw, which tends to uncritically promote competition and innovation as the highest aims of Internet policy. If a dominant search engine is abusing its position, market-oriented scholars say, market forces will usually solve the problem, and antitrust law can step in when they fail to do so. Even those who favor net neutrality rules for carriers are wary of applying them to other intermediaries, like search engines. All tend to assume that the more "innovation" happens on the Internet, the more choices users will have and the more efficient the market will become. Yet these scholars have not paid enough attention to the *kind* of innovation that is best for society, and whether the uncoordinated preferences of millions of web users for low-cost convenience are likely to address the cultural and political concerns that dominant search engines raise.

In this article, I hope to demonstrate two points. First, antitrust law terms (like "essential facility") cannot hope to capture the complexity of concerns raised by an information landscape where one company serves as the predominant map of the web, and simultaneously attempts to exploit that dominance by endlessly expanding into adjoining fields. Second, I hope to point the way toward a new concept of "essential cultural and political facility," which can help policymakers realize the situations where a bottleneck has become important enough that special scrutiny is warranted. This scrutiny may not always lead to regulation—which the First Amendment renders a dicey enterprise in any corner of the information economy. However, it could lead us to recognize the importance of publicly funded alternatives to the concentrated conduits and content-providers colonizing the web.

---

5 Oren Bracha & Frank Pasquale, *Federal Search Commission: Fairness, Access, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1193 (2008).

6 RICHARD POSNER, ANTITRUST LAW, at ix (2d ed. 2001) ("Almost everyone professionally involved in antitrust today—whether as litigator, prosecutor, judge, academic, or informed observer—not only agrees that the only goal of the antitrust laws should be to promote economic welfare, but also agrees on the essential tenets of economic theory that should be used to determine the consistency of specific business practices with that goal.").

## The Limits of Antitrust as Search Policy

Antitrust cases tend to consume a great deal of time, in part because economic conduct is subject to many different interpretations.[7] One person's anticompetitive conduct is another's effective business strategy. The same unending (and indeterminate) arguments threaten to stall discourse on search policy. For example, the Federal Trade Commission's (FTC) review of the Google–DoubleClick merger focused almost entirely on the economic effects of the proposed combination, rather than the threats to privacy it posed.[8]

Search engines are among the most innovative services in the global economy. They provide extraordinary efficiencies for advertisers and consumers by targeting messages to viewers who are most likely to want to receive them. In order to attract more users, search engines use revenues from advertising to organize and index a great deal of content on the Internet. Like the major broadcast networks, search engines are now beginning to displace. They provide opportunities to view content (organic search results) in order to sell advertising (paid search results).[9] Search engines have provoked antitrust scrutiny because proposed deals between major search engines (and between search engines and content providers) suggest undue coordination of competitors in an already concentrated industry.[10]

---

7 *See* Jonathan Zittrain, *The Un-Microsoft Un-Remedy: Law Can Prevent the Problem that It Can't Patch Later*, 31 CONN. L. REV. 1361, 1361–62 (1999) (**"**The main concern in finding a remedy for ['bad monopolist behaviors'] may be time: The technology environment moves at a lightning pace, and by the time a federal case has been made out of a problem, the problem is proven, a remedy fashioned, and appeals exhausted, the damage may already be irreversible.").

8 News Release, FTC, Federal Trade Commission Closes Google/DoubleClick Investigation (Dec. 20, 2007), *available at* www.ftc.gov/opa/2007/12/googledc.shtm ("The Commissioners ... wrote that 'as the sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition,' the FTC lacks the legal authority to block the transaction on grounds, or require conditions to this transaction, that do not relate to antitrust. Adding, however, that it takes consumer privacy issues very seriously, the Commission cross-referenced its release of a set of proposed behavioral marketing principles that were also announced today.").

9 According to the Google corporate home page, "[W]e distinguish ads from search results or other content on a page by labeling them as 'sponsored links' or 'Ads by Google.' We don't sell ad placement in our search results, nor do we allow people to pay for a higher ranking there." Google, Inc., Corporate Information: Company Overview, www.google.com/corporate/ (last visited Mar. 12, 2010).

10 For example, the deal reached between Microsoft and Yahoo! that would have Microsoft's Bing search engine deliver results for searches on Yahoo! has provoked antitrust concerns both domestically and internationally. *See* Christopher S. Rugaber, *Microsoft–Yahoo Deal to Face Tough Antitrust Probe*, ABCNEWS, July 29, 2009, **http://seattletimes.nwsource.com/html/localnews/2009563654_apusmicrosoftyahooantitrust.html**.

Those opposed to regulation often claim that antitrust law offers a more targeted and efficient response to abuses. As Justice Breyer explained in his classic work *Regulation and Its Reform*:

> [T]he antitrust laws differ from classical regulation both in their aims and in their methods … . [T]hey act negatively, through a few highly general provisions *prohibiting* certain forms of private conduct. They do not affirmatively order firms to behave in specified ways; for the most part, they tell private firms what not to do … . Only rarely do the antitrust enforcement agencies create the detailed web of affirmative legal obligations that characterizes classical regulation.[11]

Given the lack of search engine regulation in the U.S., actual and threatened antitrust investigations have been a primary government influence on Google's business practices as its dominance in search grows. Many believe that the Department of Justice's (DOJ) suspicion of the company's proposed joint venture with Yahoo! in the search advertising field effectively scuttled the deal by late 2008.[12] However, antitrust enforcement appears less promising in other aspects of search.[13] This section discusses the limits of antitrust in addressing the cultural and political dilemmas raised by Google's proposed Book Search deal with publishers,[14] and its dominance of online advertising.

---

11 STEPHEN BREYER, REGULATION AND ITS REFORM 156–57 (Harvard Univ. Press 1982). *But see* A. Douglas Melamed, *Antitrust: The New Regulation*, 10 ANTITRUST 13, 13 (1995) (describing "two paradigms," the law enforcement model and the regulatory model, and the shift of antitrust law from the former to the latter).

12 Nicholas Thompson & Fred Vogelstein, *The Plot to Kill Google*, WIRED, Jan. 19, 2009, at 88, *available at* www.wired.com/techbiz/it/magazine/17-02/ff_killgoogle (noting that antitrust scrutiny culminated in a hearing in which the DOJ threatened to bring an antitrust case against Google and that one prominent DOJ attorney expressed the view that Google already is a monopoly).

13 Daniel Rubinfeld, *Foundations of Antitrust Law and Economics*, *in* HOW THE CHICAGO SCHOOL OVERSHOT THE MARK: THE EFFECT OF CONSERVATIVE ECONOMIC ANALYSIS ON U.S. ANTITRUST 51, 57 (Robert Pitofsky ed., 2008) (describing how "conservative economics has fostered a tendency to downplay enforcement in dynamic technological industries in which innovation issues play a significant role").

14 Despite the DOJ's intervention to affect the terms of the proposed settlement, many leading antitrust experts have argued that the settlement would not violate the antitrust laws. *See, e.g.*, Einer Elhauge, *Why the Google Books Settlement Is Pro-Competitive* 58 (Harvard Law Sch., Law & Econ. Discussion Paper No. 646, Harvard Law Sch., Pub. Law & Theory Research Paper No. 09-45, 2009), *available at* **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1459028** ("The settlement does not raise rival barriers to offering [many] books, but to the contrary lowers them. The output expansion is particularly dramatic for out-of-print books, for which there is currently no new output at all.").

Privacy concerns are nearly impossible to address within the economic models of contemporary competition law. Antitrust scrutiny did little to address the privacy concerns raised when Google proposed to merge with the web advertising firm DoubleClick.[15] The proposed deal provoked a complaint from the Electronic Privacy Information Center (EPIC). EPIC claimed that Google's modus operandi amounts to a "deceptive trade practice":

> Upon arriving at the Google homepage, a Google user is not informed of Google's data collection practices until he or she clicks through four links. Most users will not reach this page … . Google collects user search terms in connection with his or her IP address without adequate notice to the user. Therefore, Google's representations concerning its data retention practices were, and are, deceptive practices.[16]

One key question raised by the proposed merger was whether privacy and consumer protection concerns like these can be addressed by traditional antitrust analysis.[17] Privacy law expert Peter Swire argued that they can, because "privacy harms reduce consumer welfare … [and] lead to a reduction in the quality of a good or service."[18] Swire believed that consumers would be worse off after the merger because of the unparalleled digital dossiers the combined entity could generate:

> Google often has "deep" information about an individual's actions, such as detailed information about search terms. Currently, DoubleClick sets one or more cookies on an individual's computers, and receives detailed information about which sites the person visits while surfing. DoubleClick has

---

15 Dawn Kawamoto & Anne Broache, *FTC Allows Google–DoubleClick Merger to Proceed*, CNET NEWS, Dec. 20, 2007, **http://news.cnet.com/FTC-allows-Google-DoubleClick-merger-to-proceed/2100-1024_3-6223631.html** (describing U.S. authorities' blessing of the proposed deal).

16 *See* Complaint and Request for Injunction, Request for Investigation and for Other Relief, *In re* Google Inc. and DoubleClick, Inc., No. 071-0170 (FTC Apr. 20, 2007), *available at* **http://epic.org/privacy/ftc/google/epic_complaint.pdf** at 9 [hereinafter Google, Inc. and DoubleClick Complaint].

17 *See* Siva Vaidhyanathan, The Googlization of Everything, Google and DoubleClick: A Bigger Antitrust Problem than I Had Imagined, www.googlizationofeverything.com/2007/10/google_and_doubleclick_a_bigge.php (Oct. 21, 2007, 16:05 EST).

18 Peter Swire, *Protecting Consumers: Privacy Matters in Antitrust Analysis*, CTR. FOR AM. PROGRESS, Oct. 19, 2007, www.americanprogress.org/issues/2007/10/privacy.html (italics omitted).

> "broad" information about an individual's actions, with its leading ability to pinpoint where a person surfs.[19]

Initial points of contention include (a) the definition of the products at issue, and (b) how to weigh the costs and benefits of a merger. The combined company would have different segments of "customers" in a two-sided market:[20] (1) searchers trying to find sites, and (2) ad buyers trying to reach searchers. Swire contends that many people care about privacy, and "[i]t would be illogical to count the harms to consumers from higher prices while excluding the harms from privacy invasions—both sorts of harms reduce consumer surplus and consumer welfare in the relevant market."[21]

However, the web searcher category not only consists of consumers who care about privacy, but also includes many people who do not highly value it or who actively seek to expose their information in order to receive more targeted solicitations. According to Eric Goldman's work on personalized search, some may even consider the gathering of data about them to be a service.[22] The more information is gathered about them, the better intermediaries are able to serve them relevant ads. Many economic models of web publication assume that users "pay" for content by viewing ads;[23] they may effectively pay less if the advertisements they view bear some relation to things they want to buy. So while Swire models advertising and data collection as a cost to be endured,

---

19 *Id.* According to Swire, "[i]f the merger is approved, then individuals using the market leader in search may face a search product that has both 'deep' and 'broad' collection of information. For the many millions of individuals with high privacy preferences, this may be a significant reduction in the quality of the search product—search previously was conducted without the combined deep and broad tracking, and now the combination will exist." *Id.*

20 For a definition of two-sided market, see Nicholas Economides & Joacim Tåg, *Net Neutrality on the Internet: A Two-Sided Market Analysis* 1 (NET Inst., Working Paper No. 07-45, N.Y. Univ. Law and Econ., Research Paper No. 07-40, 2007), **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1019121** ("[P]latforms sell Internet access services to consumers and may set fees to content and applications providers 'on the other side' of the Internet."). In the search engine context, consumers "pay" by attending to ads, and ad-purchasers pay Google for the chance to get ad viewers' attention.

21 Swire, *supra* note 18.

22 Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151, 1162–64 ("Three components determine an individual consumer's utility from a marketing exposure: (1) the consumer's substantive interest in the marketing, (2) the consumer's nonsubstantive reactions to the marketing exposure, and (3) the attention consumed by evaluating and sorting the marketing. … [A] consumer may derive utility from the rote act of being contacted by marketers or exposed to the marketing, regardless of the marketing content.").

23 David S. Evans, *The Economics of the Online Advertising Industry*, 7 REV. NETWORK ECON. 359, 359 (2008), *available at* www.bepress.com/rne/vol7/iss3/2 (describing how many of the top websites have adopted the "free-tv" model where the publisher generates traffic by not charging for readers but then sell that traffic to advertisers).

Google and DoubleClick argue that the resulting personalized ads serve customers. Their arguments prevailed, and Google officially acquired DoubleClick in 2008.[24]

Antitrust law is ill prepared to handle a "market" where some percentage of consumers consider loss of privacy a gain and others consider it a loss. Economic reasoning in general falters in the face of externalities, but usually we can all agree that, say, pollution is a harm (or negative externality) and flowers are a boon (or positive externality). Privacy preferences are much more idiosyncratic.

Critics of the merger do have a response to this problem of diverse preferences—they can shift from characterizing lost privacy as a cost of web searching to describing it as a reduction in the quality of the services offered by the merging entities.[25] Douglas Kysar's work on the product–process distinction is encouraging here. Kysar has claimed that consumers should have a right to make choices of products based on how the products are made, not just how well they work.[26] Kysar argues "in favor of acknowledging and accommodating [consumer] process preferences within policy analysis, given the potential significance that such preferences may serve in the future as outlets for public-minded behavior."[27] Nevertheless, the valuation problems here are daunting. How are we to determine how much consumers are willing to pay to avoid privacy-eroding companies?[28]

Perhaps, as Lisa Heinzerling and Frank Ackerman suggest in their book *Priceless*, we should stop even trying to pretend that these decisions can be made on

---

24 *See* Press Release, Google Inc., Google Closes Acquisition of DoubleClick (Mar. 11, 2008), *available at* www.google.com/intl/en/press/pressrel/20080311_doubleclick.html.

25 Both Supreme Court precedent and DOJ guidelines support this approach. *See* Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 695 (1978) ("The assumption that competition is the best method of allocating resources in a free market recognizes that all elements of a bargain—quality, service, safety, and durability—and not just the immediate cost, are favorably affected by the free opportunity to select among alternative offers."); U.S. DEP'T OF JUSTICE, HORIZONTAL MERGER GUIDELINES § 4, at 30–32 (1997) (efficient market behavior is indicated by lower prices, new products, and "improved quality").

26 Douglas A. Kysar, *Preferences for Processes: The Process/Product Distinction and the Regulation of Consumer Choice*, 118 HARV. L. REV. 526, 529 (2004) ("[C]onsumer preferences may be heavily influenced by information regarding the manner in which goods are produced.").

27 *Id.* at 534.

28 Christopher Yoo has demanded this kind of accounting in the context of net neutrality. *See* Christopher Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1, 54 (2005) ("There is nothing incoherent about imposing regulation to promote values other than economic welfare. … [but] such a theory must provide a basis for quantifying the noneconomic benefits and for determining when those benefits justify the economic costs.").

anything approaching a purely economic basis.[29] Engaging in a cost–benefit analysis diminishes privacy's status as a right. Though many scholars have compellingly argued for broader foundations for competition law, the mainstream of contemporary antitrust policy in the United States cannot accommodate such concerns. Antitrust's *summum bonum* is the maximization of "consumer welfare," and this measure of efficiency is notoriously narrow.[30] For example, the DOJ was hard pressed to adequately factor in a basic democratic commitment to diverse communicative channels during many media mergers.[31]

Given antitrust doctrine's pronounced tendency to suppress or elide the cultural and political consequences of concentrated corporate power, the Bureau of Competition and the Bureau of Economics within the FTC are ill-equipped to respond to the most compelling issues raised by search engines.[32] The Google–Doubleclick merger proceedings ultimately ended with an overwhelming win for Google at the FTC.[33] This outcome was all but inevitable given the foundations of contemporary antitrust doctrine,[34] and is the logical outgrowth of overreliance on legal economic theory that uncritically privileges market

---

29 Frank Ackerman & Lisa Heinzerling, Priceless: On Knowing the Price of Everything and the Value of Nothing 8–9 (The New Press 2004).

30 *See* Maurice E. Stucke, *Better Competition Advocacy*, 82 ST. JOHN'S L. REV. 951, 1001 (2008) (observing the primacy of allocative efficiency in antitrust analysis). Stucke notes that "[b]ehind allocative efficiency's façade of positivism lie [many] moral questions … ." *Id.* *See also* Julie E. Cohen, *Network Stories*, 70 LAW & CONTEMP. PROBS. 91, 92 (2007) ("What makes the network good can only be defined by generating richly detailed ethnographies of the experiences the network enables and the activities it supports, and articulating a normative theory to explain what is good, and worth preserving, about those experiences and activities.").

31 *See* C. Edwin Baker, *Media Concentration: Giving Up on Democracy*, 54 FLA. L. REV. 839, 857 (2002) ("[T]he dominant antitrust focus on *power over pricing* can be distinguished from *power over the content available for consumer choice.* In the currently dominant paradigm, a merger that dramatically reduced the number of independent suppliers of a particular category of content—say, news or local news or Black activist news—creates no antitrust problem if, as likely, it does not lead to power to raise prices.").

32 *See* STATEMENT OF THE FEDERAL TRADE COMMISSION CONCERNING GOOGLE/DOUBLECLICK, FTC File No. 071-0170 (FTC Dec. 20, 2007), *available at* **http://www.ftc.gov/os/caselist/0710170/071220statement.pdf** [hereinafter STATEMENT OF FTC CONCERNING GOOGLE/DOUBLECLICK] ("Although [privacy concerns] may present important policy questions for the Nation, the sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition.").

33 *Id.*

34 Maurice Stucke describes and critiques this bias in some detail. *See* Stucke, *supra* note 30, at 1031 (describing a "mishmash of neoclassical economic theory, vignettes of zero-sum competition, and normative weighing of the anticompetitive ethereal—deadweight welfare loss—against the conjectures of procompetitive efficiencies" at the core of too much antitrust law and theory). Among his many important contributions to the literature, Stucke makes it clear that competition policy includes far more goals and tactics than antitrust enforcement alone. *Id.* at 987–1008.

outcomes.[35] As long as contemporary doctrine holds that antitrust is singularly focused on the "consumer welfare" a proposed transaction will generate,[36] antitrust policymakers will be unable to address the cultural and political consequences of consolidation in the search industry.

Antitrust challenges to the proposed settlement of a copyright lawsuit by authors and publishers against Google's Book Search program are likely to be similarly constrained.[37] As in the Google-Doubleclick merger, the privacy implications of Google's proposed deal with publishers are profound.[38] Anyone who cares about public input into the future of access to knowledge should approach the potential deal here warily, even if the prospect of constructing a digital Library of Alexandria tempts scholars.[39] As Harvard librarian Robert Darnton has argued, only a naive optimist could ignore the perils of having one profit-driven company effectively entrusted with a comprehensive collection of the world's books.[40]

When publishers challenged Google's book scanning in 2007, many hoped that public interest groups could leverage copyright challenges to Google's book

---

35 Reza Dibadj, *Beyond Facile Assumptions and Radical Assertions: A Case for "Critical Legal Economics*," 2003 UTAH L. REV. 1155, 1161 ("[T]hree of the most basic assumptions to the popular [law & economics] enterprise—that people are rational, that ability to pay determines value, and that the common law is efficient—while couched in the metaphors of science, remain unsubstantiated."). *But see* JAMES R. HACKNEY, JR., UNDER COVER OF SCIENCE: AMERICAN LEGAL–ECONOMIC THEORY AND THE QUEST FOR OBJECTIVITY 164–66 (Duke Univ. Press 2007) (describing the "notable movement to broaden the scope of legal–economic theory under the rubric of socioeconomics").

36 *See* Leegin Creative Leather Prods., Inc. v. PSKS, Inc., 551 U.S. 877, 906 (2007) (acknowledging the economic foundations of U.S. antitrust law).

37 Motoko Rich, *Google and Authors Win Extension for Book Settlement*, N.Y. TIMES, Nov. 9, 2009, at B3, *available at* **www.nytimes.com/2009/11/10/technology/companies/10gbooks.html?_r=1**. The DOJ expressed dissatisfaction with the parties' most recent proposed settlement, as well. *See* Cecilia Kang, *Judge Puts Off Ruling on Google's Proposed Digital Book Settlement*, WASH. POST, Feb. 19, 2010, *available at* www.washingtonpost.com/wp-dyn/content/article/2010/02/18/AR2010021800944.html?hpid=moreheadlines.

38 Electronic Frontier Foundation, Google Book Search Settlement and Reader Privacy, available at **www.eff.org/issues/privacy/google-book-search-settlement** (last visited July 11, 2010). As author Michael Chabon argues, "if there is no privacy of thought — which includes implicitly the right to read what one wants, without the approval, consent or knowledge of others — then there is no privacy, period." *Id.*

39 *See, e.g.*, Diane Leenheer Zimmerman, *Can Our Culture Be Saved? The Future of Digital Archiving*, 91 MINN. L. REV. 989, 990–91 (2007) (looking at the Google Book Search project as a means of saving culture and "explor[ing] whether saving culture and saving copyright can be made compatible goals").

40 Robert Darnton, *The Library in the New Age*, 55 N.Y. REV. BOOKS, June 12, 2008, at 39, *available at* www.nybooks.com/articles/21514.

search program to promote the public interest. Courts could condition a pro-Google fair use finding on universal access to the contents of the resulting database. Landmark cases like *Sony v. Universal*[41] set a precedent for taking such broad public interests into account in the course of copyright litigation.[42] Those who opt out of the settlement may be able to fight for such concessions, but for now the battle centers on challenges to the settlement itself.

Both James Grimmelmann and Pamela Samuelson have suggested several principles and recommendations to guide judicial deliberations on the proposed settlement.[43] Grimmelmann's work has focused primarily on antitrust issues,[44] while Samuelson has concentrated on the concerns of academic authors.[45] Grimmelmann has succinctly summarized the settlement's potential threats to innovation and competition in the market for book indices, and books themselves:

> The antitrust danger here is that the settlement puts Google in a highly privileged position for book search and book sales. … The authors and publishers settled voluntarily with Google, but there's no guarantee they'll offer similar terms, or any terms at all, to anyone else. … [They] could unilaterally decide only to talk to Google.[46]

---

41 Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

42 Frank Pasquale, Breaking the Vicious Circularity: Sony's Contribution to the Fair Use Doctrine, 55 CASE W. RES. L. REV. 777, 790 (2005).

43 *See* Pamela Samuelson, *Google Book Search and the Future of Books in Cyberspace*, 94 MINN. L. REV. (forthcoming, 2010), *available at* **http://digital-scholarship.org/digitalkoans/2010/01/13/google-book-search-and-the-future-of-books-in-cyberspace/** (discussing the "six categories of serious reservations that have emerged about the settlement … reflected in the hundreds of objections and numerous amicus curiae briefs filed with the court responsible for determining whether to approve the settlement.").

44 *See generally* James Grimmelmann, *How to Fix the Google Book Search Settlement*, 12 J. INTERNET L., Apr. 2009, at 1 (arguing that the Google Book Search antitrust case settlement should be approved with additional measures designed to promote competition and protect consumers) [hereinafter Grimmelmann, *Google Book Search Settlement*].

45 Letter from Pamela Samuelson, Richard M. Sherman Distinguished Professor of Law, University of California, Berkeley School of Law, to Hon. Denny Chin, Judge, S.D.N.Y. (Sept. 3, 2009), *available at* www.scribd.com/doc/19409346/Academic-Author-Letter-090309 (urging the judge to condition "approval of the Settlement Agreement on modification of various terms identified herein so that the Agreement will be fairer and more adequate toward academic authors.").

46 James Grimmelmann, *In Google We Antitrust*, TPMCAFÉ BOOK CLUB, Jan. 15, 2009, **http://tpmcafe.talkingpointsmemo.com/2009/01/15/in_google_we_antitrust**.

Grimmelmann proposes several methods of assuring that the publishers will deal with other book search services.[47] Grimmelmann suggests an "[a]ntitrust consent decree" and "[n]ondiscrimination among copyright owners" as potential responses to the issues raised by the settlement.[48] Most of his proposal reflects a policy consensus that presumes competition is the ideal solution to abuses of power online.[49]

Yet there are many reasons why competition is unlikely to arise in book search services, even if the settlement is altered in order to promote it.[50] Licensing costs are likely to be a substantial barrier to entry. A key to competition in the search market is having a comprehensive database of searchable materials; the more these materials need to be licensed, the less likely it is that a second comer can set up its own book archive. As scholars have demonstrated, deals like Google's proposed settlement help entrench copyright holders' claims for licensing revenue.[51] Moreover, innovation in search is heavily dependent on having an installed base of users that effectively "train" the search engine to be responsive.[52] The more search queries an engine gets, the better able it is to sharpen and perfect its algorithm.[53] Each additional user tends to decrease the cost of a better quality service for all subsequent users by contributing activity that helps the search engine differentiate between high and low quality organizational strategies.[54] Thus, incumbents with large numbers of users enjoy

---

47 *Id.*

48 Grimmelmann, *Google Book Search Settlement*, *supra* note 44, at 15.

49 Grimmelmann does also propose some revised terms that would not be primarily designed to incentivize the development of new alternatives to Google Book Search; for example, he proposes "[l]ibrary and reader representation at the [Book Rights R]egistry" that would administer many aspects of the settlement. *Id.*

50 *See* Bracha & Pasquale, *supra* note 5, at 1152 ("Though the market choices of users and technological developments constrain search engine abuse to some extent, they are unlikely to vindicate [certain social] values … ."); Frank Pasquale, *Seven Reasons to Doubt Competition in the General Search Engine Market*, MADISONIAN, Mar. 18, 2009, **http://madisonian.net/2009/03/18/seven-reasons-to-doubt-competition-in-the-general-search-engine-market**.

51 *See* James Gibson, *Risk Aversion and Rights Accretion in Intellectual Property Law*, 116 YALE L.J. 882, 884 (2007) (describing how the decision as to whether to fight for fair use or license a copyrighted work can be difficult "because the penalties for infringement typically include supracompensatory damages and injunctive relief").

52 James Pitkow et al., *Personalized Search*, 45 COMMS. ACM, Sept. 2002, at 50 (discussing methods of personalizing search systems).

53 For example, if 100 people search for "alternatives to Microsoft Word software" on a search engine on a given day and all pick the third-ranked result, the search algorithm may adjust itself and put the third-ranked result as the first result the next day. The most-used search engine will have more data to tweak its algorithms than its less-used rivals.

54 Oren Bracha & Frank Pasquale, *Federal Search Commission: Fairness, Access, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1141, 1181 (2008); David A. Vise & Mark Malseed,

substantial advantages over smaller entrants. Restrictive terms of service also deter competitors who aspire to reverse engineer and develop better versions of such services.[55] In general purpose search, users cannot reproduce, copy, or resell any Google service for *any* reason, even if the behavior is manual and non-disruptive.[56] Another section proscribes "creat[ing] a derivative work of … the Software."[57] Advertisers face other restrictions, as Google's AdWords Application Programming Interface (API) Terms & Conditions "impede advertisers' efforts to efficiently copy their ad campaigns to other providers."[58] All of these factors militate against robust competition in the comprehensive book search field.

Quantum leaps in technology capable of overcoming these brute disadvantages are unlikely, particularly because search is as much about personalized service as it is about technical principles of information organization and retrieval.[59] Current advantage in search is likely to be self-reinforcing, especially given that so many more people are using the services now than when Google overtook other search engines in the early 2000s.[60]

What does an online world featuring an entrenched Google Book Search as gatekeeper look like? Initially, it will prove a vast improvement on the status

---

The Google Story 215 (2005) (noting that the most-used search engine will have more data to tweak its algorithms than its less-used rivals. ). (

55 Though the precise terms of service of Google Book Search have not been finalized, Google's more general terms of service are not promising. Google's terms of service prohibit any action that "interferes with or disrupts" Google's services, networks, or computers. Google Inc., Terms of Service § 5.4 (Apr. 16, 2007), www.google.com/accounts/TOS. Repeated queries to the service necessary to gather data on its operations may well violate these terms.

56 *Id.* § 5.5.

57 *Id.* § 10.2. Section 5.3 would proscribe both the automatic data collection and the use of a nonapproved "interface" for accessing Google's database, regardless of the exact means. *Id.* § 5.3.

58 Ben Edelman, *PPC Platform Competition and Google's 'May Not Copy' Restriction*, June 27, 2008, **http://www.benedelman.org/news/062708-1.html** (arguing that "Google's restrictions on export and copying of advertisers' campaigns … hinder competition in Internet advertising"). Though the hearing at which Professor Edelman was to testify was cancelled, he has documented these problems in some detail at his website, www.benedelman.org.

59 John Battelle, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE 8 (2005).at 8 (describing how personalized search enhances the value of search engines to both users and advertisers). Due to trade secrecy, it is impossible for policymakers to discover how much of the intermediary's success is due to its employees' inventive genius, and how much is due to the collective contributions of millions of users to the training of the intermediary's computers.

60 *See* Randall Stross, Planet Google: One Company's Audacious Plan to Organize Everything We Know 98 (Free Press 2008) (describing success of YouTube, a subsidiary of Google).

quo of bulky, hard-to-acquire, physical copies of books. But when we consider the ways in which knowledge can be rationed for profit, or structured to promote political ends, some worries arise. Google plans to monetize the book search corpus, and one predictable way of increasing its value is to make parts of it unavailable to those unwilling to pay high licensing fees. If the settlement allowed Google to charge such fees in an unconstrained manner, unmoored from the underlying costs of operating the project, the company would essentially be exploiting a public easement (to copy books) for unlimited private gain.[61] The Open Content Alliance has questioned the restrictive terms of the contracts that Google strikes when it agrees to scan and create a digital database of a library's books.[62] Those restrictive terms foreshadow potential future restrictions on book search services. The proposed deal raises fundamental questions about the proper scope of private initiative in organizing and rationing access to knowledge.

Well-funded libraries may pay a premium to gain access to all sources; lesser institutions may be granted inferior access. If permitted to become prevalent, such tiered access to information could rigidify and reinforce existing inequalities in access to knowledge.[63] Information tiering inequitably disadvantages many groups, promoting the leveraging of wealth into status, educational, or other occupational advantage. Information is not only intrinsically valuable, but also can be a positional good, useful for scoring advantages over others.[64]

---

61 Writers' Reps and Richard A. Epstein Objection filed with the Southern District of New York in re Google Book Search, available at **http://www.writersreps.com/feature.aspx?FeatureID=172** (arguing that the Google Book Search Settlement "would accomplish[] orphan legislation—but just for Google. … If [Google] is to be handed exclusive possession after stealing the scans to begin with, then it should be required to share those scans.").

62 *See* Open Content Alliance, Let's Not Settle for This Settlement, www.opencontentalliance.org/2008/11/05/lets-not-settle-for-this-settlement (last visited Mar. 12, 2010) ("At its heart, the settlement agreement grants Google an effective monopoly on an entirely new commercial model for accessing books. It re-conceives reading as a billable event. This reading event is therefore controllable and trackable. It also forces libraries into financing a vending service that requires they perpetually buy back what they have already paid for over many years of careful collection.").

63 Frank Pasquale, *Technology, Competition, and Values*, 8 MINN. J. L. SCI. & TECH. 607, 608 (2007) (explaining how "much technology is used not just simply to improve its user's life, but also to help its user gain advantage over others"). For example, "[t]est-preparation technologies … creat[e] inequalities; students able to afford test-preparation courses, such as those offered by Kaplan, have a definite advantage over those who do not have access to such courses." *Id.* at 615 (internal citation omitted).

64 Harry Brighouse & Adam Swift, *Equality, Priority, and Positional Goods*, 116 ETHICS 471, 472 (2006) ("[Positional goods] are goods with the property that one's relative place in the distribution of the good affects one's absolute position with respect to its value. The very fact that one is worse off than others with respect to a positional good means that one is

Admittedly, Google Book Search has so far proven a great resource for scholars. It has made "book learning accessible on a new, worldwide scale, despite the great digital divide that separates the poor from the computerized."[65] Current access to knowledge is stratified in many troubling ways; the works of John Willinsky[66] and Peter Suber[67] identify many troubling current forms of tiering that pale before the present impact of Google Book Search.[68] Given the aggressive pricing strategies of many publishers and content owners, Google Book Search is a vital alternative for scholars.

Nevertheless, there is no guarantee in the current version of the settlement that Google Book Search will preserve its public-regarding features.[69] It may well end up like the powerful "group purchasing organizations" in the American health care system that started promisingly, but have evolved to exploit their intermediary role in troubling ways.[70] Google is more than just one among many online service providers jostling for a competitive edge on the web. It is likely to be the key private entity capable of competing or cooperating with academic publishers and other content providers. Dedicated monitoring and regulation of the settlement terms now could help ensure that book digitization

---

worse off, in some respect, than one would be if that good were distributed equally. So while it might indeed be perverse to advocate leveling down all things considered, leveling down with respect to positional goods benefits absolutely, in some respect, those who would otherwise have less than others.

65 Darnton, *supra* note 40, at 76.

66 JOHN WILLINSKY, THE ACCESS PRINCIPLE: THE CASE FOR OPEN ACCESS TO RESEARCH AND SCHOLARSHIP 5 (The MIT Press 2005) (describing extreme "digital divide" between those most connected to information resources and those cut off from them).

67 *See generally* Peter Suber, Open Access News, www.earlham.edu/~peters/fos/fosblog.html. Suber is a leader of the open access movement, which aims to "[p]ut[] peer-reviewed scientific and scholarly literature on the internet[,] [m]ak[e] it available free of charge and free of most copyright and licensing restrictions[,] [and] remov[e] the barriers to serious research." *Id.*

68 *See id.* (chronicling on a daily basis news and controversies related to open access to scholarly materials on the Internet).

69 Siva Vaidhyanathan, *Baidu.com Accused of Rigging Search*, The Googlization of Everything, Global Google, Jan. 2009, **http://www.googlizationofeverything.com/2009/01/baiducom_accused_of_rigging_se.php** (Feb. 19, 2009, 14:20 EST) ("'Public failure' [is a] phenomenon in which a private firm steps into a vacuum created by incompetent or gutted public institutions. A firm does this not for immediate rent seeking or even revenue generation. It does so to enhance presence, reputation, or to build a platform on which to generate revenue later or elsewhere. It's the opposite of 'market failure.' And it explains a lot of what Google does.").

70 For background on group purchasing organizations, *see* S. PRAKASH SETHI, GROUP PURCHASING ORGANIZATIONS: AN UNDISCLOSED SCANDAL IN THE U.S. HEALTH CARE INDUSTRY 122 (Palgrave MacMillan 2009) ("The benefits of combined purchases would be greatly reduced in conditions where the middlemen … control the entire process through restrictive arrangements with suppliers and customers.").

protects privacy, diverse stakeholder interests, and fair pricing of access to knowledge. Alliances between Google Book Search and publishers deserve public scrutiny because they permit private parties to take on what have often been public functions of determining access to and pricing of information. Where "regulatory copyright"[71] has answered such questions with compulsory licenses,[72] the new alliances aspire to put into place a regime of cross-subsidization resistant to public scrutiny or input.[73] Given the vital public interests at stake in the development of this information infrastructure, monitoring is vital.[74] Extant law provides little assurance that it will actually occur.

## A Public Alternative?

In other work, I have proposed a number of regulations that would permit either government or public accountability groups to monitor search engines to detect abuses of their dominant position. To conclude this piece, I would like to raise one other alternative: a publicly funded search engine.

To the extent that search engines resist monitoring and accountability, governments should consider establishing public alternatives to them. Here, lessons from recent debates over health insurance may be instructive. There are structural parallels between the intermediary role of private health insurers (which stand as a gatekeeper between patients and providers of health products and services) and that of search engines (which stand between searchers and

---

71 *See* Joseph P. Liu, *Regulatory Copyright*, 83 N.C. L. REV. 87, 91 (2004) (describing the growth and scope of compulsory licensing statutes that provide for compensation for copyright holders while denying them the right to veto particular uses of their work).

72 Marybeth Peters, the U.S. Register of Copyrights, has objected to the proposed Google Books Settlement on the grounds that it would violate traditional norms of separation of powers in copyright policy. *See Hearing on Competition and Commerce in Digital Books: The Proposed Google Book Settlement Before the House Comm. on the Judiciary*, 111th Cong. (2009) (statement of Marybeth Peters, Register of Copyrights), *available at* **http://judiciary.house.gov/hearings/pdf/Peters090910.pdf**, at 2 ("In the view of the Copyright Office, the settlement proposed by the parties would encroach on responsibility for copyright policy that traditionally has been the domain of Congress. … We are greatly concerned by the parties' end run around legislative process and prerogatives, and we submit that this Committee should be equally concerned.").

73 Google considers its pricing and ranking decisions a closely held trade secret—an assertion that would seem very strange if it came from a public library. *See* Pamela Samuelson, *Google Books Is Not a Library*, THE HUFFINGTON POST, Oct. 13, 2009, **www.huffingtonpost.com/pamela-samuelson/google-books-is-not-a-lib_b_317518.html** ("Libraries everywhere are terrified that Google will engage in price-gouging when setting prices for institutional subscriptions to [Google Book Search] contents.").

74 Frank Pasquale, *Beyond Competition and Innovation: The Need for Qualified Transparency in Internet Intermediaries*, 104 Nw. U. L. REV. 105 (2010) (offering proposals for monitoring internet intermediaries).

providers of information). The 1965 decision to establish Medicare as a public option for an elderly population ill-served by private providers and insurers may prove a model for an information economy plagued by persistent digital divides.

As the United States debated health reform from 2009 to 2010, there was a tension between regulation-focused approaches (which would require revelation and alteration of private insurers' unfair practices) and a public option that would compete with existing insurers. Democrats ultimately gave up on pushing the public option, but the debate exposed the many positive aspects a state-sponsored alternative can provide in certain markets. A public option could play a role in search parallel to the role that Medicare plays in the health system: guaranteeing some baseline of transparency in pricing and evaluation.[75]

The recent Google Book Search settlement negotiations have led Siva Vaidhyanathan to characterize Google's archive project as evidence of a "public failure."[76] Whereas government intervention is often necessary in cases of "market failure," Vaidhyanathan argues that the reverse can occur: market actors can step into a vacuum where government should have been. In the case of digitized books, the problem is presented starkly: Why has the Library of Congress failed to require *digital* deposit of books, instead of merely accepting paper copies? We can debate when such a requirement became plausible; however, had the government required such deposit as soon as it became feasible, the problematic possibility of a Google monopoly here would be much less troubling. If digital deposit ever is adopted, the government could license its corpus to alternative search services. There is no good reason why the company that is best capable of reproducing books (and settling lawsuits based on that reproduction) should have a monopoly on search technologies used to organize and distribute them.

More ambitiously, an NGO or quasi-administrative NGO could undertake to index and archive the web, licensing opportunities to search and organize it to various entities that promise to maintain open standards for ranking and rating websites and other Internet presences.[77] Wikipedia, Slashdot, and eBay all

---

75 For more on the role of public options like Medicare in the modern medical sector, *see* Frank Pasquale*, Making the Case for the Public Plan, Part II: Public Option as Private Benchmark*, July 15, 2009, available at **http://balkin.blogspot.com/2009/06/making-case-for-public-plan-part-ii.html**.

76 Vaidhyanathan, *supra* note 69. (" 'Public failure' [is a] phenomenon in which a private firm steps into a vacuum created by incompetent or gutted public institutions. A firm does this not for immediate rent seeking or even revenue generation. It does so to enhance presence, reputation, or to build a platform on which to generate revenue later or elsewhere. It's the opposite of 'market failure.' And it explains a lot of what Google does.").

77 For a cultural case for government intervention here, see Mário J. Silva, *The Case for a Portuguese Web Search Engine*, **http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBUQFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.106.**

suggest methods of evaluating relevance and authority that could be employed by public, open search engines. If such a search engine became at least somewhat popular (or popular within a given niche), it could provide an important alternative source of information and metadata on ranking processes.

The need for a public option in search becomes even more apparent when we consider the waste and inefficiency caused by opaque intermediaries in other fields. Like private health insurers, Google is a middleman, standing between consumers and producers of knowledge. In programs like Book Search, it will effectively collaborate with copyright owners to determine what access people get, how much they have to pay, and on what terms. In the health field, providers and private insurers are both very concentrated in the U.S., and consumers (*i.e.*, the businesses and individuals who buy insurance plans) are not. Insurers and providers also jealously guard the secrecy of many pricing decisions.[78] That is one key reason why the U.S. spends so much more on health care than other industrialized nations, without getting consistently better results, access, or quality.

Health care reformers often split into two camps: those who believe that regulation of middlemen like insurers can bring about fair results, and those who believe that only a public option can serve as a benchmark for judging the behavior of private insurers. The Patient Protection and Affordable Care Act (PPACA) of 2010 decisively opted for the regulatory option, and the early stages of its implementation have been rocky. The constitutional challenges to search engine regulation would likely prove more serious than the many lawsuits now attacking PPACA. Therefore, even if the public option in health care is off the table now, it should inspire future proposals in information policy, where regulation of intermediaries may be even more difficult than it has proven to be in health care. If search engines consistently block or frustrate measures to increase their accountability, public alternatives could prove to be an indispensable foundation of a fair, just, and open information environment.

---

**5334%26rep%3Drep1%26type%3Dpdf&ei=IWZYTJbaCoKC8gapvY2xCw&usg=AFQjCNHdTPpTBUuNHZhTOZtGaRiVKP6C4g&sig2=9aoaKLXiXOOUuYHMewopVQ** (describing the value of a Portuguese-oriented search engine); JEAN NOEL JENNENY, GOOGLE AND THE MYTH OF UNIVERSAL KNOWLEDGE: A VIEW FROM EUROPE (Univ. of Chicago Press 2007). Whereas these authors believe that English-language bias is a particularly problematic aspect of Google's hegemony in the field, I argue that the possibility of many kinds of hidden bias counsel in favor of at least one robust, publicly funded alternative.

78 *See, e.g.*, Uwe Reinhart, *The Pricing of U.S. Hospital Services: Chaos Behind a Veil of Secrecy*, at **http://healthaff.highwire.org/cgi/content/abstract/25/1/57**; Annemarie Bridy, *Trade Secret Prices and High-Tech Devices: How Medical Device Manufacturers are Seeking to Sustain Profits by Propertizing Prices*, 17 TEX. INTELL. PROP. L.J. 187 (2009) (discussing "recent claims by the medical device manufacturer Guidant that the actual prices its hospital customers pay for implantable devices, including cardiac pacemakers and defibrillators, are protectable as trade secrets under the Uniform Trade Secrets Act.").

# The Problem of Search Engines as Essential Facilities: An Economic & Legal Assessment

By Geoffrey A. Manne*

What is wrong with calls for search neutrality, especially those rooted in the notion of Internet search (or, more accurately, Google, the policy scolds' bête noir of the day) as an "essential facility," and necessitating government-mandated access? As others have noted, the basic concept of neutrality in search is, at root, farcical.[1] The idea that a search engine, which offers its users edited access to the most relevant websites based on the search engine's assessment of the user's intent,[2] should do so "neutrally" implies that the search engine's efforts to ensure relevance should be cabined by an almost-limitless range of ancillary concerns.[3]

Nevertheless, proponents of this view have begun to adduce increasingly detail-laden and complex arguments in favor of their positions, and the European Commission has even opened a formal investigation into Google's practices, based largely on various claims that it has systematically denied access to its top search results (in some cases paid results, in others organic results) by competing services,[4] especially vertical search engines.[5] To my knowledge, no

---

* Executive Director, International Center for Law & Economics and Lecturer in Law, Lewis & Clark Law School. **www.laweconcenter.org**; **www.lclark.edu/law/faculty/geoffrey_manne**.

1 *See, e.g.*, Danny Sullivan, *The Incredible Stupidity of Investigating Google for Acting Like a Search Engine*, SEARCH ENGINE LAND, **http://searchengineland.com/the-incredible-stupidity-of-investigating-google-for-acting-like-a-search-engine-57268** ("A search engine's job is to point you to destination sites that have the information you are seeking, not to send you to other search engines. Getting upset that Google doesn't point to other search engines is like getting upset that the New York Times doesn't simply have headlines followed by a single paragraph of text that says 'read about this story in the Wall Street Journal.'").

2 A remarkable feat, given that this intent must be inferred from simple, context-less search terms.

3 Perfectly demonstrated by Frank Pasquale's call, elsewhere in this volume, for identifying search engines as "essential cultural and political facilities," thereby mandating incorporation into their structure whatever "cultural" and "political" preferences any sufficiently-influential politician (or law professors) happens to deem appropriate.

4 Competing services include, for example, MapQuest (**www.mapquest.com**) (competing with Google Maps), Veoh (**www.veoh.com**) (competing with You Tube) and Bing Shopping (**www.bing.com/shopping**) (competing with Google Products).

5 Vertical search engines are search engines that focus on a particular category of products, or on a particular type of search. Examples include Kayak (**www.kayak.com**) (travel search),

one has yet claimed that Google should offer up links to competing general search engines as a remedy for its perceived market foreclosure, but Microsoft's experience with the "Browser Choice Screen" it has now agreed to offer as a consequence of the European Commission's successful competition case against the company is not encouraging.[6] These more superficially sophisticated claims are rooted in the notion of Internet search as an "essential facility"—a bottleneck limiting effective competition.

These claims, as well as the more fundamental harm-to-competitor claims, are difficult to sustain on any economically-reasonable grounds. To understand this requires some basic understanding of the economics of essential facilities, of Internet search, and of the relevant product markets in which Internet search operates.

## The Basic Law & Economics of Essential Facilities

There are two ways to deal with a problematic bottleneck: Remove the bottleneck or regulate access to it. The latter is the more common course adopted in the U.S. and elsewhere. Complex, Byzantine and often counter-productive regulatory apparatuses are required to set and monitor the terms of access. Among other things, this paves the way for either intensely-problematic judicial oversight of court-imposed remedies or else the creation of sector-specific regulatory agencies subject to capture, political influence, bureaucratic inefficiency, and inefficient longevity. The Interstate Commerce Commission (and its successor agencies within the Department of Transportation) and the Federal Communications Commission (and its implementation beginning in 1996 of the monstrous Telecommunications Act) in the U.S. are paradigmatic examples of these costly effects, and it is certainly questionable whether the disease is worse than the cure.[7]

Obviously, an essential facility must be *essential*. Efforts over the years to shoehorn various markets into this category have sometimes strained credulity, as it has variously been claimed that Aspen, Colorado ski hills,[8] local voice mail

---

SourceTool (**www.sourcetool.com**) (business input sourcing), and Foundem (**www.foundem.com**) (retail product search and price comparison).

6 *See* European Commission, *Web browser choice for European consumers*, **http://ec.europa.eu/competition/consumers/web_browsers_choice_en.html** (last accessed Dec. 8, 2010).

7 Oren Bracha and Frank Pasquale's call for a "Federal Search Commission" modeled on the Federal Trade Commission is in fact an *embrace* of the need for a bureaucratic apparatus to regulate the forced access called for by search neutrality proponents. *See* Oren Bracha and Frank Pasquale, *Federal Search Commission: Fairness, Access, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1193 (2008).

8 Aspen Highlands Skiing Corp. v. Aspen Skiing Co., 738 F.2d 1509 (10th Cir. 1984), aff'd on other grounds, 472 U.S. 585 (1985).

services,[9] soft drinks[10] and direct freight flights between New York and San Juan[11] (among many other things) were essential facilities necessitating mandated access under the antitrust laws.[12] In these and many other cases, myriad alternatives to the allegedly-monopolized market exist and it is arguable that there was nothing whatsoever "essential" about these markets.

In antitrust literature and jurisprudence, a plaintiff would need to prove the following to prevail in a monopolization case rooted in the essential facilities doctrine:

1. Control of the essential facility by a monopolist;

2. A competitor's inability practically or reasonably to duplicate the essential facility;

3. The denial of the use of the facility to a competitor; and

4. The feasibility of providing the facility to competitors.[13]

Arguably, since the Supreme Court's 2004 *Trinko* decision,[14] a plaintiff would also need to demonstrate the absence of federal regulation governing access. The *Trinko* decision significantly circumscribed the area subject to essential facilities arguments, limiting such claims to instances where, as in the *Aspen Skiing* case, a competitor refuses to deal on reasonable terms with another competitor with whom it has, in fact, dealt in the past.[15]

A key problem with many essential facilities cases is the non-essentiality of the relevant facility. While there can be no doubt that to particular competitors, particularly those constrained to only one avenue of access to consumers by geography or natural monopoly, a facility may indeed seem essential, the touchstone of U.S. antitrust law has long been consumer, not competitor, welfare. So while, indeed, Aspen Highlands may have had difficulty competing with the Aspen Ski Company for consumers who had already chosen to ski in Aspen, consumers nonetheless had unfettered access to a wide range of alternative ski (and other vacation) destinations, such that the likelihood of the

---

9 CTC Communications Corp. v. Bell Atlantic Corp., 77 F. Supp. 2d 124 (D. Me. 1999).

10 Sun Dun v. Coca-Cola Co., 740 F. Supp. 381 (D. Md. 1990).

11 Century Air Freight, Inc. v. American Airlines, Inc., 597 F. Supp. 564 (S.D.N.Y. 1984).

12 For a more complete list of essential facilities (and attempted essential facilities) cases, as well as an important treatment of the essential facilities doctrine in US antitrust law, see Abbott B. Lipsky, Jr. & J. Gregory Sidak, *Essential Facilities*, 51 STAN. L. REV. 1187 (1999).

13 MCI Comm'ns Corp. v. American Tel. & Tel. Co., 708 F.2d 1081 (7th Cir. 1982).

14 Verizon Comm'ns. v. Law Offices of Curtis V. Trinko LLP, 540 U.S. 398 (2004).

15 *See*, e.g., PHILLIP E. AREEDA & HERBERT HOVENKAMP, ANTITRUST LAW (2004 supp.) at 199.

monopolization of Aspen's ski hills affecting overall consumer welfare was essentially non-existent.[16] In such a circumstance, should it matter if a particular competitor is harmed? Is that a function of antitrust-relevant conduct on the part of another firm, or an unfortunate set of business decisions on the part of the first firm?

As Phillip Areeda and Herbert Hovenkamp have famously said of the essential facilities doctrine, "[it] is both harmful and unnecessary and should be abandoned."[17] As another antitrust expert has described it:

> At bottom, a plaintiff making an essential facilities argument is saying that the defendant has a valuable facility that it would be difficult to reproduce, and suggesting that is a reason for a court to intervene and impose a sharing duty. But at least in the vast majority of the cases, the fact that the defendant has a highly valued facility is a reason to *reject* sharing, not to *require* it, since forced sharing "may lessen the incentive for the monopolist, the rival, or both to invest in those economically beneficial facilities."[18]

This perennial problem—antitrust laws being used to protect competitors rather than consumers—lies at the heart of claims surrounding Internet search as an essential facility.

There is much tied up in the argument, and proponents have often been careful to at least go through the motions of drawing the rhetorical line back to consumers. In its fullest expression, it is claimed that harm to competitors now will mean the absence of competitors later and thus an unfettered monopoly with the intent and power to harm consumers.[19] It is also often argued that consumers (in this case Internet users searching for certain websites or the products they sell) are intrinsically harmed by the unavailability of access to the information contained in sites that are denied access to the search engine's "essential facility."[20]

---

16 The courts, however, did not agree.

17 3A AREEDA & HOVENKAMP, ANTITRUST LAW ¶ 771c, at 173 (2002).

18 R. Hewitt Pate, *Refusals to Deal and Essential Facilities*, Testimony Submitted to DOJ/FTC Hearings on Single Firm Conduct, Jul. 18, 2006, *available at* **http://www.justice.gov/atr/public/hearings/single_firm/docs/218649.htm** (quoting *Trinko*, 540 U.S.. at 408).

19 *See, e.g., European Commission Launches Antitrust Investigation of Google*, SEARCH NEUTRALITY.ORG, Nov. 30, 2010, **http://www.searchneutrality.org** ("Google is exploiting its dominance of search in ways that stifle innovation, suppress competition, and erode consumer choice."). Meanwhile, complainants have gone to Europe where a showing of consumer harm is not necessary to prevail under its competition laws.

20 As Oren Bracha and Frank Pasquale put it, "Search engines, in other words, often function not as mere satisfiers of predetermined preferences, but as shapers of preferences," *Federal Search Commission*, 93 CORNELL L. REV. at 1185. Bracha and Pasquale also claim that "Market participants need information about products and services to make informed economic

The basic essential facilities case against Google is that it controls a bottleneck for the Internet—it is the access point for most consumers, and search results on Google determine which websites are successful and which end up in oblivion.[21] More particularly, it is argued that Google has used its control over this bottleneck to deny access by competitors to Google's users. To understand this requires a brief discussion of the economics relevant to Internet Search and its relevant market.

## The Basic Economics of Internet Search

Implicit in claims that Google controls access to an essential facility is that access by some relevant set of consumers (or competitors) to relevant content is accessible only (or virtually only) through Google. It is necessary, then, to assess whether Google's search results pages are, in fact, without significant competition for the economic activity at their heart. Of course the economic activity at their heart is advertising.[22]

It is hard to conceive of Internet search—let alone Google's website—as the only means of reducing search costs for potential consumers (Internet searchers) and prospective sellers. Leaving aside the incredible range of alternative sources to the Internet for commerce,[23] off the top of my head, I can imagine Google's competitor websites finding access to users by 1) advertising in print publications and TV; 2) using social networking sites to promote their sites, 3) being linked to by other websites including sites specializing in rating websites, online magazines, review sites, and the like; 4) implementing affiliate programs or other creative marketing schemes; 5) purchasing paid advertising, both in Google's own paid search results, as well as on other, heavily-trafficked websites; and 6) securing access via Google's general search competitors like Yahoo! and Bing. Competitors denied access to the top few search results at

---

decisions. … [A]ttaining visibility and access to users is critical to competition and cooperation online. Centralized control or manipulation by search engines may stifle innovation by firms relegated to obscurity." *Id.* at 1173-74.

21 *Id.* at 1173 ("Concentrated control over the flow of information, coupled with the ability to manipulate this flow, may reduce economic efficiency by stifling competition.").

22 *See* KEN AULETTA, GOOGLED: THE END OF THE WORLD AS WE KNOW IT 16 (2009) (quoting Google CEO Eric Schmidt as saying, "We are in the advertising business").

23 There is a tendency for Web sites to view their Internet enterprises as different than their offline counterparts', but, at root, most Internet sites (other than branded ones attached directly to offline stores) are founded by entrepreneurs who made a simple business decision to ply their trade online rather than off. That this decision may have foreclosed easy access to certain offline customers, or put the entrepreneur in a position where access to customers could be frustrated by certain competitive disadvantages specific to the Internet, does not convert these competitive disadvantages into special problems deserving of antitrust treatment. To do so would be to inappropriately and inefficiently insulate the online/offline business decision from the healthy effects of Schumpeter's "perennial gale of creative destruction." JOSEPH SCHUMPETER, THE PROCESS OF CREATIVE DESTRUCTION (1942).

Google's site are still able to advertise their existence and attract users through a wide range of other advertising outlets—extremely wide, in fact: According to one estimate Google was responsible in 2007 for only about 7.5% of the world's advertising.[24]

For Google to profit from its business—whether as a monopolist or not—it must deliver up to its advertisers a set of users. Interestingly, users of Google's general search engine are mostly uninterested in the paid results. They click through the unpaid or "organic" search results by a wide margin ahead of paid results.[25] There is thus an asymmetry. On one side of its platform are advertisers who care about the quantity and quality (the likelihood that users who see an ad will click through to advertisers' sites and purchase something while there) of the users on the other side. Meanwhile, users care very little about the quantity of advertisers and care only somewhat about the quality of advertisers (preferring greater relevance to lesser, but frequently ignoring paid results anyway). Nevertheless, the core of this enterprise is search result relevance. Greater relevance improves the quality of searchers from the advertisers' point of view, ensuring that advertisers' paid results are clicked on by the users most likely to find the advertiser's site of interest and to purchase something there.

But there are problems inherent in the ambiguity of search terms and the ability to "game the system" that prevent even the most sophisticated algorithms from offering up perfect relevance. First, search terms are often context-less, and a user searching for "jaguar" may be searching for information on the car company, the operating system, the big cat, or something else.[26] Along a different dimension, a user searching for "Nikon camera" might be looking to *buy* a Nikon camera or might be looking for a *picture* of a Nikon camera to post on his blog. Obviously advertisers care very much which of these users clicks on their paid result. At the same time, many undesirable websites (spam sites and the like) can and do take advantage of predictable search results to occupy desirable search result real estate to the detriment of the search engine, its users and its advertisers. Efforts to keep these sites out of the top results and to ensure maximum relevance from ambiguous search terms require a host of algorithm tweaks and even human interventions. That these may (intentionally or inadvertently) harm some websites' rank in certain search results is consistent with a well-functioning search platform.

---

24 *See* Erick Schonfeld, *Estimates Put Internet Advertising at $21 Billion in U.S., $45 Billion Globally*, TECHCRUNCH, Feb. 26, 2008, **http://techcrunch.com/2008/02/26/estimates-put-internet-advertising-at-21-billion-in-us-45-billion-globally/**.

25 *See, e.g.*, Neil Walker, *Google Organic Click Through Rate (CTR)*, UK SEO CONSULTANT, May 11, 2010, **http://www.seomad.com/SEOBlog/google-organic-click-through-rate-ctr.html**.

26 *See* Bill Slawski, *A Look at Google Midpage Query Refinements*, SEO BY THE SEA, Apr. 20, 2006, **http://www.seobythesea.com/?p=174**.

Google offers its organic search results and its other services as a solution to the two-sided platform problem mentioned above: In order to attract paying advertisers, Google also has to attract (and match up) the advertisers' target audience. Google offers everything it does to its users in an effort to attract these users and to glean information from them that facilitates its all-important matching (relevance) function. In the process, Google generates revenue from advertisers eager to "sell" to this audience. For a host of reasons, Google (like all search engines) does not charge searchers to access its various services, but it does charge advertisers. Just because search is an ancillary business to Google's true advertising business does not necessarily mean it is not a relevant market for purposes of antitrust analysis; nevertheless it is essential to avoid the pitfall of examining one side of a two-sided market in isolation. As David Evans notes, "[t]he analysis of either side of a two-sided platform in isolation yields a distorted picture of the business."[27] Two-sided market definition is complex, and little understood—especially by non-experts throwing around various alleged markets in which companies like Google are said to be "dominant."

There is actually substantial reason to doubt the propriety of a narrow market definition limited to online search advertising.[28] Even where there are different purposes for different types of advertising—*e.g.* brand recognition for display ads and efforts to sell for search ads and other outlets like coupons—this is merely a difference in degree. Both are fundamentally forms of reducing the costs of a user's search for a product, as we have understood since George Stigler's seminal work on the subject in 1968,[29] and the relevant question is whether the difference is significant enough to render decisions in one market essentially unaffected by decisions or prices in the other.

There is evidence that advertisers view online and offline advertising as substitutes, and this applies not only to traditional advertisers but also Internet companies. Thus, in 2009, Pepsi decided not to advertise during the 2010 Super Bowl, in order to focus instead on a particular type of online campaign. "This year for the first time in 23 years, Pepsi will not have ads in the Super Bowl telecast …. Instead it is redirecting the millions it has spent annually to the

---

27 David S. Evans, *Two-Sided Market Definition,* ABA SECTION OF ANTITRUST LAW, MARKET DEFINITION IN ANTITRUST: THEORY AND CASE STUDIES (forthcoming), available at **http://ssrn.com/abstract=1396751** at p. 9.

28 Readers interested in a fuller treatment of the market definition question surrounding Google are directed toward Geoffrey A. Manne & Joshua D. Wright, *Google and the Limits of Antitrust: The Case Against the Case Against Google*, 34 HARV. J. L. & PUB. POL'Y 1 (2011) (forthcoming), from which much of the discussion of Google's markets and economics in this essay is drawn.

29 GEORGE JOSEPH STIGLER, THE ORGANIZATION OF INDUSTRY 201 (Univ. of Chi. Press 1983) (1968).

Internet."[30] And even Google itself advertises offline.[31] Another study suggests that there is indeed a trade-off between online and more traditional types of advertising: Avid Goldfarb and Catherine Tucker have demonstrated that display advertising pricing is sensitive to the availability of offline alternatives.[32] And of course companies have limited advertising budgets, distributed across a broad range of media and promotional efforts. As one commentator notes: "By 2011 web advertising in the United States was expected to climb to sixty billion dollars, or 13 percent of all ad dollars. This meant more dollars siphoned from traditional media, with the largest slice probably going to Google."[33]

Advertising revenue on the Internet is driven initially by the size of the audience, with a significant multiplier for the likelihood that those consumers will purchase the advertisers' products[34] (based on a viewer's propensity to "click through" to the advertiser's site). Google's competition in selling ads thus comes, in varying degrees, not only from other search sites, but also from any other site that offers a service, product, or experience that consumers might otherwise find in Google's "organic" search results, for which Google is not paid. For Google's competitors, this means seeking forced access to its users. But access to eyeballs can be had from a large range of access points around the Web.

Social media sites like Twitter and Facebook are therefore significant access points, occupying, as they do, a considerable amount of Internet "eyeball" time. The Pepsi deviation of advertising revenue from the Super Bowl to the Internet is not likely to have inured much to Google's benefit as the strategy was a "social media play," building on the expressed brand loyalties and peer communications that propel social media.[35] In a world of scarce advertising dollars and effective marketing via social media sites, Google and all other advertisers, online and off, must compete with the growing threat to their revenue from these still-novel marketing outlets. "If Facebook's community of

---

30 Larry D. Woodard, *Pepsi's Big Gamble: Ditching Super Bowl for Social Media,* ABC NEWS, Dec. 23, 2009, **http://abcnews.go.com/print?id=9402514**.

31 *See* Danny Sullivan, *Google Pushes Chrome Browser Via Newspaper Ads*, SEARCH ENGINE LAND, Nov. 21, 2010, **http://searchengineland.com/google-pushes-chrome-browser-via-newspaper-ads-56600**.

32 Avi Goldfarb & Catherine Tucker, *Search Engine Advertising: Pricing Ads to Context* 96 (NET Institute Working Paper No. 07-23, 2007) *available at* **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021451&rec=1&srcabs=10084**

33 KEN AULETTA, GOOGLED: THE END OF THE WORLD AS WE KNOW IT 16 (2009).

34 David S. Evans, *The Economics of the Online Advertising Industry*, 7 REV. OF NETWORK ECON. 359, 359-60 (2008).

35 *See* Larry D. Woodard, *Pepsi's Big Gamble: Ditching Super Bowl for Social Media,* ABC NEWS, Dec. 23, 2009, **http://abcnews.go.com/print?id=9402514**.

users got more of their information through [the Facebook] network, their Internet search engine and navigator might become Facebook, not Google."[36]

The upshot: To the extent that inclusion in Google search results is about "Stiglerian" search-cost reduction for websites (and it can hardly be anything else), the range of alternate facilities for this function is nearly limitless.

Finally, Google competes not only with other general search engines (and possibly all other forms of advertising) but also with so-called vertical search engines. These are search engines and e-commerce websites with search functionality that specializes in specific content: Amazon in books, music, and other consumer goods; Kayak in travel services; eBay in consumer auctions; WebMD in medical information and products; SourceTool in business-to-business supplies; Yelp in local businesses, and many others. To the extent that Internet users bypass Google and begin their searches at one of these specialized sites (as is increasingly the case), the value to these heavily-trafficked websites from access to Google's users decreases.[37]

Competition from vertical search engines is important because ad click-through rates likely are higher when consumers are actively searching for something to buy—just as search advertising targets consumers who express some interest in a particular search term, the effect is magnified if the searcher can be identified as an immediate consumer. Thus online retailers like CDnow that can establish their own brands and their own navigation channels[38] have a significant advantage in drawing searchers—and advertisers—away from Google: The fact that a consumer is performing a search on a retail site itself conveys important and valuable information to advertisers that is not otherwise available from most undifferentiated Google searches—it certainly increases the chance that the searcher is searching to buy a CD rather than learn something about the singer. Because this "ready-to-buy" traffic is the most valuable, there is a possibility of two separate search markets, with most high-value traffic bypassing general-purpose search engines for product search sites like eBay and Amazon.com, and with Google and other general-purpose search engines serving primarily non-targeted, lower-value traffic. The implication is that, while even relatively small-scale competition may present a potentially significant threat to Google's search business, this threat does not depend on links to these sites from Google's search results. And thus these competitors have a strong,

---

36 KEN AULETTA, GOOGLED: THE END OF THE WORLD AS WE KNOW IT 172–73 (2009).

37 For example, in the thirty days ending on February 23, 2010, less than ten percent of visits to eBay.com originated from a search engine. *See* ALEXA, *eBay.com Site Info*, **http://www.alexa.com/siteinfo/ebay.com**.

38 *See* Donna L. Hoffman & Thomas P. Novak, *How to Acquire Customers on the Web,* HARV. BUS. REV., May–June 2000, at 3, 5, 7. (CDnow was acquired by Amazon.com in 2001.)

independent incentive to develop marketing programs outside of Google's search pages—and there is good reason not to deputize Google in the process.

## Is Google an Essential Facility?

Recall that the basic claim is that Google's competitors are foreclosed from access to Google's desirable (essential) marketing platform and thereby suffer significant harm. Of course from the outset, this has it backwards (and this is a core problem with the essential facilities doctrine as a whole).

If there is a problem, it should be the problem of limited access *by Google's users* to Google's competitors. Sometimes the absence of access by competitors to consumers is the same thing as the absence of access by consumers to competitors, but it depends on how well the market has been defined. In the most fundamental sense Google has precisely zero control over access by consumers (meaning users who use Google to search the Internet) to competitors: Anyone with access to a browser can access any site on the Internet simply by typing its URL into the browser. Perhaps understanding this, proponents of the "Internet search is an essential facility" claim argue that mere access is insufficient, and that consumers are essentially ignorant about the valuable content on the web except by search engines, which are subject to the search engine's editorial control over that access. To the typical Google user, according to this view, Google's competitors are effectively non-existent unless they appear in the top few search results.

Now we are dangerously close to the sort of arbitrary market definition exercise, devoid of the discipline imposed by economics, that identifies an anticompetitive problem by narrowing the market until every company is a monopolist over some small group of consumers. Indeed, one can always define a market by focusing on idiosyncratic preferences or product variations. Justice Fortas decried this type of analysis in his dissent in *Grinnell* (regarding home security systems), and it merits quoting at length:

> The trial court's definition of the "product" market even more dramatically demonstrates that its action has been Procrustean—that it has tailored the market to the dimensions of the defendants. It recognizes that a person seeking protective services has many alternative sources. It lists "watchmen, watchdogs, automatic proprietary systems confined to one site, (often, but not always,) alarm systems connected with some local police or fire station, often unaccredited CSPS [central station protective services], and often accredited CSPS." The court finds that even in the same city a single customer seeking protection for several premises may "exercise its option" differently for different locations. It may choose accredited CSPS for one of its locations and a different type of service for another.

> But the court isolates from all of these alternatives only those services in which defendants engage. It eliminates all of the alternative sources despite its conscientious enumeration of them. Its definition of the "relevant market" is not merely confined to "central station" protective services, but to those central station protective services which are "accredited" by insurance companies.
>
> There is no pretense that these furnish peculiar services for which there is no alternative in the market place, on either a price or a functional basis. *The court relies solely upon its finding that the services offered by accredited central stations are of better quality*, and upon its conclusion that the insurance companies tend to give "noticeably larger" discounts to policyholders who use accredited central station protective services. This Court now approves this strange red-haired, bearded, one-eyed man-with-a-limp classification.[39]

In Internet search as well, complainants imply a market based on the fact that Google offers "better quality" access to a larger set of Internet users than the myriad existing alternatives. But claiming essentiality based on a competitor's relative high quality is deeply problematic.

This point is of great importance in assessing the economics of the essential facilities doctrine generally and its application to Internet search in particular. It is clear, even under a fairly expansive reading of the essential facilities doctrine, that even a monopolist has no duty to subsidize the efforts of a less-effective rival.[40] Arguably the Aspen Skiing case should have been tossed out on this basis. As a practical matter, the Aspen Ski Company, by entering into a joint marketing agreement with its smaller rival, Aspen Highlands, allowed Highlands to take advantage of its markedly larger productivity (both in developing ski terrain and amenities, as well as marketing Aspen as a ski destination). Its subsequent decision to drop Highlands from its marketing program for failing to offer sufficient return on its investment should have been unobjectionable.[41]

Similarly, the explicit claim in cases brought against Google by its allegedly-foreclosed rivals is that these (relatively miniscule) sites should have access to Google's effective and inexpensive marketing tool. But it is by no means clear that Google does or should have this duty to promote its rivals (without compensation to Google, as it happens). This is particularly true when, as discussed above, other modes of access exist for competitors' activities, even if

---

39 *U.S. v. Grinnell Corp.*, 384 U.S. 563, 590-91 (1966) (emphasis added).

40 *See* Olympia Equip. Leasing Co. v. Western Union Tel. Co., 797 F.2d 370 (7th Cir. 1986).

41 *See* KEITH N. HYLTON, ANTITRUST LAW: ECONOMIC THEORY AND COMMON LAW EVOLUTION 205-06 (2003).

these modes of access are of lower quality or higher cost. Particularly where, as here, the alleged bottleneck arises not out of a combination with another firm or firms but out of unilateral conduct (success in the marketplace), the claim that a superior access point among many (inferior) access points should be pried open for the benefit of its competitors is specious.

It is worth noting that an alleged Google competitor, SourceTool, in the TradeComet complaint,[42] has made a version of this argument, alleging that Google once engaged in profitable commerce with SourceTool (by selling SourceTool ads next to Google search results) and then penalized SourceTool to its (Google's) economic detriment.[43] The shape of this argument is a transparent effort to remain under what is left of the essential facilities doctrine following *Trinko*. But notice that even if it is true that Google intentionally ended a profitable arrangement with SourceTool (which is by no means clear), the claim still doesn't pass muster. It is almost impossible that Google could be receiving less revenue from whatever site has replaced SourceTool in the paid search result spots SourceTool once paid for. As a result, even if Google were foregoing a previously-profitable relationship *with SourceTool*, it is not, in fact, suffering any economic harm because another advertiser has stepped into SourceTool's shoes.

Of course the argument that Google's competitors are effectively absent without (guaranteed?) access to Google's top few search results proves too much. There is a scarcity of "top few search results," and any effective search engine must have the ability to ensure that those results are the most relevant possible, as well as that they do not violate various quality, safety, moral or other standards that the search engine chooses to promote. "Forcing [owners of essential facilities] to share access may not enhance consumer welfare."[44] Pure "neutrality" is neither possible nor desirable, and the exclusion of certain websites from these coveted positions should be deemed utterly unpersuasive in making out even a *prima facie* monopolization case against a search engine.

And it is not even the case that SourceTool, Foundem,[45] and other competing websites are absent from Google; it is, however, sometimes the case that these

---

42 Complaint , *TradeComet.Com LLC v. Google, Inc.*, 693 F. Supp. 2d 370 (S.D.N.Y. 2009) (No. 09Civ.1400(SHS)).

43 *Id.* ¶ 8.

44 KEITH N. HYLTON, ANTITRUST LAW: ECONOMIC THEORY AND COMMON LAW EVOLUTION 208 (2003).

45 Foundem is a "vertical search and price comparison" site in the UK. *See* **www.foundem.co.uk**. The company is at the heart of the "search neutrality" debate in Internet search. It has created a website to advocate its views on the neutrality issue at **www.searchneutrality.org**, and its claims are at the heart of the European Commission's investigation of Google. See Foundem's discussion of the EU action and its relationship to Foundem's claims in *European Commission Launches Antitrust Investigation of Google*, SEARCH NEUTRALITY.ORG, Nov. 30, 2010, **http://www.searchneutrality.org**.

sites do not show up in the top few organic search results (and, often at the same time, Google's own competing product search results do). But if access to the top few search results is required to ensure the requisite access sought by Google's competitors, the relevant market has been narrowed considerably, creating a standard that can't possibly be met, no matter how "neutral" a search engine's results.

Meanwhile, if Foundem were to disappear from the face of the Earth, who, other than its investors and employees (and perhaps their landlords), would be harmed? The implicit claim (if an antitrust case is to be made) is that websites like Foundem apply a constraint on Google's ability to extract monopoly rents (presumably from advertisers). But this is a curious claim to make while simultaneously arguing that Google itself is made "better" (as in, searchers are indeed looking for Foundem in searches from which the site may be excluded) by the inclusion of Foundem in its search results (thus, presumably, increasing Google's attractiveness to its users and thus its advertisers), while also claiming that Foundem would cease to exist without access to the top few Google search results.

Google does not sell retail goods, and does not profit directly from its own product search offerings (which compete with Foundem), instead receiving benefit by increasing its customer base and the efficacy (presumably) of paid advertisements on its search pages that include a link to its own price comparison results. It is a remarkably tenuous claim to make that Google profits more by degrading its search results than by improving them. If the contrary claim is really true—if, that is, Google harms itself or its advertisers by intentionally penalizing competing sites like Foundem—then that argument and any evidence for it is absent from the current debate. And, of course, if Google is, as it claims, actually improving its product by applying qualitative decisions to demote sites like Foundem and others that, Google claims, merely re-publish information from elsewhere on the web with precious little original content, then Google's efforts should be seen as a feature and not a bug.

Moreover, the extension of the essential facilities logic to competition between Google and competitors like Foundem, MapQuest or Kayak is extremely problematic. To the extent that Google and Foundem, for example, are competitors, they are competitors not in the advertising space but rather in the "information dissemination and retail distribution channel" space. I'm not sure what else to call it. Foundem earns revenue by directing customers to retail sites to purchase goods. In this sense, Foundem acts like a shopping mall. Google does the same, only instead of receiving a cut from the sale, as Foundem does, Google sells advertisements. Thus, when Foundem complains about access to Google's site, it is a competing channel of distribution, complaining that it needs access to its competitor's distribution channel in order to compete.

It's a weird sort of complaint. It isn't the same as the classic essential facilities sort of complaint where, to simplify, the owner of a vertically-integrated railroad

and rail transport company prevents access by other transport companies to its railroad line. Instead this would be like railroad company A arguing that railroad B must give A access to B's tracks so A can sell access to those tracks to other rail transport companies.

But even this doesn't completely capture the audacity of the complaint, because for the analogy to hold, railroad A would actually be asking the court to force railroad B to put up a sign at the head of its tracks allowing railroad A to offer to trains already on B's railroad the opportunity to jump off B's railroad and start over again on A's railroad that follows another route—but without knowing for sure if the route is better or worse until you jump onto A's tracks. Something like that. Again, it's weird.

And note, of course, the problem that "at the head of the tracks" (as in something like "the first, second or third organic result") is a problematic requirement as only three sites at any given time can occupy those spots—but there may be many more than three firms complaining of Google's conduct and/or affected by the vagaries of its product design decisions. Or to keep with the shopping mall analogy, it's like the owner of any of a number of small, new shopping malls requiring the owner of a large, established shopping mall to permit each of the new mall's owners to set up a bus line to ferry shoppers to the new mall as they enter the established mall. Even where the established mall has a geographic, reputational and resource advantage, no one would argue that this access was essential to efficient commerce, and the cost to the successful incumbent would be manifestly too high.

As discussed above, sites like Foundem do indeed have access to Google's end users via any number of keywords on Google's site. Type "UK price comparison site" into Google and a number of Google competitors come up including Foundem (and Google's own price comparison site is seemingly absent). The claim thus becomes one that is either inappropriately aggregated ("for all search terms on average that may direct users to Foundem, Foundem is effectively denied access to the top search results") or else overly narrow ("we prefer customers to find us by typing 'Nikon camera' into Google, not by typing 'price comparison Nikon camera' into Google"). In any case, access is in fact available for these competitors, and "the indispensable requirement for invoking the [essential facilities] doctrine is the unavailability of access to the 'essential facilities'; where access exists, the doctrine serves no purpose."[46]

Meanwhile, it is difficult to see how relevance (and thus efficiency) could be well-served by a neutrality principle that required a tool that *reduces* search costs to inherently *increase* those costs by directing searchers to a duplicate search on another site. If one is searching for a specific product and hoping to find price comparisons on Google, why on earth would that person be hoping to find not Google's own efforts at price comparison, built right into its search engine, but

---

46 *Trinko*, 540 U.S. at 411.

instead a link to another site that requires another several steps before finding the information?

Seen this way, Google's decision to promote its own price comparison results is a simple product pricing and design decision, protected by good sense and the *Trinko* decision (at least in the U.S.). Unlike the majority of its vertical search competitors and by design, Google makes no direct revenue from users clicking through to purchase anything from its shopping search results, and this allows it to offer a different (and, to many consumers, a significantly better) set of results. The page has paid search results only in small boxes at the top and bottom, the information is all algorithmically generated, and retailers do not pay to have their information on the page. For this product design—by definition of great value to users (in effect lowering the price to them of their product search)—to merit Google's investment, it is necessary that its own, more-relevant and less-expensive results receive priority. If this is generating something of value for Google it is doing so only in the most salutary fashion: by offering additional resources for users to improve their "search experience" and thus induce them to use Google's search engine. To require "neutrality" in this setting is to impair the site's ability to design and price its own product. Even the *Aspen Skiing* decision didn't go that far, requiring access to a joint marketing arrangement but not obligating Aspen Ski Company to alter its prices for skiers seeking to access only its own slopes.

And the same analysis holds for assessments of Google's other offerings (maps and videos, for example) that compete with other sites. Look for the nearest McDonalds in Google and a Google Map is bound to top the list (but not be the exclusive result, of course). But why should it be any other way? In effect, what Google does is give you the Web's content in as accessible and appropriate a form as it can—design decisions that, Google must believe, increase quality and reduce effective price for its users. By offering not only a link to McDonalds' web site, as well as various other links, but also a map showing the locations of the nearest restaurants, Google is offering up results in different forms, hoping that one is what the user is looking for. There is no economic justification for requiring a search engine in this setting to offer another site's rather than its own simply because there happen to be other sites that do, indeed, offer such content (and would like cheaper access to consumers).

## Conclusion

Search neutrality and forced access to Google's results pages is based on the proposition that—Google's users' interests be damned—if Google is the easiest way competitors can get to potential users, Google must provide that access. The essential facilities doctrine, dealt a near-death blow by the Supreme Court in *Trinko*, has long been on the ropes. It should remain moribund here. On the one hand Google does not preclude, nor does it have the power to preclude, users from accessing competitors' sites; all users need do is type "foundem.com" into their web browser—which works even if it's Google's

own Chrome browser! To the extent that Google can and does limit competitors' access to its search results page, it is not controlling access to an "essential facility" in any sense other than Wal-Mart controls access to its own stores. "Google search results generated by its proprietary algorithm and found on its own web pages" do not constitute a market to which access should be forcibly granted by the courts or legislature.

The set of claims that are adduced under the rubric of "search neutrality" or the "essential facilities doctrine" against Internet search engines in general and, as a practical matter, Google in particular, are deeply problematic. They risk encouraging courts and other decision makers to find antitrust violations where none actually exist, threatening to chill innovation and efficiency-enhancing conduct. In part for this reason, the essential facilities doctrine has been relegated by most antitrust experts to the dustbin of history. As Joshua Wright and I conclude elsewhere:

> Indeed, it is our view that in light of the antitrust claims arising out of innovative contractual and pricing conduct, and the apparent lack of any concrete evidence of anticompetitive effects or harm to competition, an enforcement action against Google on these grounds creates substantial risk for a "false positive" which would chill innovation and competition currently providing immense benefits to consumers.[47]

---

47 Geoffrey A. Manne & Joshua D. Wright, *Google and the Limits of Antitrust: The Case Against the Case Against Google*, 34 HARV. J. L. & PUB. POL'Y at 62.

# Some Skepticism About Search Neutrality

By James Grimmelmann*

> *The perfect search engine would be like the mind of God.*[1]
>
> *The God that holds you over the pit of hell, much as one holds a spider, or some loathsome insect, over the fire, abhors you, and is dreadfully provoked; his wrath towards you burns like fire; he looks upon you as worthy of nothing else, but to be cast into the fire …*[2]
>
> *If God did not exist, it would be necessary to invent him.*[3]

Search engines are attention lenses; they bring the online world into focus. They can redirect, reveal, magnify, and distort. They have immense power to help and to hide. We use them, to some extent, always at our own peril. And out of the many ways that search engines can cause harm, the thorniest problems of all stem from their ranking decisions.[4]

What makes ranking so problematic? Consider an example. The U.K. technology company Foundem offers "vertical search"[5]—it helps users compare prices for electronics, books, and other goods. That makes it a Google competitor.[6] But in June 2006, Google applied a "penalty" to Foundem's

---

* Associate Professor of Law, New York Law School. I would like to thank Aislinn Black and Frank Pasquale for their comments. 

1 Charles Ferguson, *What's Next for Google*, TECH. REV., Jan. 1, 2005, at 38, available at **http://www.technologyreview.com/web/14065/** (quoting Sergey Brin, co-founder of Google).

2 Jonathan Edwards, *Sinners in the Hands of an Angry God* (sermon delivered July 8, 1741 in Enfield, Connecticut), *available in* 22 WORKS OF JONATHAN EDWARDS 411 (Harry S. Stout & Nathan O. Hatch eds., Yale University Press 2003).

3 Voltaire, *Epître à l'auteur du livre des Trois imposteurs* [*Letter to the Author of* The Three Impostors] (1768), *available at* **http://www.whitman.edu/VSA/trois.imposteurs.html**.

4 *See* James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 17–44 (2007) (identifying nine distinct types of harm search engines can cause to users, information providers, and third parties).

5 *See generally* JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE 274–76 (2005) (discussing "domain-specific search").

6 *See Google Product Search Beta,* GOOGLE, **http://www.google.com/prdhp**.

website, causing all of its pages to drop dramatically in Google's rankings.[7] It took more than three years for Google to remove the penalty and restore Foundem to the first few pages of results for searches like "compare prices shoei xr-1000."[8] Foundem's traffic, and hence its business, dropped off dramatically as a result. The experience led Foundem's co-founder, Adam Raff, to become an outspoken advocate: creating the site searchneutrality.org,[9] filing comments with the Federal Communications Commission (FCC),[10] and taking his story to the op-ed pages of *The New York Times*,[11] calling for legal protection for the Foundems of the world.

Of course, the government doesn't get involved every time a business is harmed by a bad ranking—or *Consumer Reports* would be out of business.[12] Instead, search-engine critics base their case for regulation on the immense power of search engines, which can "break the business of a Web site that is pushed down the rankings."[13] They have the power to shape what millions of users, carrying out billions of searches a day, see.[14] At that scale, search engines are the new mass media[15]—or perhaps the new *meta* media—capable of shaping public discourse itself. And while power itself may not be an evil, abuse of power is.

Search-engine critics thus aim to keep search engines—although in the U.S. and much of the English-speaking world, it might be more accurate to say simply "Google"[16]—from abusing their dominant position. The hard part comes in defining "abuse." After a decade of various attempts, critics have hit on the

---

7 *See Foundem's Google Story*, SEARCHNEUTRALITY.ORG (Aug. 18, 2009), **http://www.searchneutrality.org/foundem-google-story**.

8 The Shoei XR-1000 is a motorcycle helmet—according to Foundem, it's £149.99 plus £10 delivery from Helmet City.

9 *About*, SEARCH NEUTRALITY.ORG, Oct. 9, 2009, **http://www.searchneutrality.org/about**.

10 Reply Comments of Foundem, In the Matter of Preserving the Open Internet Broadband Industry Practices, GN Docket No. 09-191 (F..C.C).

11 Adam Raff, *Search, But You May Not Find*, N.Y. TIMES, Dec. 27, 2009, at A27.

12 *Cf.* Bose Corp. v. Consumers Union, 466 U.S. 485 (1984) (holding *Consumer Reports* not subject to product disparagement liability for negative review of Bose speaker).

13 *The Google Algorithm*, N.Y. TIMES, July 14, 2010, at A30.

14 *See* GRANT ESKELSEN ET AL., THE DIGITAL ECONOMY FACT BOOK 12–13 (10th ed. 2009), **http://pff.org/issues-pubs/books/factbook_10th_Ed.pdf**.

15 *See generally* KEN AULETTA, GOOGLED: THE END OF THE WORLD AS WE KNOW IT (2009) (trying to understand Google by adopting the perspective of the media industry). *Cf.* Aaron Swartz, *Googling for Sociopaths*, RAW THOUGHT (Dec. 14, 2009), **http://www.aaronsw.com/weblog/googled** (describing *Googled* as "a history of [Google] as told by the incumbent sociopaths").

16 *See* ESKELSEN ET AL., FACT BOOK, *supra* note 14.

idea of "neutrality" as a governing principle. The idea is explicitly modeled on network neutrality, which would "forbid operators of broadband networks to discriminate against third-party applications, content or portals."[17] Like broadband Internet service providers (ISPs), search engines "accumulate great power over the structure of online life."[18] Thus, perhaps search engines should similarly be required not to discriminate among websites.

For some academics, this idea is a thought experiment: a way to explore the implications of network neutrality ideas.[19] For others, it is a real proposal: a preliminary agenda for action.[20] Lawyers for ISPs fighting back against network neutrality have seized on it, either as a *reductio ad absurdum* or a way to kneecap their bitter rival Google.[21] Even the *New York Times* has gotten into the game, running an editorial calling for scrutiny of Google's "editorial policy."[22] Since *New York Times* editorials, as a rule, reflect no independent thought but only a kind of prevailing conventional wisdom, it is clear that search neutrality has truly arrived on the policy scene.

Notwithstanding its sudden popularity, the case for search neutrality is a muddle. There is a fundamental misfit between its avowed policy goal of protecting users and most of the tests it proposes to protect them. Scratch beneath the surface of search neutrality and you will find that it would protect

---

17 Barbara van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 J. TELECOMM. & HIGH TECH. L. 329, 333 (2007), available at **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=812991**.

18 Frank Pasquale, *Internet Nondiscrimination Principles: Commercial Ethics for Carries and Search Engines*, 2008 U. CHI. LEGAL. FORUM 263, 298, available at **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1134159** [hereinafter Pasquale, *Internet Nondiscrimination Principles*].

19 *See* Mark R. Patterson, *Non-Network Barriers to Network Neutrality*, 78 FORDHAM L. REV. 2843 (2010); Andrew Odlyzko, *Network Neutrality, Search Neutrality, and the Never-ending Conflict Between Efficiency and Fairness in Markets*, 8 REV. NETWORK ECON. 40 (2009).

20 *See* DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE (2009) [hereinafter NUNZIATO, VIRTUAL FREEDOM]; Pasquale, *Internet Nondiscrimination Principles, supra* note 18; Oren Bracha & Frank Pasquale, *Federal Search Commission: Access, Fairness, and Accountability in the Law of Speech*, 93 CORNELL L. REV. 1149 (2008) [hereinafter Bracha & Pasquale, *Federal Search Commission*]; Jennifer A. Chandler, *A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet*, 35 HOFSTRA L. REV. 1095 (2007).

21 Letter from Robert W. Quinn, Jr., Senior Vice President, AT&T, to Sharon Gillett, Chief, Wireline Competition Bureau Federal Communications Commission (Sept. 25, 2009), available at **http://graphics8.nytimes.com/packages/pdf/technology/20090925_ATT-Letter.pdf**.

22 *The Google Algorithm*, *supra* note 13. But see Danny Sullivan, *The New York Times Algorithm & Why It Needs Government Regulation*, SEARCH ENGINE LAND (July 15, 2010) (parodying New York Times editorial on Google).

not search users, but websites. In the search space, however, websites are as often users' *enemies* as not; the whole point of search is to help users avoid the sites they don't want to see.

In short, search neutrality's ends and means don't match. To explain why, I will deconstruct eight proposed search-neutrality principles:

1. *Equality*: Search engines shouldn't differentiate at all among websites.
2. *Objectivity*: There are correct search results and incorrect ones, so search engines should return only the correct ones.
3. *Bias*: Search engines should not distort the information landscape.
4. *Traffic*: Websites that depend on a flow of visitors shouldn't be cut off by search engines.
5. *Relevance*: Search engines should maximize users' satisfaction with search results.
6. *Self-interest*: Search engines shouldn't trade on their own account.
7. *Transparency*: Search engines should disclose the algorithms they use to rank web pages.
8. *Manipulation*: Search engines should rank sites only according to general rules, rather than promoting and demoting sites on an individual basis.

As we shall see, all eight of these principles are unusable as bases for sound search regulation.

I would like to be clear up front about the limits of my argument. Just because search neutrality is incoherent, it doesn't follow that search engines deserve a free pass under antitrust, intellectual property, privacy, or other well-established bodies of law.[23] Nor is search-specific legal oversight out of the question. Search engines are capable of doing dastardly things: According to BusinessWeek, the Chinese search engine Baidu explicitly shakes down websites, demoting them in its rankings unless they buy ads.[24] It's easy to tell horror stories about what search engines *might* do that are just plausible enough to be genuinely scary.[25] My argument is just that search neutrality, as currently proposed, is unlikely to be workable and quite likely to make things worse. It fails at its own goals, on its own definition of the problem.

---

[23] This essay is not the place for a full discussion of these issues (although we will meet antitrust and consumer protection law in passing). Grimmelmann, *The Structure of Search Engine Law*, *supra* note 4, provides a more detailed map.

[24] Chi-Chu Tschang, *The Squeeze at China's Baidu*, BUSINESSWEEK, Dec. 31, 2008, **http://www.businessweek.com/magazine/content/09_02/b4115021710265.htm** (alleging that Baidu directly retaliates against sites that refuse to buy sponsored links by demoting them in its organic rankings).

[25] *See, e.g.*, Cory Doctorow, *Scroogled*, **http://craphound.com/scroogled.html**; Tom Slee, *Mr. Google's Guidebook*, WHIMSLEY (Mar. 7, 2008), **http://whimsley.typepad.com/whimsley/2008/03/mr-googles-guid.html**.

## Theory

Before delving into the specifics of search-neutrality proposals, it will help to understand the principles said to justify them. There are two broad types of arguments made to support search neutrality, one each focusing on users and on websites. A search engine that misuses its ranking power might be seen either as *misleading users* about what's available online, or as *blocking* websites from reaching users.[26] Consider the arguments in turn.

*Users*: Search helps people find the things they want and need. Good search results are better for them. And since search is both subjective and personal, users themselves are the ones who should define what makes search results good. The usual term for this goal is "relevance": relevant results are the ones that users themselves are most satisfied with.[27] All else being equal, good search policy should try to maximize relevance.

A libertarian might say that this goal is trivial.[28] Users are free to pick and choose among search engines and other informational tools.[29] They will naturally flock to the search engine that offers them the most relevant results; the market will provide just as much relevance as it is efficient to provide.[30] There is no need for regulation; relevance, being demanded by users, will be

---

26 Other arguments for search neutrality reduce to these two. Bracha and Pasquale, for example, are concerned about democracy. They want "an open and relatively equal chance to all members of society for participation in the cultural sphere." Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1183–84. Search engines provide that chance if individuals can both find (as users) and be found (as websites) when they participate in politics and culture. Similarly, Bracha and Pasquale's economic efficiency argument turns on users' ability to find market information, *id.* at 1173–75. and their fairness concern speaks to websites' losses of "audience or business," *id.* at 1175–76. Whatever interest society has in search neutrality arises from users' and websites' interests in it—so we are justified in focusing our attention on users and websites.

27 *See* BATTELLE, THE SEARCH, *supra* note 5, at 19–25.

28 For a clear statement of a libertarian perspective on search neutrality, see Mike Masnick's posts at Techdirt on the subject, collected at **http:/www.techdirt.com/blog.php?tag=search+neutrality**. Eric Goldman's *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 YALE J. L. & TECH. 188 (2006), makes a general case against the regulation of relevance on similar grounds.

29 In Google's words, "Competition is just one click away." Adam Kovacevich, *Google's Approach to Competition*, GOOGLE POLICY BLOG (May 8, 2009), **http://googlepublicpolicy.blogspot.com/2009/05/googles-approach-to-competition.html**.

30 *See* Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151.

supplied by search engines. And this is exactly what search engines themselves say: relevance is their principal, or only, goal.[31]

The response to this point of view—most carefully argued by Frank Pasquale[32]—is best described as "liberal." It focuses on maximizing the effective autonomy of search users, but questions whether market forces actually enable users to demand optimal relevance. For one thing, it questions whether users can actually detect deviations from relevance.[33] The user who turns to a search engine, by definition, doesn't yet know what she's looking for or where it is. Her own knowledge, therefore, doesn't provide a fully reliable check on what the search engine shows her. The information she would need to know that the search engine is hiding something from her may be precisely the information it's hiding from her—a relevant site that she didn't know existed.[34]

Perhaps just as importantly, structural features of the search market can make it hard for users to discipline search engines by switching. Search-neutrality advocates have argued that search exhibits substantial barriers to entry.[35] The web is so big, and search algorithms so complex and refined, that there are substantial fixed costs to competing at all.[36] Moreover, the rise of personalized search both creates switching costs for individual users[37] and also makes it harder for them to share information about their experiences with multiple search engines.[38]

*Websites*: The case for protecting websites reaches back into free speech theory. Jerome Barron's 1967 article, *Access to the Press—A New First Amendment Right*,[39]

---

31 *See, e.g.*, *Technology Overview*, GOOGLE, www.google.com/corporate/tech.html; *How Web Documents Are Ranked*, YAHOO!, **http://help.yahoo.com/l/us/yahoo/search/indexing/ranking-01.html**; *Ask Search Technology*, ASK, **http://sp.ask.com/en/docs/about/ask_technology.shtml**.

32 *See* Pasquale, *Internet Nondiscrimination Principles*, *supra* note 18; Bracha & Pasquale, *Federal Search Commission*, *supra* note 20; Frank Pasquale, *Asterisk Revisited: Debating a Right of Reply on Search Results*, 3 J. BUS. & TECH. L. 61 (2008); Frank Pasquale, *Rankings, Reductionism, and Responsibility*, 54 CLEV. ST. L. REV. 115 (2006).

33 *See* Chandler, *Right to Reach an Audience*, *supra* note 20, at 1116; Patterson, *Non-Network Barriers*, *supra* note 19, at 2860-62.

34 *See* Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1183–84.

35 *See id.* at 1181–82.

36 *See id.* at 1181.

37 *See* Pasquale, *Internet Nondiscrimination Principles*, *supra* note 18, at 265.

38 *See* Frank Pasquale, *Could Personalized Search Ruin Your Life?*, CONCURRING OPINIONS (Feb. 7, 2008), **http://www.concurringopinions.com/archives/2008/02/personalized_se.html**.

39 80 HARV. L. REV. 1641 (1967).

argued that freedom of speech is an empty right in a mass-media society unless one also has access to the mass media themselves. He thus argued that newspapers should be required to open their letters to the editor and their advertising to all points of view.[40] Although his proposed right of access is basically a dead letter as far as First Amendment doctrine goes,[41] it captured the imaginations of media-law scholars and media advocates.[42]

Scholars have begun to adapt Barron's ideas to online intermediaries, including search engines. Dawn Nunziato's book *Virtual Freedom* draws extensively on Barron to argue that Congress may need to "authorize the regulation of dominant search engines to require that they provide meaningful access to content."[43] Jennifer Chandler applies Barron's ideas to propose a "right to reach an audience"[44] that would give website owners various protections against exclusion[45] and demotion by search engines.[46] Similarly, Frank Pasquale suggests bringing "universal service" over into the search space,[47] perhaps through a government-provided search engine.[48]

The Barronian argument for access, however, needs to be qualified. The free-speech interest in access to search engine ranking placement is really *audiences*' free speech interest; the real harm is that search users have been deprived of access to the speech of websites, not that websites have been deprived of access to users. Put another way, websites' access interest is derivative of users' interests. In the Supreme Court's words, "The First Amendment protects the right of every citizen to 'reach the minds of *willing* listeners.'"[49] Or, in Jerome

---

40 *Id.* at 1667.

41 *See* Miami Herald Pub'g Co. v. Tornillo, 418 U.S. 241 (1974) (striking down Florida law requiring newspapers to provide equal space for political responses).

42 *See, e.g.*, *Reclaiming the First Amendment: Constitutional Theories of Media Reform*, 35 HOFSTRA L. REV. 917–1582 (symposium issue collecting papers from conference honoring the 40th anniversary of publication of *Access to the Press*).

43 NUNZIATO, VIRTUAL FREEDOM, *supra* note 20, at 150.

44 Chandler, *Right to Reach an Audience*, *supra* note 20, at 1103–17 (search engines), 1124-30 (proposed right).

45 Exclusion from a search index may sound like a bright-line category of abuse, but note that a demotion from, say, #1 to #58,610 will have the same effect. No one ever clicks through 5861 pages of results. Thus, in practice, any rule against exclusion would also need to come with a—more problematic—rule against substantial demotions.

46 *Id.* at 1117–18.

47 Pasquale, *Internet Nondiscrimination Principles*, *supra* note 18, at 289–92. His example, which focuses on Google's scans of books for its Book Search project, is interesting, but is "universal access" only in a loose, metaphorical sense.

48 *See* Frank Pasquale, *Dominant Search Engines: An Essential Cultural and Political Facility*, *infra* 258.

49 Hefron v. Int'l Soc. for Krishna Consciousness, Inc., 452 U.S. 640, 655 (1981) (quoting Kovacs v. Cooper, 336 U.S. 77, 87 (1949)) (emphasis added).

Barron's, "[T]he point of ultimate interest is not the words of the speakers but the minds of the hearers."[50] With these purposes in mind, let us turn to actual search-neutrality proposals.

## Equality

Scott Cleland observes that Google's "algorithm reportedly has over 1,000 variables/discrimination biases which decide which content gets surfaced."[51] He concludes that "Google is not neutral" and thus should be subject to any FCC network-neutrality regulation.[52] On this view, a search engine does something wrong if it treats websites differently, "surfac[ing]" some, rather than others. This is a theory of neutrality as equality, it comes from the network-neutrality debates, and it is nonsensical as applied to search.

Equality has a long pedigree in telecommunications. For years, common-carrier regulations required the AT&T system to offer its services on equal terms to anyone who wanted a phone.[53] This kind of equality is at the heart of proposed network neutrality regulations: treating all packets identically once they arrive at an ISP's router, regardless of source or contents.[54] Whether or not equality in packet routing is a good idea as a technical matter, the rule itself is simple enough and relatively clear. One can, without difficulty, identify Comcast's forging of packets to terminate BitTorrent connections as a violation of the principle.[55] As long as an ISP isn't overloaded to the point of losing too many packets, equality does what it's supposed to: ensures that every website enjoys access to the ISP's network and customers.

Try to apply this form of equality to search and the results are absurd. Of course Google differentiates among sites—that's why we use it. Systematically favoring certain types of content over others isn't a defect for a search engine—it's the *point*.[56] If I search for "Machu Picchu pictures," I want to see llamas in a

---

50 Barron, *Access to the Press*, *supra* note 39, at 1653.

51 Scott Cleland, *Why Google Is Not Neutral*, PRECURSOR BLOG (Nov. 4, 2009), **http://precursorblog.com/content/why-google-is-not-neutral**.

52 *Id.*

53 *See generally* JONATHAN E. NEUCHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS 45–68 (2005).

54 For an accessible introduction to the technical issues, see Edward W. Felten, *The Nuts and Bolts of Network Neutrality* (2006), **http://itpolicy.princeton.edu/pub/neutrality.pdf**.

55 *See In re Formal Compl. of Free Press & Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications*, WC Docket No. 07-52, Order, 23 F.C.C. Rcd. 13,028, 13,029–32 (discussing blocking), 13,050–58 (finding that blocking violated federal policy) (2008), *vacated*, Comcast v. FCC, 600 F.3d 642 (D.C. Cir. 2010).

56 *See* Karl Bode, *Google Might Stop Violating "Search Neutrality" If Anybody Knew What That Actually Meant*, TECHDIRT (May 7, 2010),

ruined city on a cloud-forest mountaintop, not horny housewives who whiten your teeth while you wait for them to refinance your mortgage. Search inevitably requires some form of editorial control.[57] A search engine cannot possibly treat all websites equally, not without turning into the phone book. But for that matter, even the phone book is not neutral in the sense of giving fully equal access to all comers, as the proliferation of AAA Locksmiths and Aabco Plumbers attests. Differentiating among websites, without something more, is not wrongful.

## Objectivity

If search engines must make distinctions, perhaps we should insist that they make correct distinctions. Foundem, for example, argues that the Google penalty was unfair by pointing to positive write-ups of Foundem from "the UK's leading technology television programme" and "the UK's leading consumer body," and to its high search ranks on Yahoo! and Bing.[58] The unvoiced assumption here is that search queries can have objectively right and wrong answers. A search on "James Grimmelmann blog" should come back with my weblog at **http://laboratorium.net**; anything else is a wrong answer.

But this view of what search is and does is wrong. A search for "apple" could be looking for information about Fiji apples, Apple computers, or Fiona Apple. "bbs" could refer to airgun pellets, bulletin-board systems, or bed-and-breakfasts. Different people will have different intentions in mind; even the same person will have different intentions at different times. Sergey Brin's theological comparison of perfect search to the "mind of God"[59] shows us why perfect search is impossible. Not even Google is—or ever could be—omniscient. The search query itself is necessarily an incomplete basis on which to guess at possible results.[60]

The objective view of search, then, fails for two related reasons. First, search users are profoundly diverse. They have highly personal, highly contextual goals. One size cannot fit all. And second, a search engine's job always involves guesswork.[61] Some guesses are better than others, but the search

---

**http://www.techdirt.com/articles/20100504/1324279300.shtml** ("[T]he entire purpose of search is to discriminate and point the user toward more pertinent results.").

57 *See* Goldman, *Search Engine Bias*, *supra* note 28, at 115–18.

58 *Foundem's Google Story*, *supra* note 7.

59 *Supra* note 1.

60 *See generally* ALEX HALAVAIS, THE SEARCH-ENGINE SOCIETY 32–55 (2009) (discussing difficulties of ascertaining meaning in search process).

61 *See* Eric Goldman, *Deregulating Relevancy in Internet Trademark Law*, 54 EMORY L.J. 507, 521–28 (2005).

engine will always have to guess. "James Grimmelmann blog" shouldn't take users to Toyota's corporate page—but perhaps they were interested in my guest-blogging at *Concurring Opinions*, or in blogs about me, or they have me mixed up with Eric Goldman and were actually looking for *his* blog. Time Warner Cable's complaint that "significant components of [Google's] Ad Rank scheme are subjective"[62] is beside the point. *Search itself is subjective.*[63]

Few scholars go so far as to advocate explicit re-ranking to correct search results.[64] But even those who acknowledge that search is subjective sometimes write as though it were not. Frank Pasquale gives a hypothetical in which "YouTube's results always appear as the first thirty [Google] results in response to certain video queries for which [a rival video site] has demonstrably more relevant content."[65] One might ask, "demonstrably more relevant" *by what standard*? Often the answer will be contentious.

In Foundem's case, what difference should it make that Yahoo! and others liked Foundem? So? That's their opinion. Google had a different one. Who is to say that Yahoo! was right and Google was wrong?[66] One could equally well argue that Google's low ranking was correct and Yahoo!'s high ranking was the mistake. "compare prices shoei xr-1000" is not the sort of question that admits

---

62 Comments of Time Warner Cable Inc. 77, In the Matter of Preserving the Open Internet Broadband Industry Practices, GN Docket No. 09-191 (F.C.C. comments filed Jan. 14, 2010).

63 *See* Goldman, *Search Engine Bias*, supra note 28, at 112–13. This point should not be confused with a considered opinion on the question of how the First Amendment applies to search-ranking decisions. Search engines make editorial judgments about relevance, but they also present information that can only be described as factual (such as maps and addresses), extol their objectivity in marketing statements, and are perceived by users as having an aura of reliability. It is possible to make false statements even when speaking subjectively—for example, I would be lying to you if I said that I enjoy eating scallops. The fact that search engines' judgments are expressed algorithmically, including in ways not contemplated by their programmers, complicates the analysis even further. The definitive First Amendment analysis of search-engine speech has yet to be written. Academic contributions to that conversation include Goldman, *Search Engine Bias*, *supra* note 28, at 112–15; Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1188–1201; Pasquale, *Asterisk Revisited*, *supra* note 32, at 68–85; NUNZIATO, VIRTUAL FREEDOM, *supra* note 20, *passim* (and particularly pages 149–51); Chandler, *Right to Reach an Audience*, *supra* note 20, at 1124–29; James Grimmelmann, *The Google Dilemma*, 53 N.Y.L.S. L. REV. 939, 946 (2009); Grimmelmann, *The Structure of Search Engine Law*, *supra* note 4, at 58–60. Some leading cases are listed in note 85, *infra*.

64 *But see* Sandeep Pandey et al., *Shuffling a Stacked Deck: The Case for Partially Randomized Search Results*, PROC. 31ST VERY LARGE DATABASES CONF. 781 (2005) (arguing for randomization in search results to promote obscure websites).

65 Pasquale, *Internet Nondiscriminaion Principles, supra* note 18, at 296.

66 *Cf.* Rebecca Tushnet, *It Depends on What the Meaning of "False" Is, Falsity and Misleadingness in Commercial Speech Doctrine*, 41 LOYOLA L.A. L. REV. 101 (2008) (arguing that judgments about falsity frequently embody contested social policies).

of a right answer. This is why it doesn't help to say that the Foundem vote is four-to-one against Google. If deviation from the majority opinion makes a search engine wrong, then so much for search engine innovation—and so much for unpopular views.[67]

## Bias

Ironically, it is the goal of protecting unpopular views that drives the concern with search engine "bias." Lucas Introna and Helen Nissenbaum, for example, are concerned that search engines will direct users to sites that are already popular and away from obscure sites.[68] Alex Halavais calls for "resistance to the homogenizing process of major search engines,"[69] including governmental interventions.[70] These are structural concerns with popularity-based search. Others worry about more particular biases. AT&T complains that "Google's algorithms unquestionably *do* favor some companies or sites."[71] Scott Cleland objects that Google demotes content from other countries in its country-specific search pages.[72]

The point that a technological system can display bias is one of those profound observations that is at once both startling and obvious.[73] It naturally leads to the question of whether, when, and how one could correct for the bias search engines introduce.[74] But to pull that off, one must have a working understanding of what constitutes search-engine bias. Batya Friedman and Helen Nissenbaum define a computer system to be "biased" if it "*systematically* and *unfairly* discriminates against certain individuals or groups of individuals in favor of others."[75] Since search engines systematically discriminate by design,

---

67 This last point should be especially troubling to Barron-inspired advocates of "access," since the point of such a regime is to *promote* opinions that are not widely shared.

68 Lucas D. Introna & Helen Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, 16 INFO. SOC. 169, 175 (2000).

69 HALAVAIS, SEARCH ENGINE SOCIETY, *supra* note 60, at 106.

70 *Id.* at 132–38.

71 Comments of AT&T Inc. 102, In the Matter of Preserving the Open Internet Broadband Industry Practices, GN Docket No. 09-191 (F.C.C. comments filed Jan. 14, 2010).

72 Cleland, *Why Google Is Not Neutral*, *supra* note 51.

73 In Landgon Winner's phrase, "artifacts have politics." LANGDON WINNER, THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY19 (University of Chicago Press 1986).

74 *See, e.g.*, Pandey et al, *Shuffling a Stacked Deck*, *supra* note 64.

75 Batya Friedman & Helen Nissenbaum, *Bias in Computer Systems*, 14 ACM TRANS. ON COMPUTER SYS. 330, 332 (1996). *See also* Alejandro M. Diaz, Through the Google Goggles: Sociopolitical Bias in Search Engine Design (May 23, 2005) (unpublished B.A. thesis, Stanford University), *available at* **http://epl.scu.edu/~stsvalues/readings/Diaz_thesis_final.pdf**.

all of the heavy lifting in the definition is done by the word "unfair." But this just kicks the problem down the road. One still must explain when discrimination is "unfair" and when it is not. Friedman and Nissenbaum's discussion is enlightening, but does not by itself help us identify which practices are abusive.[76]

The point that socio-technical systems have embedded biases also cuts against search neutrality. We should not assume that if only the search *engine* could be made properly neutral, the search *results* would be free of bias. Every search result requires both a user to contribute a search query, and websites to contribute the content to be ranked. Neither users nor websites are passive participants; both can be wildly, profoundly biased.

On the website side, the web is anything but neutral.[77] Websites compete fiercely, and not always ethically, for readers.[78] It doesn't matter *what* the search engine algorithm is; websites will try to game it. Search-engine optimization, or SEO, is as much a fixture of the Internet as spam. Link farms,[79] spam blog comments, hacked websites—you name it, and they'll try it, all in the name of improving their search rankings. A fully invisible search engine, one that introduced no new values or biases of its own, would merely replicate the underlying biases of the web itself:[80] heavily commercial, and subject to a truly mindboggling quantity of spam. Raff says that search algorithms should be "comprehensive."[81] But should users be subjected to a comprehensive presentation of discount Canadian pharmaceutical sites?

On the user side, sometimes the bias is between the keyboard and the chair. Fully de-biasing search results would also require de-biasing search queries—and users' ability to pick which results they click on. Take a search for "jew," for example. Google has been criticized both for returning anti-Semitic sites (to

---

76 If one fears, with Bracha and Pasquale, that "a handful of powerful gatekeepers" wield disproportionate influence, then the solution is simple: break up the bastards. If they reassemble or reacquire too much power, do it again. Neutrality will always be an imperfect half-measure if power itself is the problem.

77 *See* Clay Shirky, *Power Laws, Weblogs, and Inequality*, SHIRKY.COM (Feb. 8, 2003), **http://www.shirky.com/writings/powerlaw_weblog.html** (discussing vast disproportion of prominence between famous and obscure weblogs).

78 *See* IAN H. WITTEN ET AL., WEB DRAGONS: INSIDE THE MYTHS OF SEARCH TECHNOLOGY 145–75 (Morgan Kaufmann Publishers 2007).

79 A link farm is a group of automatically generated web sites that heavily link to each other. The point is to trick a popularity-based search engine into believing that all of the sites in the group are popular. *See* Grimmelmann, *The Google Dilemma*, *supra* note 63, at 946,

80 *See* Patterson, *Non-Network Barriers*, *supra* note 19, at 2854–55.

81 Raff, *Search, But You May Not Find*, *supra* note 11.

American users) and for *not* returning such sites (to German users).[82] The inescapable issue is that Google has users who want to read anti-Semitic web pages and users who don't. One might call some of those users "biased," but if they are, it's not Google's fault.

Some bias is going to leak through as long as search engines help users find what they want. And helping users find what they want is such a profound social good that one should be skeptical of trying to inhibit it.[83] Telling users what they *should* see is a serious intrusion on personal autonomy, and thus deeply inconsistent with the liberal argument for search neutrality. If you want Google to steer users to websites with views that differ from their own,[84] your goal is not properly described as search *neutrality*. In effect, you have gone back to asserting the objective correctness of search results: Certain sites are good for users, like whole grains.

## Traffic

The most common trope in the search debates is the website whose traffic vanishes overnight when it disappears from Google's search results.[85] Because so much traffic flows through Google, it holds websites over the flames of website hell, ready at any instant to let them fall in the rankings. Chandler's proposed right to reach an audience and Foundem's proposed "effective, accessible, and transparent appeal process"[86] attempt to protect websites from

---

82 *See* Grimmelmann, *The Google Dilemma*, *supra* note 63, at 943–45.

83 *See* James Grimmelmann, *Don't Censor Search*, 117 YALE L.J. POCKET PART 48 (2007).

84 *See generally* CASS SUNSTEIN, REPUBLIC.COM 2.0 (Princeton University Press 2007).

85 *See, e.g.*, BATTELLE, THE SEARCH, *supra* note 5, at 153–59 (2bigfeet.com, main index); NUNZIATO, VIRTUAL FREEDOM, *supra* note 20, at 14–17 (various sites, AdWords and Google News); Chandler, *Right to Reach an Audience*, *supra* note 20, at 1110 (BMW Germany and Ricoh Germany, main index); Michael Y. Park, *Journalist Who Exposes U.N. Corruption Disappears from Google*, FOX NEWS, Feb. 18, 2008, **http://www.foxnews.com/story/0,2933,331106,00.html** (Inner City Press, Google News); Cleland, *Why Google Is Not Neutral*, *supra* note 51 (ExtremeTech.com and Fotolog.com, AdWords); Dan Mcsai, *G-Railed: Why Did Google Bury the Web's Oldest Entertainment Publication?*, FASTCOMPANY.COM (Dec. 2, 2009), **http://www.fastcompany.com/blog/dan-macsai/popwise/why-did-neutral-google-de-list-webs-oldest-entertainment-publication** (Studio Briefing, AdWords and main index); *Foundem's Google Story*, *supra* note 7 (Foundem, main index). Opinions in lawsuits challenging demotions or exclusions include Langdon v. Google Inc., 474 F. Supp. 622 (D. Del. 2007) (NCJusticeFraud.com and ChinaIsEvil.com, AdWords); Kinderstart.com LLC v. Google, Inc., No. C 06-2057 JF (RS), 2006 U.S. Dist. LEXIS 82481 (N.D. Cal. July 13, 2006) (Kinderstart.com, main index) and Search King, Inc. v. Google Tech., Inc., No. CIV-02-1457-M, 2003 U.S. Dist. LEXIS 27193 (W.D. Okla. 2003) (SearchKing.com, main index).

86 *Foundem's Google Story*, *supra* note 7.

being dropped. Dawn Nunzatio, for her part, would require search engines to open their sponsored links to political candidates.[87]

A right to continued customer traffic would be a legal anomaly; offline businesses enjoy no such right. Some Manhattanites who take the free IKEA ferry to its store in Brooklyn eat at the nearby food trucks in the Red Hook Ball Fields.[88] The food truck owners would have no right to complain if IKEA discontinued the ferry or moved its store. Search neutrality advocates, however, would say that RedHookFoodTruck.com has a Jerome Barron-style free-speech interest in having access to the search engine's result pages, and thus has more right to complain if the Google ferry no longer comes to its neighborhood.[89]

But, as we saw above, this is really an argument that *users* have a *relevance* interest in seeing the site. If no one actually wants to visit RedHookFoodTruck.com, then its owner shouldn't be heard to complain about her poor search ranking. When push comes to shove, search neutrality advocates recognize that websites must plead their case in terms of users' needs. Chandler's modern right of access is a "right to reach a *willing* audience,"[90] which she describes as "the right to be free of the imposition of discriminatory filters *that the listener would not otherwise have used*."[91] Even Foundem's Adam Raff presents his actual search-neutrality principle in user-protective terms: "search engines should have no editorial policies other than that their results be comprehensive, impartial and *based solely on relevance*."[92] Relevance is, of course, the touchstone of users' interests, not websites'.

Indeed, looking at the rankings from a website's perspective, rather than from users', can be counterproductive to free-speech values. If users really find other websites more relevant, then making them visit RedHookFoodTruck.com impinges on their autonomy and on *their* free speech interests as listeners. For any given search query, there may be dozens, hundreds, thousands of competing websites. The *vast majority* of them will thus have interests that diverge from users'—and every incentive to override users' wishes.

---

87 NUNZIATO, VIRTUAL FREEDOM, *supra* note 20, at 150–51.

88 *See* Adam Kuban, *Red Hook Vendors: A Quick Guide for the Uninitiated*, SERIOUS EATS (July 18, 2008), **http://newyork.seriouseats.com/2008/07/red-hook-vendors-soccer-tacos-guide-how-to-get-there-what-to-eat.html**.

89 *See* Chandler, *Right to Reach an Audience*, *supra* note 20; NUNZIATO, VIRTUAL FREEDOM, *supra* note 20.

90 Chandler, *Right to Reach an Audience*, *supra* note 20, at 1099 (emphasis added).

91 *Id.* at 1103 (emphasis added).

92 Raff, *Search, But You May Not Find*, *supra* note 11 (emphasis added).

Even when users are genuinely indifferent among various websites, some search neutrality advocates think websites should be protected from "arbitrary" or "unaccountable" ranking changes as a matter of fairness.[93] We should call the websites that currently sit at the top of search engine rankings by their proper name—*incumbents*—and we should look as skeptically on their demands to remain in power as we would on any other incumbent's. The search engine that ranks a site highly has conferred a benefit on it; turning that gratuitous benefit into a permanent entitlement gets the ethics of the situation exactly backwards.

Indeed, giving highly-ranked websites what is in effect a property right in search rankings runs counter to everything we know about how to hand out property rights. Websites don't create the rankings; search engines do. Similarly, search engines are in a better position to manage rankings and prevent waste. And if each individual search ranking came with a right to placement, every search-results page would be an anti-commons in the making.[94]

Thus, it is *irrelevant* that Foundem had a prominent search placement on Google before it landed in the doghouse. Just as the subjectivity of search means that search engines will frequently disagree with each other, it also means that a search engine will disagree with itself over time. From the outside looking in, we have no basis to say whether the initial high ranking or the subsequent low ranking made more sense. To give Foundem—and every other website currently enjoying a good search ranking—the right to continue where it is would lock in search results for all time, obliterating search-engine experimentation and improvement.

## Relevance

Given the importance of user autonomy to search-neutrality theory, relevance is a natural choice for a neutrality principle. In Foundem's words, search results should be "based solely on relevance."[95] Chandler proposes a rule against "discrimination that listeners would not have chosen."[96] Bracha and Pasquale decry "search engines [that] highlight or suppress critical information" and thereby "shape and constrain [users'] choices"—that is, hide information that users would have found relevant.[97]

---

93 Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1175–76.

94 *See generally* Michael Heller, *The Tragedy of the Anticommons*, 111 HARV. L. REV. 621 (1998) (arguing that when too many owners have exclusion rights over a resource, it is prone to underuse).

95 *Search Neutrality*, SEARCH NEUTRALITY.ORG (Oct. 11, 2009), **http://www.searchneutrality.org/**.

96 Chandler, *Right to Reach an Audience*, *supra* note 20, at 1098.

97 Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1177.

Relevance, however, is such an obvious good that its virtue verges on the tautological. Search engines *compete* to give users relevant results; they exist at all only because they do. Telling a search engine to be more relevant is like telling a boxer to punch harder. Of course, sometimes boxers do throw fights, so it isn't out of the question that a search engine might underplay its hand. How, though, could regulators tell? Regulators can't declare a result "relevant" without expressing a view as to why other possibilities are "irrelevant," and that is almost always going to be contested.

Here's an example: Foundem. Recall that Foundem is a "vertical search site" that specializes in consumer goods. Well, a great many vertical search sites are worthless. (If you don't believe me, please try using a few for a bit.) Like other kinds of sites that simply roll up existing content and slap some of their own ads on it—Wikipedia clones and local business directories also come to mind—they superficially resemble legitimate sites that provide something of value to users.[98] But only superficially. The "penalties" that reduce vertical search sites' Google ranks aren't an attempt to reduce competition at the expense of relevance; they're an attempt to *implement* relevance.[99] There are a few relatively good, usable product-search sites, but most of them are junk and good riddance to them. You're welcome to disagree—search is subjective—but I'd rather have the anti-vertical penalty in place than not. Those who would argue that Google's rankings don't reflect relevance have a heavy burden of proof, in the face of ample, easily verified evidence to the contrary.

In fact, behind almost every well-known story of search engine caprice, there is a more persuasive relevance-enhancing counter-story. For example, SourceTool, another vertical search engine, has sued Google under antitrust law for, in effect, demoting it in Google's rankings for search ads.[100] SourceTool, though, is a "directory" with a taxonomic logic of dubious utility—the United Nations Standard Products and Services Code—and almost no content of its own. It's the rare user indeed who will find SourceTool relevant. If you care about relevance and user autonomy, you should applaud Google's decision to demote SourceTool.

---

98 *See* Chris Lake, *Foundem vs Google: A Case Study in SEO Fail*, ECONSULTANCY (Aug. 18, 2009), **http://econsultancy.com/blog/4456-foundem-vs-google-a-case-study-in-seo-fail**; *Little or No Original Content*, GOOGLE WEBMASTER CENTRAL (updated June 10, 2009), www.google.com/support/webmasters/bin/answer.py?answer=66361.

99 *See* John Lettice, *When Algorithms Attack, Does Google Hear You Scream?*, THE REGISTER (Nov. 19, 2009), **http://www.theregister.co.uk/2009/11/19/google_hand_of_god/**.

100 *See* TradeComet.com LLC v. Google Inc., No. 09–CIV-1400 (S.D.N.Y. complaint filed Feb. 17, 2009). The District Court dismissed the case on the basis of the forum-selection clause in Google's advertiser agreement, without reaching the merits of the case. *See* TradeComet.com LLC v. Google Inc., 693 F. Supp. 2d 370 (S.D.N.Y. 2010).

## Self-Interest

In practice, even as search-neutrality advocates claim "relevance" as their goal, they rely on proxies for it. The most common is self-interest. A Consumer Watchdog report accuses Google of "an abandonment of [its] pledge to provide neutral search capability" by "steering Internet searchers to its own services" to "muscle its way into new markets."[101] Foundem alleges that Google demotes it and other vertical search sites to fend off competition, and alleges that Google's links to itself give it "an unassailable competitive advantage."[102] Bracha and Pasquale worry that search engines can change their rankings "in response to positive or negative inducements from other parties."[103]

Bad motive may lead to bad relevance, but it's also a bad proxy for it. The first problem is evidentiary. By definition, motivations are interior, personal.[104] Of course, the law has to guess at motives all the time, but the task is by its nature harder than looking to extrinsic evidence. People get it wrong all the time. In 2009, an Amazon employee with a fat finger hit a wrong button and categorized tens of thousands of gay-themed books as "adult."[105] An angry mob of Netizens assumed the company had deliberately pulled the books from its search engine out of anti-gay animus, and used the Twitter hashtag #amazonfail to express their very public outrage.[106] Amazon's reclassification was a mistake (a quickly corrected one), and a vivid demonstration of the power of search algorithms—but not a case of bad motives.[107]

In all but the most blatant of cases, in fact, a search engine will be able to tell a plausible relevance story about its ranking decisions.Proving that a relevance story is pretextual will be extraordinarily difficult, in view of the complexity and subjectivity of search. But it would also be disastrous to adopt the opposite point of view and presume pretext. The absence of bad motive is a negative that it will often be impossible for the search engine to prove. How can it

---

101 TRAFFIC REPORT: HOW GOOGLE IS SQUEEZING OUT COMPETITORS AND MUSCLING INTO NEW MARKETS (Consumer Watchdog 2010), **http://www.consumerwatchdog.org/resources/TrafficStudy-Google.pdf**.

102 *Reply Comments of Foundem*, *supra* note 10, at 1.

103 Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1170.

104 As an artificial corporate entity, a search engine may not even have motives other than the ones the law attributes to it.

105 *See* Nick Eaton, *AmazonFail: An Inside Look at What Happened*, AMAZON & THE ONLINE RETAIL BLOG (Apr. 13, 2009), **http://blog.seattlepi.com/amazon/archives/166384.asp**.

106 *See* Clay Shirky, *The Failure of #amazonfail*, SHIRKY.COM (Apr. 15, 2009), **http://www.shirky.com/weblog/2009/04/the-failure-of-amazonfail/**.

107 *But see* Mary Hodder, *Why Amazon Didn't Just Have a Glitch*, TECHCRUNCH (Apr. 14, 2009), **http://techcrunch.com/2009/04/14/guest-post-why-amazon-didnt-just-have-a-glitch/**.

establish, for example, that the engineer who added the anti-vertical penalty didn't have a lunchroom conversation with an executive who played up the competition angle? This is not to say that serious cases of abuse are implausible,[108] just that investigation will be unusually hard and that false positives will be dangerously frequent.

There *is* a nontrivial antitrust issue lurking here. In the United States, Google has a dominant market share in both search and search advertising, and one could argue that Google has started to leverage its position in anticompetitive ways.[109] Antitrust, however approaches such questions with a well-developed analytical toolkit: relevant markets, market power, pro-competitive and anti-competitive effects, and so on.[110] Antitrust rightly focuses on the effects of business practices on consumers; search neutrality should not short-circuit that consumer-centric analysis by overemphasizing the role of a search engine's motives. Some things can be good for Google *and* good for its users.

Thus, when Google links to its own products, not only can there be substantial technical benefits from integration, but often Google is helping users by pointing them to services that really are better than the competition. Consumer Watchdog, for example, cries foul that Google "put its own [map] service atop all others for generic address searches,"[111] and that Google Maps has taken half of the local search market at the expense of previously dominant MapQuest and Yahoo! Maps.[112] But perhaps MapQuest and Yahoo! Maps deserved to lose. Google Maps was groundbreaking when launched, and years later, it remains one of the best-implemented services on the Internet, with astonishingly clever scripting, flexible route-finding, and a powerful application programming interface (API).[113]

---

108 Baidu's alleged shakedown (*see supra* note 24 and accompanying text), if true, would be an example. Willingness to buy Baidu search ads is not in itself a reliable indicator of relevance to Baidu searchers. But then again, even pay-for-placement was once considered a plausible model for main-column search results—and willingness to pay is not inherently a crazy proxy for relevance. *See* BATTELLE, THE SEARCH, *supra* note 5, at 104–14 (discussing GoTo's pay-for-placement model). *See also* Goldman, *Coasean Analysis*, *supra* note 30 (envisioning a future in which advertisers and users negotiate over access to users' attention). Indeed, search ads today are sold on an auction-based basis. They're often as relevant as main-column search results, sometimes more so. It might be better to say that Baidu's real problems are monopoly pricing and (compulsory) stealth marketing.

109 *See, e.g.*, Brad Stone, *Sure, It's Big, But Is That Bad?*, N.Y. TIMES, May 21, 2010, at BU1.

110 See generally Geoffrey A. Manne & Joshua D. Wright, *Google and the Limits of Antitrust: The Case Against the Antitrust Case Against Google*, HARV. J. L. & PUB. POL'Y. (forthcoming).

111 TRAFFIC REPORT, *supra* note 101, at 5.

112 *Id.* at 5–7.

113 *See, e.g.*, John Carroll, *Google Maps and Innovation*, A DEVELOPER'S VIEW (Oct. 12, 2005), **http://www.zdnet.com/blog/carroll/google-maps-and-innovation/1499**.

One form of self-interest that may be well-enough defined to justify regulatory scrutiny is the straightforward bribe: a payment from a website to change its ranking, or a competitor's. Search-engine critics argue that search engines should disclose commercial relationships that bear on their ranking decisions.[114] This is a standard, sensible policy response to the fear of stealth marketing.[115] Indeed, the Federal Trade Commission (FTC) has specifically warned search engines not to mix their organic and paid search results.[116] More generally, the FTC endorsement guidelines provide that endorsements must "reflect the honest opinions, findings, beliefs, or experience of the endorser"[117] and that any connections between endorser and seller that "might materially affect the weight or credibility of the endorsement"[118] must be fully disclosed. These policies have a natural application to search engines. A search engine that factors payments from sponsors into its ranking decisions is lying to its users unless it discloses those relationships, and this sort of lie would trigger the FTC's jurisdiction.[119] This isn't a neutrality principle, or even unique to search; it's just a natural application of a well-established legal norm.

## Transparency

Search-engine critics generally go further and argue that search engines should also be required to disclose their *algorithms* in detail:

- Introna and Nissenbaum: "As a first step we would demand full and truthful disclosure of the underlying rules (or algorithms) governing indexing, searching, and prioritizing, stated in a way that is meaningful to the majority of web users."[120]
- Foundem: "Search Neutrality can be defined as the principle that search engines should be open and transparent about their editorial policies … ."[121]

---

114 *See, e.g.*, Pasquale, *Internet Nondiscrimination Principles*, *supra* note 18, at 286.

115 See generally Ellen P. Goodman, Stealth Marketing and Editorial Integrity, 85 TEX. L. REV. 83 (2006).

116 *See* Letter from Heather Hippsley, Acting Assoc. Dir., Div. of Adver. Practices, Fed. Trade Comm., to Gary Ruskin, Executive Dir. at Commercial Alert (June 27, 2007), available at **http://www.ftc.gov/os/closings/staff/commercialalertletter.shtm**.

117 16 CFR § 255.1(a).

118 16 CFR § 255.5.

119 Disclosure in common cases need not be onerous. Where, for example, a search engine auctions off sponsored links on its results pages, telling users that those links *are* auctioned off should generally suffice. *See generally* Letter from Heather Hippsley, *supra* note 116.

120 Introna and Nissenbaum, *supra* note 68, at 181.

121 *Search Neutrality*, SEARCHNEUTRALITY.ORG (Oct. 11, 2009), **http://www.searchneutrality.org/search-neutrality**.

- Pasquale: "[Dominant search engines] should submit to regulation that bans stealth marketing *and reliably verifies the absence of the practice*."[122]

These disclosures are meant to inform users about what they're getting from a search engine (Introna and Nissenbaum), to inform websites about the standards they're being judged by (Foundem),[123] or to inform regulators about what the search engine is actually doing (Pasquale).[124]

Algorithmic transparency is a delicate business. Full disclosure of the algorithm itself runs up against critical interests of the search engine. A fully public algorithm is one that the search engine's competitors can copy wholesale.[125] Worse, it is one that websites can use to create highly optimized search-engine spam.[126] Writing in 2000, long before the full extent of search-engine spam was as clear as it is today, Introna and Nissenbaum thought that the "impact of these unethical practices would be severely dampened if both seekers and those wishing to be found were aware of the particular biases inherent in any given search engine."[127] That underestimates the scale of the problem. Imagine instead your inbox without a spam filter. You would doubtless be "aware of the particular biases" of the people trying to sell you fancy watches and penis pills—but that will do you little good if your inbox contains a thousand pieces of spam for every email you want to read. That is what will happen to search results if search algorithms are fully public; the spammers will win.

For this reason, search-neutrality advocates now acknowledge the danger of SEO and thus propose only limited transparency.[128] Pasquale suggests, for example, that Google could respond to a question about its rankings with a list of a few factors that principally affected a particular result.[129] But search is immensely complicated—so complicated that it may not be possible to boil a ranking down to a simple explanation. When the law demands disclosure of complex matters in simple terms, we get pro forma statements and boilerplate.

---

122 Pasquale, *Internet Nondiscrimination Principles*, *supra* note 18, at 299 (emphasis added).

123 *See also id.* at 285 (arguing that search engines benefit from hidden algorithms because websites, lacking clear information about how to achieve high organic search rankings, must resort to buying paid search ads).

124 *See also The Google Algorithm*, *supra* note 13 (recommending required disclosure).

125 *See* Grimmelmann, *Structure of Search Engine Law*, *supra* note 4, at 49, 55.

126 *Id.* at 44–46, 56.

127 Introna and Nissenbaum, *supra* note 68, at 181.

128 *See* Pasquale, *Internet Nondiscrimination Principles*, *supra* note 18, at 297; Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1201–02; Chandler, *Right to Reach an Audience*, *supra* note 20, at 1117.

129 Pasquale, *Internet Nondiscrimination Principles*, *supra* note 18, at 296–97.

Consumer credit disclosures and securities prospectuses have brought important information into the open, but they haven't done much to aid the understanding of their average recipient.

Google's algorithm depends on more than 200 different factors.[130] Google makes about 500 changes to it a year,[131] based on ten times as many experiments.[132] One sixth of the hundreds of millions of queries the algorithm handles daily are queries it has never seen before.[133] The PageRank of any webpage depends, in part, on every other page on the Internet.[134] And even with all the computational power Google can muster, a full PageRank recomputation takes weeks.[135] PageRank is, as algorithms go, elegantly simple—but I certainly wouldn't want to have the job of making Markov chains and eigenvectors "meaningful to the majority of Web users."[136] In practice, any simplified disclosure is likely to leave room for the search engine to bury plenty of bodies.

Some scholars have suggested that concerns about transparency could be handled through regulatory opacity: The search engine discloses its algorithm to the government, which then keeps the details from the public.[137] This is a promising way of dealing with search engines' operational needs for secrecy, but it sharpens the question of regulators' technical competence. If the record is sealed, they won't have third-party experts and interested amici to walk them through novel technical issues. Everything will hinge on their own ability to evaluate the implications of small details in search algorithms. The track record of agencies and courts in dealing with other digital technologies does not provide grounds for optimism on this score.[138] Pasquale makes an important

---

130 *See, e.g.*, *Technology Overview*, GOOGLE, **http://www.google.com/corporate/tech.html**.

131 *See* Steven Levy, *Inside the Box*, WIRED, Mar. 2010, at 96.

132 *See* Rob Hof, *Google's Udi Manber: Search Is About People, Not Just Data*, THE TECH BEAT (Oct. 1, 2009), **http://www.businessweek.com/the_thread/techbeat/archives/2009/10/googles_udi_manber_search_is_about_people_not_just_data.html**.

133 *Id.*

134 *See* AMY N. LANGVILLE & CARL D. MEYER, GOOGLE'S PAGERANK AND BEYOND: THE SCIENCE OF SEARCH (Princeton University Press 2006).

135 *Id.*

136 In *The Google Dilemma*, *supra* note 63, I didn't even try to explain the math to law professors.

137 Pasquale, *Internet Nondiscrimination Principles, supra* note 18 at 297–98; Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1294–96. *See generally* Viva R. Moffat, *Regulating Search*, 22 HARV. J. L. & TECH. 475 (2009) (discussing institutional choice issues in search regulation).

138 *But see* Frank Pasquale, *Trusting (and Verifying) Online Intermediaries' Policing, supra* at 258 (proposing "Internet Intermediary Regulatory Council" and arguing that it could develop

point that "it is essential that *someone* has the power to 'look under the hood,'"[139] but it is also important that algorithmic disclosure remain connected to a workable theory of what regulators are looking for and what they would do if they found it.

## Manipulation

Perhaps the most interesting idea in the entire search neutrality debate is the "manipulation" of search results. It's a slippery term, and used inconsistently in the search-engine debates—including by me.[140] In the dictionary sense of "process, organize, or operate on mentally or logically; to handle with mental or intellectual skill,"[141] all search results are manipulated and the more skillfully the better. But in the dictionary sense of "manage, control, or influence in a subtle, devious, or underhand manner,"[142] it's a bad thing indeed: no one likes to be manipulated.[143]

In practice—although this is rarely made explicit—the concern is with what I have described elsewhere as "hand manipulation."[144] This idea imagines the search engine as having both an automatic, general-purpose ranking algorithm and a human-created list of exceptions. Consumer Watchdog, for example, derides Google's claim to rank results "automatically by algorithms," saying, "It is hard to see how this can still be true, given the increasingly pronounced tilt toward its own services in Google's search results."[145] Foundem calls it "manual intervention," "special treatment," and "manual bias," and documents how Google's public statements have quietly backed away from claims that its rankings are "objective" and "automatic."[146]

Put this way, the distinction between objective algorithm and subjective manipulation is incoherent. Both kinds of decisions come from the same

---

sufficient technical expertise to "generate official and even public understanding of [search engines'] practices").

139 Pasquale, *Internet Nondiscrimination Principles*, *supra* note 18, at 286.

140 *Compare* Grimmelmann, *Structure of Search Engine Law*, *supra* note 4, at 44 ("technical arms race between engines and manipulators") *with id.*, at 59–60 ("hand manipulation of results [by search engines]").

141 Oxford English Dictionary (June 2010 draft).

142 *Id.*

143 *See* Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1176–79 (discussing effects of manipulation on user autonomy).

144 Grimmelmann, *Structure of Search Engine Law*, *supra* note 4, at 59.

145 TRAFFIC REPORT, *supra* note 101, at 8.

146 *Foundem's Google Story*, *supra* note 7.

source: the search engine's programmers.[147] Nor can the algorithm provide a stable baseline against which to measure manipulation, since each "manipulation" is a change to the algorithm itself. It's not like Bing has rooms full of employees looking over search results pages and making last-minute tweaks before the pages are delivered to users.

Academics, being more careful with concepts, have focused on intentionality: does the search engine intend the promotions and demotions that will result from an algorithmic change? Mark Patterson, for example, refers to "intentional manipulation of results."[148] Bracha and Pasquale sharpen this idea to speak of "highly specific or local manipulations," such as singling out websites for special treatment.[149] Chandler argues that "search engines should not manipulate *individual* search results except to address instances of suspected abuse."[150] Google itself is remarkably coy about whether and when it changes rankings on an individual basis.[151]

Surprisingly, no one has explained why special-casing in and of itself is a problem. One possibility is that it captures the distinction between individual adjudication and general rulemaking: changes that only affect a few websites trigger a kind of due process interest in individualized procedural protections.[152] There is also a kind of Rawlsian argument[153] here, that algorithmic decisions should be made from behind a veil of ignorance, not knowing which websites they will favor. For whatever reason, local manipulations make people nervous, nervous enough that most of the stories told to instill fear of search engines involve what is or looks like manipulation.[154]

Local manipulation, however, is a distraction. The real goal is relevance. From that point of view, most local manipulations aren't wrongful at all. Foundem should know; it benefited from a local manipulation. The penalty that afflicted

---

147 *See* Goldman, *Search Engine Bias*, *supra* note 28, at 112–15; Grimmelmann, *Structure of Search Engine Law*, *supra* note 4, at 59–60.

148 Patterson, *Non-Network Barriers*, *supra* note 19, at 2854.

149 Bracha & Pasquale, *Federal Search Commission*, *supra* note 20, at 1168.

150 Chandler, *Right to Reach an Audience*, *supra* note 20, at 1117 (emphasis added).

151 *See, e.g.*, Lettice, *When Algorithms Attack*, *supra* note 99; James Grimmelmann, *Google Replies to SearchKing Lawsuit,* LAWMEME (Jan. 9, 2003), **http://lawmeme.research.yale.edu/modules.php?name=News&file=article&sid=807**.

152 *Compare* Londoner v. Denver, 210 U.S. 373, 386 (1908) (hearing required when tax assessment affects only a few people) *with* Bi-Metallic Inv. Co. v. Colorado, 239 U.S. 441, 445–46 (hearing not required when tax assessment affects all citizens equally).

153 *See* JOHN RAWLS, A THEORY OF JUSTICE (1971).

154 *See, e.g.*, Lettice, *When Algorithms Attack*, *supra* note 99.

it for three years appears to have been a relatively general change to Google's algorithm, one designed to affect a great many low-value vertical search sites.[155] When Foundem was promoted back to prominent search placement, *that* was actually the manipulation, since it affected Foundem and Foundem alone. Google thus "manipulated" its search results to exempt Foundem from what would otherwise have been a generally applicable rule. To condemn manipulation on the basis of its specificity is to say that Google acted more rightfully when it demoted Foundem in 2006 than when it promoted it back in 2009.[156]

The point is that local manipulations, being quick and easy to implement, are often a useful part of a search engine's toolkit for delivering relevance. Search-engine-optimization is an endless game of loopholing. Regulators who attempt to prohibit unfair manipulations will have to wade quite far into the swamp of white-hat and black-hat SEO.[157] Prohibiting local manipulation altogether would keep the search engine from closing loopholes quickly and punishing the loopholers—giving them a substantial leg up in the SEO wars. Search results pages would fill up with spam, and users would be the real losers.

## Conclusion

Search neutrality gets one thing very right: Search is about user autonomy. A good search engine is more exquisitely sensitive to a user's interests than *any other communications technology*.[158] Search helps her find whatever she wants, whatever she needs to live a self-directed life. It turns passive media recipients into active seekers and participants. If search did not exist, then for the sake of human freedom it would be necessary to invent it. Search neutrality properly seeks to make sure that search is living up to its liberating potential.

Having asked the right question—*are structural forces thwarting search's ability to promote user autonomy?*—search neutrality advocates give answers concerned with protecting websites rather than users. With disturbing frequency, though, websites are not users' friends. Sometimes they are, but often, the websites want visitors, and will be willing to do what it takes to grab them.

---

155 *Id.*

156 If you are bothered more by demotions than promotions, remember that search rankings are zero-sum. Foundem's 50-place rise is balanced out by 50 one-place falls for other websites.

157 On the distinction between ethical, permitted "white-hat" SEO and unethical, forbidden "black-hat" SEO, see Frank Pasquale, *Trusting (and Verifying) Online Intermediaries' Policing*, *supra* at 258. I believe that what Pasquale calls the intermediate "grey-hat" zone between the two is generally less grey than he and his sources perceive it to be.

158 Except, perhaps, the library reference desk. Unfortunately, librarians don't scale.

If Flowers by Irene sells a bouquet for $30 that Bob's Flowers sells for $50, then Bob's interest in being found is in direct conflict with users' interest in being directed to Irene. The last thing that Bob wants is for the search engine to maximize relevance. Search-neutrality advocates fear that Bob will pay off the search engine to point users at his site. But that's not the only way the story can play out. Bob could also engage in self-help SEO to try to boost his ranking. In that case, the search engine may respond by demoting his site. And if that happens, then Bob has another card to play: search-neutrality itself.

Regulators bearing search neutrality can inadvertently prevent search engines from helping users find the websites they want. The typical model assumed by search neutrality is of a website and a search engine corruptly conspiring to put one over on users. But much, indeed most, of the time, the real alliance is between search engines and users, together trying to sort through the clamor of millions of websites' sales pitches. Giving websites search-neutrality rights gives them a powerful weapon in their wars with each other—one that need not be wielded with users' interests in mind.[159] Search neutrality will be born with one foot already in the grave of regulatory capture.

There is a profound irony at the heart of the liberal case for search neutrality. Requiring search *engines* to behave "neutrally" will not produce the desired goal of neutral search *results*. The web is a place where site owners compete fiercely, sometimes viciously, for viewers and users turn to intermediaries to defend them from the sometimes-abusive tactics of information providers. Taking the search engine out of the equation leaves users vulnerable to precisely the sorts of manipulation search neutrality aims to protect them from. Whether it ranks sites by popularity, by personalization, or even by the idiosyncratic whims of its operator, a search engine provides an *alternative* to the Hobbesian world of the unmediated Internet, in which the richest voices are the loudest, and the greatest authority on any subject is the spammer with the fastest server. Search neutrality is cynical about the Internet—but perhaps not cynical enough.

---

[159] This has already happened in trademark law, which is supposed to prevent consumer confusion, but just as often is a form of offensive warfare among companies, consumer interests be damned. *See* Mark A. Lemley & Mark P. McKenna, *Owning Mark(et)s* (Stanford Law and Economics Olin Working Paper No. 395, May 2010), *available at* **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1604845**. For an exploration of the competitive dynamics of trademark in the search-engine context, *see* Goldman, *Deregulating Relevancy*, *supra* note 61.

# Search Engine Bias & the Demise of Search Engine Utopianism

By Eric Goldman*

In the past few years, search engines have emerged as a major force in our information economy, helping searchers perform hundreds of millions (or even billions) of searches per day.[1] With this broad reach, search engines have significant power to shape searcher behavior and perceptions. In turn, the choices that search engines make about how to collect and present data can have significant social implications.

Typically, search engines automate their core operations, including the processes that search engines use to aggregate their databases and then sort/rank the data for presentation to searchers. This automation gives search engines a veneer of objectivity and credibility.[2] Machines, not humans, appear to make the crucial judgments, creating the impression that search engines bypass the structural biases and skewed data presentations inherent in any human-edited media.[3] Search engines' marketing disclosures typically reinforce this perception of objectivity.

Unfortunately, this romanticized view of search engines does not match reality. Search engines are media companies. Like other media companies, search

---

* Associate Professor, Santa Clara University School of Law and Director, High Tech Law Institute. Home page: **http://www.ericgoldman.org**. Email: **egoldman@gmail.com**. I appreciate the comments of Nico Brooks, Soumen Chakrabarti, Ben Edelman, Elizabeth Van Couvering and the participants at the Yale Law School Regulating Search Symposium and the 2005 Association of Internet Researchers (AoIR) Annual Meeting. This essay focuses principally on American law and consumer behavior. Consumer behavior and marketplace offerings vary by country, so this discussion may not be readily generalizable to other jurisdictions.

1 In 2003, search engines performed over a half-billion searches a day. *See* Danny Sullivan, *Searches Per Day*, SEARCH ENGINE WATCH, Feb. 25, 2003, **http://searchenginewatch.com/reports/article.php/2156461**.

2 *See* Jason Lee Miller, *Left, Right, or Center? Can a Search Engine Be Biased?*, WEBPRONEWS.COM, May 10, 2005, **http://www.webpronews.com/insidesearch/insidesearch/wpn-56-20050510LeftRightorCenterCanaSearchEngineBeBiased.html**.

3 There is a broad perception that search engines present search results passively and neutrally. *See* Leslie Marable, *False Oracles: Consumer Reaction to Learning the Truth About How Search Engines Work*, CONSUMER REPORTS WEBWATCH, June 30, 2003, **http://www.consumerwebwatch.org/dynamic/search-report-false-oracles-abstract.cfm**; Maureen O'Rourke, *Defining the Limits of Free-Riding in Cyberspace: Trademark Liability for Metatagging*, 33 GONZ. L. REV. 277 (1998).

engines make editorial choices designed to satisfy their audience.[4] These choices systematically favor certain types of content over others, producing a phenomenon called "search engine bias."

Search engine *bias* sounds scary, but this essay explains why such bias is both necessary and desirable. The essay also explains how emerging personalization technology will soon ameliorate many concerns about search engine bias.

## Search Engines Make Editorial Choices

Search engines frequently claim that their core operations are completely automated and free from human intervention,[5] but this characterization is false. Instead, humans make numerous editorial judgments about what data to collect and how to present that data.[6]

*Indexing.* Search engines do not index every scrap of data available on the Internet. Search engines omit (deliberately or accidentally) some web pages entirely[7] or may incorporate only part of a web page.[8]

---

4 *See*, *e.g.*, C. EDWIN BAKER, ADVERTISING AND A DEMOCRATIC PRESS (1994).

5 *See*, *e.g.*, *Does Google Ever Manipulate Its Search Results?*, GOOGLE.COM, **http://www.google.com/support/bin/answer.py?answer=4115&topic=368** ("The order and contents of Google search results are completely automated. No one hand picks a particular result for a given search query, nor does Google ever insert jokes or send messages by changing the order of results."); *Does Google Censor Search Results?*, GOOGLE.COM, **http://www.google.com/support/bin/answer.py?answer=17795&topic=368** ("Google does not censor results for any search terms. The order and content of our results are completely automated; we do not manipulate our search results by hand."); *Technology Overview*, GOOGLE.COM, **http://www.google.com/corporate/tech.html** ("There is no human involvement or manipulation of results…."); *How Can I Improve My Site's Ranking?*, GOOGLE.COM, **http://www.google.com/support/webmasters/bin/answer.py?answer=34432&topic=8524** ("Sites' positions in our search results are determined automatically based on a number of factors, which are explained in more detail at **http://www.google.com/technology/index.html**. We don't manually assign keywords to sites, nor do we manipulate the ranking of any site in our search results.") *see also* Complaint at ¶¶ 37-38, 52-56, KinderStart.com LLC v. Google, Inc., Case No. C 06-2057 RS (N.D. Cal. Mar. 17, 2006) (giving other examples of Google's claims to be passive). Note that Google has subsequently revised some of these cited pages after its censorship controversy in China.

6 *See generally* Abbe Mowshowitz & Akira Kawaguchi, *Bias on the Web*, COMM. ACM, Sept. 2002, at 56 (distinguishing "indexical bias" and "content bias").

7 *See* Judit Bar-Ilan, *Expectations Versus Reality – Search Engine Features Needed for Web Research at Mid-2005*, 9 CYBERMETRICS 2 (2005), **http://www.cindoc.csic.es/cybermetrics/articles/v9i1p2.html**.

8 For example, many search engines ignore metatags. *See* Eric Goldman, *Deregulating Relevancy in Internet Trademark Law*, 54 EMORY L.J. 507, 567-68 (2005). Search engines also incorporate only portions of very large files. *See* Bar-Ilan, *supra* note 7; *Why Doesn't My Site Have a Cached Copy or a Description?*, GOOGLE.COM, **http://www.google.com/support/bin/answer.py?answer=515&topic=365** (describing how some pages are "partially indexed");

During indexing, search engines are designed to associate third party "metadata" (data about data) with the indexed web page. For example, search engines may use and display third party descriptions of the website in the search results.[9] Search engines may also index "anchor text" (the text that third parties use in hyperlinking to a website),[10] which can cause a website to appear in search results for a term the website never used (and may object to).[11]

Finally, once indexed, search engines may choose to exclude web pages from their indexes for a variety of reasons, ranging from violations of quasi-objective search engine technical requirements[12] to simple capriciousness.[13]

*Ranking.* To determine the order of search results, search engines use complex proprietary "ranking algorithms." Ranking algorithms obviate the need for humans to make individualized ranking decisions for the millions of search

---

*Has Google Dropped Their 101K Cache Limit?*, RESEARCHBUZZ!, Jan. 31, 2005, **http://www.researchbuzz.org/2005/01/has_google_dropped_their_101k.shtml** (discussing how historically Google indexed only the first 101k of a document).

9 *See My Site's Listing Is Incorrect and I Need it Changed*, GOOGLE.COM, **http://www.google.com/webmasters/3.html**. Google's automated descriptions have spawned at least one lawsuit by a web publisher who believed the compilation created a false characterization. *See* Seth Fineberg, *Calif. CPA Sues Google Over "Misleading" Search Results*, ACCT. TODAY, Apr. 19, 2004, at 5, *available at* **http://www.webcpa.com/article.cfm?articleid=193&pg-acctoday&print=yes**.

10 *See* Jagdeep S. Pannu, *Anchor Text Optimization*, WEBPRONEWS.COM, Apr. 8, 2004, **http://www.webpronews.com/ebusiness/seo/wpn-4-20040408AnchorTextOptimization.html**.

11 For example, the first search result in Google and Yahoo! for the keyword "miserable failure" is President George W. Bush's home page because so many websites have linked to the biography using the term "miserable failure." *See* Tom McNichol, *Your Message Here*, N.Y. TIMES, Jan. 22, 2004, at G1. This algorithmic vulnerability has spawned a phenomenon called "Google bombing," where websites coordinate an anchor text attack to intentionally distort search results. *See* John Hiler, *Google Time Bomb*, MICROCONTENT NEWS, Mar. 3, 2002, **http://www.microcontentnews.com/articles/googlebombs.htm**.

12 *See, e.g.*, Stefanie Olsen, *Search Engines Delete Adware Company*, CNET NEWS.COM, May 13, 2004, **http://news.com.com/2102-1024_3-5212479.html?tag=st.util.print** (Google and Yahoo kicked WhenU.com out of their indexes for allegedly displaying different web pages to searchers and search engine robots, a process called "cloaking").

13 This is the heart of KinderStart's allegations against Google. *See* Complaint, KinderStart.com LLC v. Google, Inc., Case No. C 06-2057 (N.D. Cal. Mar. 17, 2006). Although the complaint's allegations about Google's core algorithmic search may not be proven, Google does liberally excise sources from Google News. For example, Google claims that "news sources are selected without regard to political viewpoint or ideology," *see Google News (Beta)*, GOOGLE.COM, **http://news.google.com/intl/en_us/about_google_news.html#25**, but Google dropped a white supremacist news source from Google News because it allegedly promulgated "hate content." *See* Susan Kuchinskas, *Google Axes Hate News*, INTERNETNEWS.COM, Mar. 23, 2005, **http://www.internetnews.com/xSP/article.php/3492361**.

terms used by searchers, but they do not lessen the role of human editorial judgment in the process. Instead, the choice of which factors to include in the ranking algorithm (and how to weight them) reflects the search engine operator's editorial judgments about what makes content valuable. Indeed, to ensure that these judgments are producing the desired results, search engines manually inspect search results[14] and make adjustments accordingly.

Additionally, search engines claim they do not modify algorithmically-generated search results, but there is some evidence to the contrary. Search engines allegedly make manual adjustments to a web publisher's overall ranking.[15] Also, search engines occasionally modify search results presented in response to particular keyword searches. Consider the following:

- Some search engines blocked certain search terms containing the keyword "phpBB."[16]
- In response to the search term "Jew," for a period of time (including, at minimum November 2005 when the author observed the phenomenon), Google displayed a special result in the sponsored link, saying "Offensive Search Results: We're disturbed about these results as well. Please read our note here." The link led to a page explaining the results.[17]
- Reportedly, Ask.com blocked search results for certain terms like "pedophile," "bestiality," "sex with children" and "child sex."[18]
- Google removed some websites from its index in response to a Digital Millenium Copyright Act (DMCA) take-down demand from the Church of Scientology. However, Google displayed the following legend at the bottom of affected search results pages (such as search results for "scientology site:xenu.net"): "In response to a complaint we received under the US Digital Millennium Copyright Act, we have

---

14 *See* Posting of Eric Goldman to Technology & Marketing Law Blog, *Google's Human Algorithm*, **http://blog.ericgoldman.org/archives/2005/06/googles_human_a.htm** (June 5, 2005, 14:11 EST) (Google hires students to manually review search results for quality purposes).

15 *See* Search King, Inc. v. Google Tech., Inc., No. CIV-02-1457-M, at 4 (W.D. Okla. Jan. 13, 2003) ("Google knowingly and intentionally decreased the PageRanks assigned to both SearchKing and PRAN."). This manual adjustment has also been alleged in the recent *KinderStart* lawsuit. *See* Complaint, KinderStart.com L.L.C. v. Google, Inc., Case No. C 06-2057 RS (N.D. Cal. Mar. 17, 2006).

16 *See MSN Blockades phpBB Searchers*, TRIMMAIL'S EMAIL BATTLES, Jan. 18, 2006, **http://www.emailbattles.com/archive/battles/vuln_aacgfbgdcb_jd/**.

17 *See* **http://www.google.com/explanation.html**.

18 *See* Jennifer Laycock, *Ask.com Actively Censoring Some Search Phrases*, SEARCH ENGINE GUIDE, June 25, 2006, **http://www.searchengineguide.com/searchbrief/senews/007837.html**. On Aug. 1, 2006, I was unable to replicate these results.

> removed 2 result(s) from this page. If you wish, you may read the DMCA complaint that caused the removal(s) at ChillingEffects.org."[19]

*Conclusion.* Search engines have some duality in their self-perceptions, and this duality creates much confusion.[20] Search engines perceive themselves as objective and neutral because they let automated technology do most of the hard work. However, in practice, search engines make editorial judgments just like any other media company. Principally, these editorial judgments are instantiated in the parameters set for the automated operations, but search engines also make individualized judgments about what data to collect and how to present it. These manual interventions may be the exception and not the rule, but these exceptions only reinforce that search engines play an active role in shaping their users' experiences when necessary to accomplish their editorial goals.

## Search Engine Editorial Choices Create Biases

Search results ordering has a significant effect on searchers and web publishers. Searchers usually consider only the top few search results; the top-ranked search result gets a high percentage of searcher clicks, and click-through rates quickly decline from there.[21] Therefore, even if a search engine delivers hundreds or even thousands of search results in response to a searcher's query, searchers

---

19 *See* Chris Sherman, *Google Makes Scientology Infringement Demand Public*, SEARCH ENGINE WATCH, Apr. 15, 2002, **http://searchenginewatch.com/searchday/article.php/2159691**.

20 *See* Danny Sullivan, *KinderStart Becomes KinderStopped In Ranking Lawsuit Against Google*, SEARCH ENGINE WATCH, July 14, 2006, **http://blog.searchenginewatch.com/blog/060714-084842**. This duality, if it ends up leading to the dissemination of false information, could also create some legal liability. *See* KinderStart v. Google, No. 5:06-cv-02057-JF (N.D. Cal. motion to dismiss granted July 13, 2006) (pointing out the potential inconsistency of Google's position that PageRank is both Google's subjective opinion but an objective reflection of its algorithmic determinations).

21 *See iProspect Search Engine User Behavior Study*, IPROSPECT, Apr. 2006, **http://www.iprospect.com/premiumPDFs/WhitePaper_2006_SearchEngineUserBehavior.pdf** (62% of searchers click on a search result on the first results page); Jakob Nielsen, *The Power of Defaults*, JAKOB NIELSEN'S ALERTBOX, Sept. 26, 2005, **http://www.useit.com/alertbox/defaults.html** (citing a study by Cornell professor Thorsten Joachims that the first search result gets 42% of clicks and the second search result gets 8%; further, when the first two search results are switched, the first search result gets 34%—meaning that positioning dictated searcher behavior); Nico Brooks, *The Atlas Rank Report: How Search Engine Rank Impacts Traffic*, ATLAS INSTITUTE DIGITAL MARKETING INSIGHTS, June 2004, **http://app.atlasonepoint.com/pdf/AtlasRankReport.pdf** (the first-ranked search result may get ten times the quantity of clicks as the tenth-ranked search result).

effectively ignore the vast majority of those search results. Accordingly, web publishers desperately want to be listed among the top few search results.[22]

For search engines, results placement determines how the searcher perceives the search experience. If the top few search results do not satisfy the searcher's objectives, the searcher may deem the search a failure. Therefore, to maximize searcher perceptions of search success, search engines generally tune their ranking algorithms to support majority interests.[23] In turn, minority interests (and the websites catering to them) often receive marginal exposure in search results.

To gauge majority interests, search engines frequently include a popularity metric in their ranking algorithm. Google's popularity metric, PageRank, treats inbound links to a website as popularity votes, but votes are not counted equally; links from more popular websites count more than links from lesser-known websites.[24]

Beyond promoting search results designed to satisfy majority interests, PageRank's non-egalitarian voting structure causes search results to be biased towards websites with economic power[25] because these websites get more links due to their marketing expenditures and general prominence.

Indeed, popularity-based ranking algorithms may reinforce and perpetuate existing power structures.[26] Websites that are part of the current power elite get better search result placement, which leads to greater consideration of their messages and views. Furthermore, the increased exposure attributable to better placement means that these websites are likely to get more votes in the future,

---

22 *See* Michael Totty & Mylene Mangalindan, *Web Sites Try Everything To Climb Google Rankings*, WALL ST. J. ONLINE, Feb. 26, 2003, **http://online.wsj.com/article/SB104622616088496394 3.html?emailf=yes**.

23 *See* Lucas D. Introna & Helen Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, INFO. SOC'Y, July-Sept. 2000, at 169.

24 *See Our Search: Google Technology*, GOOGLE.COM, **http://www.google.com/technology/**.

25 *See* Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. DAYTON L. REV. 179, 188 (2001); Frank Pasquale, *Rankings, Reductionism, and Responsibility*, SETON HALL PUBLIC LAW RESEARCH PAPER NO. 888327, at 25, Feb. 25, 2006, **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=888327**; Trystan Upstill et al., *Predicting Fame and Fortune: PageRank or Indegree?*, PROC. OF THE 8TH AUSTRALASIAN DOCUMENT COMPUTING SYMP., Dec. 15, 2003, **http://research.microsoft.com/users/nickcr/pubs/upstill_adcs03.pdf** (showing that BusinessWeek Top Brand, Fortune 500 and Fortune Most Admired companies get disproportionately high PageRank).

26 *See* Introna & Nissenbaum, *supra* note 23; Matthew Hindman et al., *"Googlearchy": How a Few Heavily-Linked Sites Dominate Politics on the Web*, Mar. 31, 2003, **http://www.princeton.edu/~mhindman/googlearchy--hindman.pdf**.

leading to a self-reinforcing process.[27] In contrast, minority-interest and disenfranchised websites may have a difficult time cracking through the popularity contest, potentially leaving them perpetually relegated to the search results hinterlands.[28]

A number of commentators have lamented these effects and offered some proposals in response:

- *Improve Search Engine Transparency.* Search engines keep their ranking algorithms secret.[29] This secrecy hinders search engine spammers from gaining more prominence than search engines want them to have, but the secrecy also prevents searchers and commentators from accurately assessing any bias. To enlighten searchers, search engines could be required to disclose more about their practices and their algorithms.[30] This additional information has two putative benefits. First, it may improve market mechanisms by helping searchers make informed choices among search engine competitors. Second, it may help searchers determine the appropriate level of cognitive authority to assign to their search results.
- *Publicly Fund Search Engines.* Arguably, search engines have "public good"-like attributes, such as reducing the social costs of search behavior. If so, private actors will not incorporate these social benefits into their decision-making. In that case, public funding of search engines may be required to produce socially-optimal search results.[31]

---

27 *See Egalitarian Engines*, ECONOMIST, Nov. 17, 2005 ("there is a widespread belief among computer, social and political scientists that search engines create a vicious circle that amplifies the dominance of established and already popular websites"); *see also* Junghoo Cho & Sourashis Roy, *Impact of Search Engines on Page Popularity*, WWW 2004, May 2004, **http://oak.cs.ucla.edu/~cho/papers/cho-bias.pdf**; Upstill, *supra* note 25. *But see* Santo Fortunato et al., *The Egalitarian Effect of Search Engines*, Nov. 2005, **http://arxiv.org/pdf/cs.CY/0511005** (questioning the consequences of the "rich-gets-richer" effect).

28 *See* Cho & Roy, *supra* note 27; *but see* Filippo Menczer et al., *Googlearchy or Googlocracy?*, IEEE SPECTRUM, Feb. 2006 (providing empirical evidence suggesting that "search engines direct more traffic than expected to less popular sites").

29 *See* Search King Inc. v. Google Tech., Inc., No. CIV-02-1457-M, at 3 n.2 (W.D. Okla. Jan. 13, 2003) ("Google's mathematical algorithm is a trade secret, and it has been characterized by the company as 'one of Google's most valuable assets.'"); Stefanie Olsen, *Project Searches for Open-Source Niche*, CNET NEWS.COM, Aug. 18, 2003, **http://news.com.com/2102-1032_3-5064913.html?tag=st_util_print**.

30 *See* Introna & Nissenbaum, *supra* note 23.

31 *See id.*; Eszter Hargittai, *Open Portals or Closed Gates? Channeling Content on the World Wide Web*, 27 POETICS 233 (2000); *cf.* CASS SUNSTEIN, REPUBLIC.COM 170-72 (2001) (advocating publicly funded "deliberative domains").

Indeed, there have been several proposals to create government-funded search engines.[32]

- *Mandate Changes to Ranking/Sorting Practices.* Search engines could be forced to increase the exposure of otherwise-marginalized websites. At least five lawsuits[33] have requested judges to force search engines to reorder search results to increase the plaintiff's visibility.[34]

In addition to plaintiffs, some academics have supported mandatory reordering of search results. For example, Pandey et al. advocate a "randomized rank promotion" scheme where obscure websites randomly should get extra credit in ranking algorithms, appearing higher in the search results on occasion and getting additional exposure to searchers accordingly.[35] In another essay in this collection, Frank Pasquale proposes that, when people think the search engines are providing false or misleading information, search engines should be forced to include a link to corrective information.[36]

## Search Engine Bias Is Necessary and Desirable

Before trying to solve the problem of search engine bias, we should be clear how search engine bias creates a problem that requires correction. From my perspective, search engine bias is the unavoidable consequence of search

---

32 *See* Kevin J. O'Brien, *Europeans Weigh Plan on Google Challenge*, INT'L HERALD TRIB., Jan. 18, 2006 (discussing a European initiative called Quaero, which is intended to break the American hegemony implicit in Google's dominant market position); Graeme Wearden, *Japan May Create Its Own Search Engine*, CNET NEWS.COM, Dec. 21, 2005, **http://news.com.com/Japan+may+create+its+own+search+engine/2100-1025_3-004037.html**.

33 *See* Search King, Inc. v. Google Tech., Inc., No. CIV-02-1457-M (W.D. Okla. Jan. 13, 2003); KinderStart.com LLC v. Google, Inc., No. C 06-2057 RS (N.D. Cal. dismissed July 13, 2006); Langdon v. Google, Inc., No. 1:06-cv-00319-JJF (D. Del. complaint filed May 17, 2006); Roberts v. Google, No. 1-06-CV-063047 (Cal. Superior Ct. complaint filed May 5, 2006); Datner v. Yahoo! Inc, Case No. BC355217 (Cal. Superior Ct. complaint filed July 11, 2006) [note: this list updated as of July 24, 2006].

34 As Google said in its response to the KinderStart lawsuit, "Plaintiff KinderStart contends that the judiciary should have the final say over [search engines'] editorial process. It has brought this litigation in the hopes that the Court will second-guess Google's search rankings and order Google to view KinderStart's site more favorably." Motion to Dismiss at 1, KinderStart.com LLC v. Google, Inc., No. C 06-2057 RS (N.D. Cal. May 2, 2006).

35 *See* Sandeep Pandey et al., *Shuffling a Stacked Deck: the Case for Partially Randomized Ranking of Search Engine Results*, **http://www.cs.cmu.edu/~olston/publications/randomRanking.pdf**; *cf.* SUNSTEIN, *supra* note 31 (explaining that websites should be forced to link to contrary views as a way of increasing exposure to alternative viewpoints).

36 *See* Pasquale, *supra* at 401; *see also* Pasquale, *supra* note 25, at 28-30 (proposing that the link be displayed as an asterisk to the search results).

engines exercising editorial control over their databases. Like any other media company, search engines simply cannot passively and neutrally redistribute third party content (in this case, web publisher content). If a search engine does not attempt to organize web content, its system quickly and inevitably will be overtaken by spammers, fraudsters and malcontents.[37] At that point, the search engine becomes worthless to searchers.

Instead, searchers (like other media consumers) expect search engines to create order from the information glut. To prevent anarchy and preserve credibility, search engines must exercise some editorial control over their systems. In turn, this editorial control necessarily will create some bias.

Fortunately, market forces limit the scope of search engine bias.[38] Searchers have high expectations for search engines: they expect search engines to read their minds[39] and infer their intent based solely on a small number of search keywords.[40] Search engines that disappoint (either by failing to deliver relevant results, or by burying relevant results under too many unhelpful results) are held

---

37 Every Internet venue accepting user-submitted content inevitably gets attacked by unwanted content. If left untended, the venue inexorably degrades into anarchy. *See, e.g.*, *Step-by-Step: How to Get BILLIONS of Pages Indexed by Google*, MONETIZE BLOG, June 17, 2006, **http://merged.ca/monetize/flat/how-to-get-billions-of-pages-indexed-by-Google.html** (Google indexed over five billion "spam" pages from a single spammer before manually de-indexing the sites); Alorie Gilbert, *Google Fixes Glitch That Unleashed Flood of Porn*, CNET NEWS.COM, Nov. 28, 2005, **http://news.com.com/2102-1025_3-5969799.html?tag=st.util.print** (describing how Google Base, a venue for user-submitted content, was overtaken by pornographers: "the amount of adult content on Google Base was staggering considering Google only launched the tool a week ago."); Josh Quittner, *The War Between alt.tasteless and rec.pets.cats*, WIRED, May 1994, at 46 (describing how a group of anarchists, for fun, took over a USENET newsgroup about pets).

38 *See* Mowshowitz & Kawaguchi, *supra* note 6, at 60 (market forces are the best way to counter adverse effects of search engine bias).

39 *See Our Philosophy*, GOOGLE.COM, **http://www.google.com/corporate/tenthings.html** ("The perfect search engine … would understand exactly what you mean and give back exactly what you want."); Chris Sherman, *If Search Engines Could Read Your Mind*, SEARCH ENGINE WATCH, May 11, 2005, **http://searchenginewatch.com/searchday/article.php/3503931**.

40 Searchers routinely use a very small number of keywords to express their search interests. *See* iProspect.com, Inc., *iProspect Natural SEO Keyword Length Study*, Nov. 2004, **http://www.iprospect.com/premiumPDFs/keyword_length_study.pdf** (eighty-eight percent of search engine referrals are based on only one or two keywords); *see also* Declan Butler, *Souped-Up Search Engines*, NATURE, May 11, 2000, at 112, 115 (citing an NEC Research Institute study showing that up to 70% of searchers use only a single keyword as a search term); Bernard J. Jansen et al., *Real Life Information Retrieval: A Study of User Queries on the Web*, 32 SIGIR FORUM 5, 15 (1998) (stating that the average keyword length was 2.35 words; one-third of searches used one keyword and 80% used three keywords or fewer); Jakob Nielsen, JAKOB NIELSEN'S ALERTBOX, *Search: Visible and Simple*, May 13, 2001, **http://www.useit.com/alertbox/20010513.html** (stating that the average keyword length was 2.0 words).

accountable by fickle searchers.[41] There are multiple search engines available to searchers,[42] and few barriers to switching between them.[43]

As a result, searchers will shop around if they do not get the results they want,[44] and this competitive pressure constrains search engine bias. If a search engine's bias degrades the relevancy of search results, searchers will explore alternatives even if searchers do not realize that the results are biased. Meanwhile, search engine proliferation means that niche search engines can segment the market and cater to underserved minority interests.[45] Admittedly, these market forces

---

41 *See* Kim Peterson, *Microsoft Learns to Crawl*, SEATTLE TIMES, May 2, 2005 (MSN Search "learned that the arcane searches were the make-or-break moments for Web searchers. People weren't just happy when a search engine could find answers to their most bizarre, obscure and difficult queries. They would switch loyalties."); Bob Tedeschi, *Every Click You Make, They'll Be Watching You*, N.Y. TIMES, Apr. 3, 2006, **http://www.nytimes.com/2006/04/03/business/03ecom.html?ei=5090&en=9e55ae64f692433a&ex=1301716800&partner=rssuserland&emc=rss&pagewanted=print**.

42 In addition to the recent launch of major new search engines by providers like MSN, the open-source software community is developing Nutch to allow anyone to build and customize his or her own web search engine. **http://nutch.apache.org/**; *see also* Olsen, *Open-Source Niche*, *supra* note 29.While there are multiple major search engines, the market may still resemble an oligopoly; a few major players (Google, Yahoo, MSN, Ask Jeeves) have the lion's share of the search engine market. However, this may construe the search engine market too narrowly. Many types of search providers compete with the big mass-market search engines, ranging from specialty search engines (e.g., Technorati) to alternative types of search technology (e.g., adware) to non-search information retrieval processes (e.g., link navigation). Ultimately, every search engine competes against other search engines and these other search/retrieval options.

43 *See* Rahul Telang et al., *An Empirical Analysis of Internet Search Engine Choice*, Aug. 2002 (on file with author). For example, search engines use the same basic interface (a white search box), and searchers rarely use advanced search features that might require additional learning time at other search engines.

44 *See* Grant Crowell, *Understanding Searcher Behavior*, SEARCH ENGINE WATCH, June 14, 2006, **http://searchenginewatch.com/showPage.html?page=3613291** (citing a Kelsey Research study that 63% of searchers used two or more search engines); Press Release, Vividence, Inc., *Google Wins Users' Hearts, But Not Their Ad Clicks* (May 25, 2004), **http://www.vividence.com/public/company/news+and+events/press+releases/2004-05-25+ce+rankings+search.htm** (stating that up to 47% of searchers try another search engine when their search expectations are not met).

45 *See* Rahul Telang et al., *The Market Structure for Internet Search Engines*, 21 J. MGMT. INFO. SYS. 137 (2004), *available at* **http://www.heinz.cmu.edu/~rtelang/engine_jmis_final.pdf** (describing how searchers sample heterogeneous ranking algorithms, which support a diversity of search engines); Mário J. Silva, *The Case for a Portuguese Web Search Engine*, **http://xldb.fc.ul.pt/data/Publications_attach/tumba-icwi2003-final.pdf** (describing the value of a Portuguese-oriented search engine); Jeffrey McMurray, *Social Search Promises Better Intelligence*, ASSOCIATED PRESS, July 9, 2006 (discussing niche search engines that draw on social networking); *cf.* Jakob Nielsen, *Diversity is Power for Specialized Sites*, JAKOB NIELSEN'S ALERTBOX, June 16, 2003, **http://www.useit.com/alertbox/20030616.html** (describing how specialized sites will flourish on the Internet).

are incomplete—searchers may never consider what results they are not seeing—but they are powerful nonetheless.

In contrast, it is hard to imagine how regulatory intervention will improve the situation. First, regulatory solutions become a vehicle for normative views about what searchers should see—or should *want* to see.[46] How should we select among these normative views? What makes one bias better than another?

Second, regulatory intervention that promotes some search results over others does not ensure that searchers will find the promoted search results useful. Determining relevancy based on very limited data (such as decontextualized keywords) is a challenging process, and search engines struggle with this challenge daily. Due to the complexity of the relevancy matching process, government regulation rarely can do better than market forces at delivering results that searchers find relevant. As a result, searchers likely will find some of the promoted results irrelevant.

The clutter of unhelpful results may hinder searchers' ability to satisfy their search objectives, undermining searchers' confidence in search engines' mind-reading abilities.[47] In this case, regulatory intervention could counter-productively degrade search engines' value to searchers. Whatever the adverse consequences of search engine bias, the consequences of regulatory correction are probably worse.[48]

## Technological Evolution Will Moot Search Engine Bias

Currently, search engines principally use "one-size-fits-all" ranking algorithms to deliver homogeneous search results to searchers with heterogeneous search objectives.[49] One-size-fits-all algorithms exacerbate the consequences of search engine bias in two ways: (1) they create winners (websites listed high in the

---

46 *See, e.g.*, Susan L. Gerhart, *Do Web Search Engines Suppress Controversy?*, FIRST MONDAY, Jan. 2004, **http://www.firstmonday.org/issues/issue9_1/gerhart/**. Gerhart argues that search engines do not adequately prioritize search results that expose controversies about the search topic. However, her argument assumes that controversy-related information has value to consumers, an assumption that deserves careful evaluation.

47 *See* Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151, *available at* **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=912524**.

48 *See* Susan P. Crawford, *Shortness of Vision: Regulatory Ambition in the Digital Age*, 74 FORDHAM L. REV. 695 (2005) (discussing the shortcomings of regulatory intervention in organic information systems).

49 *See* James Pitkow et al., *Personalized Search*, COMM. ACM, Vol. 45:9 (Sept. 2002) at 50-1.

search results) and losers (those with marginal placement), and (2) they deliver suboptimal results for searchers with minority interests.[50]

These consequences will abate when search engines migrate away from one-size-fits-all algorithms towards "personalized" ranking algorithms.[51] Personalized algorithms produce search results that are custom-tailored to each searcher's interests, so searchers will see different results in response to the same search query. For example, Google offers searchers an option that "orders your search results based on your past searches, as well as the search results and news headlines you've clicked on."[52]

Personalized ranking algorithms represent the next major advance in search relevancy. One-size-fits-all ranking algorithms have inherent limits on their maximum relevancy potential, and further improvements in one-size-fits algorithms will yield progressively smaller relevancy benefits. Personalized algorithms transcend those limits, optimizing relevancy for each searcher and thus implicitly doing a better job of searcher mind-reading.[53]

Personalized ranking algorithms also reduce the effects of search engine bias. Personalized algorithms mean that there are multiple "top" search results for a particular search term instead of a single "winner,"[54] so web publishers will not compete against each other in a zero-sum game. In turn, searchers will get results more influenced by their idiosyncratic preferences and less influenced by the embedded preferences of the algorithm-writers. Also, personalized algorithms necessarily will diminish the weight given to popularity-based metrics (to give more weight for searcher-specific factors), reducing the structural biases due to popularity.

---

50 *See* Michael Kanellos, *Microsoft Aims for Search on Its Own Terms*, CNET NEWS.COM, Nov. 24, 2003, **http://news.com.com/2102-1008_3-5110910.html?tag=st.util.print** (quoting a Microsoft researcher as saying "If the two of us type a query [into a search engine], we get the same thing back, and that is just brain dead. There is no way an intelligent human being would tell us the same thing about the same topic."); David H. Freedman, *Why Privacy Won't Matter*, NEWSWEEK, Apr. 3, 2006; Personalization of Placed Content Ordering in Search Results, U.S. Patent App. 0050240580 (filed July 13, 2004).

51 *See* Pitkow, *supra* note 49, at 50.

52 *What's Personalized Search?*, GOOGLE.COM, **http://www.google.com/support/bin/answer.py?answer=26651&topic=1593**.

53 *See* Jaime Teevan et al., *Personalizing Search via Automated Analysis of Interests and Activities*, SIGIR '05, **http://haystack.lcs.mit.edu/papers/teevan.sigir05.pdf**; Terry McCarthy, *On the Frontier of Search*, TIME, Aug. 28, 2005 ("Search will ultimately be as good as having 1,000 human experts who know your tastes scanning billions of documents within a split second.") (quoting Gary Flake, Microsoft Distinguished Engineer).

54 *See* Kevin Lee, *Search Personalization and PPC Search Marketing*, CLICKZ NEWS, July 15, 2005, **http://www.clickz.com/experts/search/strat/print.php/3519876**.

Personalized ranking algorithms are not a panacea—any process where humans select and weight algorithmic factors will produce some bias[55]—but personalized algorithms will eliminate many of the current concerns about search engine bias.

## Conclusion

Complaints about search engine bias implicitly reflect some disappointed expectations. In theory, search engines can transcend the deficiencies of predecessor media to produce a type of utopian media. In practice, search engines are just like every other medium—heavily reliant on editorial control and susceptible to human biases. This fact shatters any illusions of search engine utopianism.

Fortunately, search engine bias may be largely temporal. In this respect, I see strong parallels between search engine bias and the late 1990s keyword metatag "problem."[56] Web publishers used keyword metatags to distort search results, but these techniques worked only so long as search engines considered keyword metatags in their ranking algorithms. When search engines recognized the distortive effects of keyword metatags, they changed their algorithms to ignore keyword metatags.[57] Search result relevancy improved, and the problem was solved without regulatory intervention.

Similarly, search engines naturally will continue to evolve their ranking algorithms and improve search result relevancy—a process that, organically, will cause the most problematic aspects of search engine bias to largely disappear. To avoid undercutting search engines' quest for relevance, this effort should proceed without regulatory distortion.

---

55 Personalized algorithms have other potentially adverse consequences, such as creating self-reinforcing information flows. *See* SUNSTEIN, *supra* note 31. For a critique of these consequences, see Goldman, *Coasean Analysis*, *supra* note 47.

56 *See generally* Goldman, *Deregulating Relevancy*, supra note 8.

57 *See* Danny Sullivan, *Death of a Meta Tag*, SEARCH ENGINE WATCH, Oct. 1, 2002, **http://www.searchenginewatch.com/sereport/print.php/34721_2165061**.

# CHAPTER 8

## WHAT FUTURE FOR PRIVACY?

# Privacy Protection in the Next Digital Decade: "Trading Up" or a "Race to the Bottom"?

By Michael Zimmer*

Apparent to most citizens of contemporary, industrialized society, people no longer exist and live in fixed locations and spaces. Instead people are on the move in their personal, professional, intellectual, and social spheres. Within and across these spheres, mobility, rather than permanence, is likely to be the norm. Manuel Castells captures this feature of modern life in his theory of the space of flows, arguing that "our society is constructed around flows: flows of capital, flows of information, flows of technology, flows of organizational interaction, flows of images, sounds, and symbols."[1] These flows—particularly *information* flows—constitute what Castells describes as the "network society," where "networks constitute the new social morphology of our societies, and the diffusion of networking logic substantially modifies the operation and outcomes in processes of production, experience, power and culture."[2]

Nowhere is Castells "network society" more apparent than in our contemporary global digital information network, with the Internet as its backbone. Originating from a handful of universities and research laboratories in the 1960s, the Internet began to take shape as a ubiquitous information network with the emergence of the "dot-com" economy in the 1990s. Dot-com business models varied—and met varied levels of success—but most relied on the rapid delivery of services and exchange of information. While much of the dot-com economy burst with the dot-com bubble in 2000, the Internet remained a powerful network enabling robust flows of information, continually modifying "experience, power and culture," just as Castells described.

In the past digital decade, the Internet has provided new linkages and spaces for information flows, and has particularly emerged as a potent infrastructure for the flow and capture of *personal* information. These flows take many forms and stem from various motivations. Large-scale web advertising platforms and search engines utilize robust infrastructures to collect data about web browsing and search activities in order to provide relevant advertising. Users' consumption habits are captured by online service providers like Amazon and Netflix, fueling powerful recommendation systems meant to improve user

* School of Information Studies, University of Wisconsin-Milwaukee

1 MANUEL CASTELLS, THE RISE OF THE NETWORK SOCIETY 412 (1996).

2 *Id.* at 469.

satisfaction. Individuals openly share personal information with friends and colleagues on social networking services such as Facebook and LinkedIn, and their thoughts with the world on platforms like Blogger and Twitter. Looking back at the past decade, the Internet has become a platform for the open flow of personal information—flows that are largely voluntarily provided by users—and as such, appear to have validated Scott McNealy's (in)famous 1999 remark that "You have zero privacy anyway … get over it."[3]

Notwithstanding McNealy's view, privacy has remained a central concern amid the open information flows in our contemporary network society, including worries about the growing size and role of networked databases,[4] the possibility of tracking and surveillance by Internet service providers[5] and Web search engines,[6] privacy threats from digital rights management technologies,[7] and growing concerns about protecting the privacy of users of social networking sites and related Web 2.0 services.[8]

While scholars continue to detail possible threats to privacy spawned by the last decade of innovations on the Internet, governments have struggled with whether—and how—to regulate information flows across these global networks

---

3 Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED, March 31, 2007, **http://www.wired.com/politics/law/news/1999/01/17538**.

4 SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (2000).

5 Colin J. Bennett, Cookies, *Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web*, 3(3) ETHICS AND INFORMATION TECHNOLOGY 195, 197-210 (2001); Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 UNIVERSITY OF ILLINOIS LAW REVIEW 1417-1496.

6 M. Goldberg, *The Googling of Online Privacy: Gmail, Search-Engine Histories, and the New Frontier of Protecting Private Information on the Web*, 9 Lewis & Clark Law Review 249-272 (2005); Michael Zimmer, *The Gaze of the Perfect Search Engine: Google as an Infrastructure of Dataveillance* in WEB SEARCHING: MULTIDISCIPLINARY PERSPECTIVES 77-99 (Amanda Spink & Michael Zimmer, eds., 2008).

7 Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace*, 28(4) CONNECTICUT LAW REVIEW 981-1039 (1996); Julie E. Cohen, *DRM and privacy*, 18 BERKELEY TECHNOLOGY LAW JOURNAL 575-617 (2003).

8 Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks* (ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, 2005); Michael Zimmer, *The Externalities of Search 2.0: The Emerging Privacy Threats When the Drive for the Perfect Search Engine Meets Web 2.0,* FIRST MONDAY, Mar. 3, 2010, **http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2136/1944**; Joseph Bonneau & Sören Preibusch, *The Privacy Jungle: On the Market for Data Protection in Social Networks* (The Eighth Workshop on the Economics of Information Security (WEIS 2009)); James Grimmelmann, *Facebook and the Social Dynamics of Privacy*, 95(4) IOWA LAW REVIEW 1137 (2009); Marc Parry, *Library of Congress, Facing Privacy Concerns, Clarifies Twitter Archive Plan*, THE CHRONICLE OF HIGHER EDUCATION, June 1, 2010, **http://chronicle.com/blogPost/Library-of-Congress-Facing/23818/**.

to protect the privacy of their citizens. Given the diversity of interests, histories, and cultural contexts, a complicated terrain of trans-national laws and policies for the protection of privacy and personal data flows across networks has emerged across the globe. Some jurisdictions have opted for broad, and relatively strict, laws regulating the collection, use and disclosure of personal information, such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)[9] or the European Union's Data Protection Directive.[10] The United States, however, maintains a more sectoral approach to privacy legislation, with laws addressing only specific types of personal information. For example, the Health Insurance Portability and Accountability Act (HIPAA)[11] offers protection of personal medical information, the Fair Credit Reporting Act[12] regulates the collection and flow of personal financial data, and the Video Privacy Protection Act[13] makes the wrongful disclosure of video rental records illegal.

The differences between Canadian/EU approaches to privacy and that of the United States have been well documented and analyzed.[14] Put bluntly, the Canadian/EU regulators can be described as embracing a more paternalist approach to data protection policy, aiming to preserve a fundamental human right of its citizens through preemptive governmental action. In contrast, the governance of privacy in the U.S. typically emerges only after some informational harm has occurred, often taking the form of industry self-regulation or very targeted legislation, with the responsibility of initiating enforcement resting on the harmed data subject herself. As Dorothee Heisenberg summarizes, "In practical terms, the EU and the US reached very different conclusions about the rights of businesses and individuals related to personal data."[15] While the EU and Canada focus on direct and preemptive

---

9 R.S., 1985, c. P-21, **http://laws.justice.gc.ca/en/P-21/index.html**.

10 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML**.

11 Health Insurance Portability and Accountability Act of 1996, H. Rept. 104-736, **http://www.gpo.gov/fdsys/search/pagedetails.action?granuleId=CRPT-104hrpt736&packageId=CRPT-104hrpt736**.

12 Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., **http://www.ftc.gov/os/statutes/031224fcra.pdf**.

13 Video Privacy Protection Act of 1988, Pub. L. 100-618 (codified at 18 U.S.C. § 2710), **http://www.law.cornell.edu/uscode/18/2710.html**.

14 *See, e.g.*, DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION (2005); COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE (2003).

15 Heisenberg, *supra* note 14 at 2.

regulation of the collection and use of personal data, prohibiting "excess" data collection and restricting use to the original and stated purposes of the collection, the U.S, framework begins with the assumption that most data collection and use is both acceptable and beneficial, that guidelines should be primarily voluntary and non-invasive, and that regulation should only address documented instances of abuse.

This difference in regulatory approaches to privacy—and the underpinning tensions between different jurisdictions' views towards the rights of data subjects—becomes complicated further given the increasing flows of personal information across and between transnational networks, and thus, across jurisdictions. Internet companies like Google have customers accessing their products and services from across the globe, with data processing and storage facilities equally scattered. A Canadian citizen, for example, might be accessing a Google product in the United States, while the record of the particular information exchange might be stored on a server in Ireland. Each jurisdiction has its own complex set of regulations and rights assigned to the treatment of any personal information shared and stored.

These kinds of scenarios have prompted growing concerns about whether the global diversity of privacy governance will result in a "race to the bottom" where corporate interests in processing personal data will migrate to jurisdictions where there is little or no control over the circulation and capture of personal information flows, or a "race to the top" where the fashioning of privacy policy to the highest possible standards in order to be perceived as the "best" protector of personal information flows. After considering the available evidence, political scientists Colin Bennett and Charles Raab have suggested that privacy protection is actually improving globally—a "trading up" of the governance of privacy.[16] Companies are, on the whole, not moving around in order to avoid strict privacy regulations, such as those developed in the EU; instead, there has been a gradual increase in awareness and action on the issue of privacy. Examples of this "trading up" include Facebook's strengthening of its privacy policies and practices in reaction to an investigation by the Office of the Privacy Commissioner of Canada, or Google's modifying its Web cookie and partially anonymizing search logs in response to Norwegian privacy regulators.[17] In each case, large multi-national Internet companies reacted to strong regional privacy laws in ways that benefited all users across the globe.

---

16 Bennett & Raab, *supra* note 14.

17 Office of the Privacy Commissioner of Canada, *Facebook Agrees to Address Privacy Commissioner's Concerns*, Aug. 20, 2010, **http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm**; Nate Anderson, *Google To Anonymize Logs In A Nod To Privacy Advocates*, ARS TECHNICA, Aug. 20, 2010, **http://arstechnica.com/business/news/2007/03/google-to-anonymize-logs-in-a-nod-to-privacy-advocates.ars**.

Offsetting this positive note, however, is the realization that privacy protection may not be "trading up" as rapidly as other global factors, such as the extensive, intensive processing of personal data across borders and platforms; the increased focus on economic growth through the use of electronic communications and information infrastructures; and the harmonization of law enforcement and security objectives. Bennett and Raab go to some length to expose the limitations of relying solely on individual countries to impose isolated privacy policies in the face of a globally-networked computer system permitting—indeed encouraging—transnational information flows.[18] While state-specific data protection governance might have been sufficient in the past, they argue, today's digitally networked society demands that any country's efforts to protect its citizens will inescapably be linked with (as well as dependent on) the actions and laws of other, often disparate, jurisdictions.

This leads to obvious problems, when, for example, a legal approach like that of the United States, with an emphasis on self-regulation and public-sector enforcement, meets a different philosophy, such as the more top-down, paternalistic approach to data protection held by Canada and the European Union. This clash between U.S. and non-U.S. standards for governing personal information flows has prompted large, multi-national companies dependent on the relatively unfettered flow of information across global digital networks to lobby for some middle ground to be reached. In the case of the U.S. and the European Union, the result was the 2000 Safe Harbor agreement[19] between the two global economic powers to avoid the most egregious misuse of Europeans' private data, while at the same time creating a semi-permanent "cease fire" that would allow transatlantic data (and hence commerce) to flow, despite failing to meet the letter, and perhaps not even the intent, of the E.U. Data Protection Directive. In the end, while U.S. based companies are forced to provide more privacy protections than U.S. law demands, the Safe Harbor provisions are weaker than the full European Directive on Data Protection. As Heisenberg explains, "the evolution … of the [European Union] Commission's stance on data protection seems to have been one of softening a bit" during the Safe Harbor negotiations, as the "Commission began to accommodate the US as privacy legislation clashed with first commercial, and then security concerns."[20]

So, while there has been no clear "race to the bottom" in global privacy protections, the "trading up" to an increased level of protection of personal

---

18 Bennett & Raab, *supra* note 14.

19 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML**.

20 Heisenberg, *supra* note 14 at 136.

information flows on our transnational digital networks has not materialized as quickly or clearly as one might expect. Heisenberg correctly notes that with the Safe Harbor Agreement, the EU was able to force the U.S. to deal with the privacy issues that might have otherwise been ignored, force some minor concessions, and show that the EU's privacy standard was significant, granting the EU something like a "first-mover advantage" in future trans-border privacy disputes.[21] Yet, beyond isolated examples of Internet companies' hesitant acquiescence to non-U.S. regulatory bodies—like the Facebook and Google examples provided above—new norms of personal data protection are unlikely to emerge in the next digital decade, as data protection officials in Europe have begun to publicly question the appropriateness of the current levels of protections.[22]

Recalling Castells' warning that "networks constitute the new social morphology of our societies, and the diffusion of networking logic substantially modifies the operation and outcomes in processes of production, experience, power and culture," we are left to consider the status of privacy protections in the next digital decade. Our network society will continue to grow in size and density, as well as in its global importance and interconnectedness. Without concerted efforts to ensure a "trading up" in global privacy protections—a renewed commitment to the rights of data subjects embodied in the Canadian and European Union approach to data protection—those caught within the inescapable "diffusion of networking logic" may have little control over how the increased flows of their personal information will modify "experience, power and culture" over the next digital decade.

---

21 *Id.* at 170.

22 W. Scott Blackmer, The Information Law Group, *European Reservations?*, Aug. 26, 2010, **http://www.infolawgroup.com/2010/08/articles/eu-1/european-reservations/**.

# The Privacy Problem: What's Wrong with Privacy?

By Stewart Baker*

Why are privacy groups so viscerally opposed to government action that could reduce the risks posed by exponential technologies? The cost of their stance was made clear on September 11, 2001. That tragedy might not have occurred if not for the aggressive privacy and civil liberties protection imposed by the Foreign Intelligence Surveillance Court and the Department of Justice's Office of Intelligence; and it might have been avoided if border authorities had been able to use airline reservation data to screen the hijackers as they entered the United States.

But even after 9/11, privacy campaigners tried to rebuild the wall and to keep the Department of Homeland Security (DHS) from using airline reservation data effectively. They failed; too much blood had been spilled.

But in the fields where disaster has not yet struck—computer security and biotechnology—privacy groups have blocked the government from taking even modest steps to head off danger.

I like to think that I care about privacy, too. But I had no sympathy for privacy crusaders' ferocious objection to any new government use of technology and data. Where, I wondered, did their objection come from?

So I looked into the history of privacy crusading. And that's where I found the answer.

## The Birth of the Right of Privacy

In the 1880s, Samuel Dennis Warren was near the top of the Boston aristocracy. He had finished second in his class at Harvard Law School. He founded a law firm with the man who finished just ahead of him, Louis Brandeis, and they prospered mightily. Brandeis was a brilliant, creative lawyer and social reformer who would eventually become a great Supreme Court justice.

But Samuel Dennis Warren was haunted. There was a canker in the rose of his life. His wife was a great hostess, and her parties were carefully planned. When

---

* **Stewart A. Baker** is a partner in the Washington office of Steptoe & Johnson LLP. He returned to the firm following 3½ years at the Department of Homeland Security as its first Assistant Secretary for Policy.

Warren's cousin married, Mabel Warren held a wedding breakfast and filled her house with flowers for the event. The papers described her home as a "veritable floral bower."

No one should have to put up with this. Surely you see the problem. No? Well, Brandeis did.

He and Warren both thought that, by covering a private social event, the newspapers had reached new heights of impertinence and intrusiveness. The parties and guest lists of a Boston Brahmin and his wife were no one's business but their own, he thought. And so was born the right to privacy.

Angered by the press coverage of these private events, Brandeis and Warren wrote one of the most frequently cited law review articles ever published. In fact, "The Right to Privacy," which appeared in the 1890 Harvard Law Review, is more often cited than read—for good reason, as we'll see. [1] But a close reading of the article actually tells us a lot about the modern concept of privacy.

Brandeis,[2] also the father of the policy-oriented legal brief, begins the article with a candid exposition of the policy reasons why courts should recognize a new right to privacy. His argument is uncompromising:

> The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery … To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury … Even gossip apparently harmless, when widely and persistently circulated, is potent for evil … When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what

---

1 Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193 (1890).

2 Because the article owes much of its current fame to Brandeis's later career, I will from this point on discuss only his views without each time laboriously giving credit, if that is the right word, to his coauthor.

> wonder that the ignorant and thoughtless mistake its relative importance … Triviality destroys at once robustness of thought and delicacy of feeling.[3]

What does Brandeis mean by this? To be brief, he thinks it should be illegal for the newspapers to publish harmless information about himself and his family. That, he says, is idle gossip, and it distracts "ignorant and thoughtless" newspaper readers from more high-minded subjects. It also afflicts the refined and cultured members of society—like, say, Samuel Dennis Warren and his wife—who need solitude but who are instead harassed by the fruits of "modern enterprise and invention."

What's remarkable about "The Right to Privacy" is that the article's title still invokes reverence, even though its substance is, well, laughable.

Is there anyone alive who thinks it should be illegal for the media to reveal the guest-list at a prominent socialite's dinner party or to describe how elaborate the floral arrangements were? Today, it's more likely that the hostess of a prominent dinner party will blog it in advance, and that the guests will send Twitter updates while it's under way. For most socialites, what would really hurt is a lack of media coverage. To be blunt, when he complains so bitterly about media interest in a dinner party, Brandeis sounds to modern ears like a wuss.

Equally peculiar is the suggestion that we should keep such information from the inferior classes lest they abandon self-improvement and wallow instead in gossip about their betters. That makes Brandeis sound like a wuss and a snob.

He does sound quite up-to-date when he complains that "modern enterprise and invention" are invading our solitude. That is a familiar complaint. It's what privacy advocates are saying today about Google, not to mention the National Security Agency (NSA). Until you realize that he's complaining about the scourge of "instantaneous photographs and newspaper enterprise."[4] Huh? Brandeis evidently thinks that publishing a private citizen's photo in the newspaper causes "mental pain and distress, far greater than could be inflicted by mere bodily injury."[5]

If we agreed today, of course, we probably wouldn't have posted 5 billion photographs of ourselves and our friends on Flickr.[6]

---

3 *The Right to Privacy*, at 196 (1890).

4 *Id.* at 195.

5 *Id.* at 196.

6 Zack Sheppard, *5,000,000,000*, Flickr Blog, Sept. 19, 2010, **http://blog.flickr.net/en/2010/09/19/5000000000/**.

## Spirit of the Privacy Movement Today

Anachronistic as it seems, the spirit of Brandeis's article is still the spirit of the privacy movement. The right to privacy was born as a reactionary defense of the status quo, and so it remains. Then, as now, new technology suddenly made it possible to spread information more cheaply and more easily. This was new, and uncomfortable. But apart from a howl of pain—pain "far greater than … mere bodily injury"—Brandeis doesn't tell us why it's so bad. I guess you had to be there—literally. Unless you were an adult when photography came to newspapers, you'll probably never really understand what the fuss was about. We've all been photographed, and most of us aren't happy with the results, at least not all the time. But that's life, and we've learned to live with it. Most of us can't imagine suing to prevent the distribution of our photographs—which was the tort Brandeis wanted the courts to create.

We should not mock Brandeis too harshly. His article clearly conveys a heartfelt sense of invasion. But it is a sense of invasion we can never share. The sensitivity about being photographed or mentioned in the newspapers, a raw spot that rubbed Brandeis so painfully, has calloused over. So thick is the callous that most of us would be tickled, not appalled, to have our dinner parties make the local paper, and especially so if it included our photos.

And that's the second thing that Brandeis's article can tell us about more contemporary privacy flaps. His brand of resistance to change is still alive and well in privacy circles, even if the targets have been updated. Each new privacy kerfuffle inspires strong feelings precisely because we are reacting against the effects of a new technology. Yet as time goes on, the new technology becomes commonplace. Our reaction dwindles away. The raw spot grows a callous. And once the initial reaction has passed, so does the sense that our privacy has been invaded. In short, we get used to it.

At the beginning, of course, we don't want to get used to it. We want to keep on living the way we did before, except with a few more amenities. And so, like Brandeis, we are tempted to ask the law to stop the changes we see coming. There's nothing more natural, or more reactionary, than that.

Most privacy advocates don't see themselves as reactionaries or advocates for the status quo, of course. Right and left, they cast themselves as underdogs battling for change against the entrenched forces of big government. But virtually all of their activism is actually devoted to stopping change—keeping the government (and sometimes industry) from taking advantage of new technology to process and use information.

But simply opposing change, especially technological change, is a losing battle. At heart, the privacy groups know it, which may explain some of their shrillness and lack of perspective. Information really does "want to be free"—or at least

cheap. And the spread of cheap information about all of us will change our relationship to the world. We will have fewer secrets. Crippling government by preventing it from using information that everyone else can get will not give us back our secrets.

In the 1970s, well before the personal computer and the Internet, privacy campaigners persuaded the country that the FBI's newspaper clipping files about U.S. citizens were a threat to privacy. Sure, the information was public, they acknowledged, but gathering it all in one file was viewed as vaguely sinister. The attorney general banned the practice in the absence of some legal reason for doing so, usually called an investigative "predicate."

So, in 2001, when Google had made it possible for anyone to assemble a clips file about anyone in seconds, the one institution in the country that could not print out the results of its Google searches about Americans was the FBI. This was bad for our security, and it didn't protect anyone's privacy either.

The privacy campaigners are fighting the inevitable. The "permanent record" our high school principals threatened us with is already here—in Facebook. Anonymity, its thrills and its freedom, has been characteristic of big cities for centuries. But anonymity will also grow scarce as data becomes easier and easier to gather and correlate. We will lose something as a result, no question about it. The privacy groups' response is profoundly conservative in the William F. Buckley sense—standing athwart history yelling, "Stop!"[7]

I'm all for conservatism, even in unlikely quarters. But using laws to fight the inevitable looks a lot like Prohibition. Prohibition was put in place by an Anglo-Saxon Protestant majority that was sure of its moral superiority but not of its future. What the privacy community wants is a kind of data Prohibition for government, while the rest of us get to spend more and more time in the corner bar.

That might work if governments didn't need the data for important goals such as preventing terrorists from entering the country. After September 11, though, we can no longer afford the forced inefficiency of denying modern information technology to government. In the long run, any effective method of ensuring privacy is going to have to focus on using technology in a smart way, not just trying to make government slow and stupid.

---

7 *See* William F. Buckley Jr., *Publisher's Statement*, NATIONAL REVIEW, Nov. 19, 1955, at 5, *available at* **www.nationalreview.com/articles/223549/our-mission-statement/william-f-buckley-jr**.

## The Evolution of Technology & the "Zone of Privacy"

That doesn't mean we have to give up all privacy protection. It just means that we have to look for protections that work with technology instead of against it. We can't stop technology from making information cheap and reducing anonymity, but we can deploy that same technology to make sure that government officials can't misuse data and hide their tracks. This new privacy model is partially procedural—greater oversight and transparency—and partly substantive—protecting individuals from actual adverse consequences rather than hypothetical informational injuries.

Under this approach, the first people who should lose their privacy are the government workers with access to personal data. They should be subject to audit, to challenge, and to punishment if they use the data for improper purposes. That's an approach that works with emerging technology to build the world we want to live in. In contrast, it is simple Luddism to keep government from doing with information technology what every other part of society can do.

The problem is that Luddism always has appeal. "Change is bad" is a slogan that has never lacked for adherents, and privacy advocates sounded alarm after alarm with that slogan as the backdrop when we tried to put in place a data-based border screening system.

But would we really thank our ancestors if they'd taken the substance of Brandeis's article as seriously as its title? If, without a legislature ever considering the question, judges had declared that no one could publish true facts about a man's nonpolitical life, or even his photograph, without his permission?

I don't think so. Things change. Americans grow less private about their sex lives but more private about financial matters. Today, few of us are willing to have strangers living in our homes, listening to our family conversations, and then gossiping about us over the back fence with the strangers who live in our friends' homes. Yet I'll bet that both Brandeis and Warren tolerated without a second thought the limits that having servants put on their privacy.

Why does our concept of privacy vary from time to time? Here's one theory: Privacy is allied with shame. We are all ashamed of something about ourselves, something we would prefer that no one, or just a few people, know about. We want to keep it private. Sometimes, of course, we should be ashamed. Criminals always want privacy for their acts. But we're also ashamed—or at least feel embarrassment, the first cousin of shame—about a lot of things that aren't crimes.

We may be ashamed of our bodies, at least until we're sure we won't be mocked for our physical shortcomings. Privacy is similar; we are often quite willing to share information about ourselves, including what we look like without our clothes, when we trust our audience, or when the context makes us believe that our shortcomings will go unnoticed. Most of us would rather be naked with our spouse than a random stranger. And we would not appear at the office in our underwear, even if it covers more than the bathing suit we wore at the beach on the weekend.

For that reason, enforced nudity often feels like a profound invasion of our privacy. At least at first. In fact, though, we can get used to it pretty quickly, as anyone who has played high school sports or served in the army can attest. That's because the fear of mockery is usually worse than the experience. So when we discover that being naked in a crowd of other naked people doesn't lead to mockery and shame, we begin to adapt. We develop a callous where we once were tender.

The things that Brandeis considered privacy invasions are similar. Very few of us are happy the first time we see our photograph or an interview in the newspaper. But pretty soon we realize it's just not that big a deal. Our nose and our style of speech are things that the people we know have already accepted, and no one else cares enough to embarrass us about them. The same is true when we Google ourselves and see that a bad review of our dinner-theater performance is number three on the list. Our first reaction is embarrassment and unhappiness, but the reaction is oddly evanescent.

If this is so, then the "zone of privacy" is going to vary from time to time and place to place—just as our concept of physical modesty does. The zone of privacy has boundaries on two sides. We don't care about some information that might be revealed about us, probably because the revelation causes us no harm—or we've gotten used to it. If the information is still embarrassing, we want to keep it private, and society may agree. But we can't expect privacy for information that society views as truly shameful or criminal.

Over time, information will move into and out of the zone of privacy on both sides. Some information will simply become so unthreatening that we'll laugh at the idea that it is part of the privacy zone. Photographs long ago entered that category, despite Brandeis's campaigning. Some information will move from criminal evidence into the zone of privacy, as sexual preference has. Conversely, it may move in the other direction: information that a man beats his wife is no longer protected by a zone of familial privacy, as it once was; now it's viewed as evidence of a crime.

The biggest privacy battles will often be in circumstances where the rules are changing. The subtext of many Internet privacy fights, for example, is whether some new measure will expose the identities of people who download

pornography or copyrighted music and movies. Society is divided about how shameful it is to download these items, and it displaces that moral and legal debate into a fight about privacy.

Divorce litigation, for instance, is brutal in part because information shared in a context of love and confidence ends up being disclosed to the world in a deliberately harmful way. Often the activity in question (like making a telephone call or a credit card purchase) is something that the individual does freely, with clear knowledge that some other people (his bank or his phone company) know what he is doing. Sometimes the activities are proudly public in nature—protests against government policy, for example.

In those cases, the privacy concern is not that the bank or the phone company (or our spouse) actually has the information, but rather what they will do with the information they have—whether they will use the data in ways we didn't expect or give the data to someone who can harm us. We want to make sure the data will not be used to harm us in unexpected ways.

And that helps explain why privacy advocates are so often Luddite in inclination. Modern technology keeps changing the ways in which information is used. Once, we could count on practical obscurity—the difficulty of finding bits of data from our past—to protect us from unexpected disclosures. Now, storage costs are virtually nil, and processing power is increasing exponentially. It is no longer possible to assume that your data, even though technically public, will never actually be used. It is dirt cheap for data processors to compile dossiers on individuals, and to use the data in ways we didn't expect.

Some would argue that this isn't really "privacy" so much as a concern about abuse of information. However it's defined, though, the real question is what kind of protection is it reasonable for us to expect. Can we really write a detailed legislative or contractual pre-nup for each disclosure, setting forth exactly how our data will be used before we hand it over? I doubt it. Maybe we can forbid obvious misuses, but the more detailed we try to get, the more we run into the problem that our notions of what is private, and indeed of what is embarrassing, are certain to change over time. If so, does it make sense to freeze today's privacy preferences into law?

In fact, that's the mistake that Brandeis made—and the last lesson we can learn from the odd mix of veneration and guffawing that his article provokes. Brandeis wanted to extend common law copyright until it covered everything that can be recorded about an individual. The purpose was to protect the individual from all the new technologies and businesses that had suddenly made it easy to gather and disseminate personal information: "the too enterprising

press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds."[8]

This proposal is wacky in two ways. First it tries to freeze in 1890 our sense of what is private and what is not. Second, it tries to defy the gravitational force of technology.

Every year, information gets cheaper to store and to duplicate. Computers, iPods, and the Internet are all "modern devices" for "reproducing scenes or sounds," which means that any effort to control reproduction of pictures, sounds, and scenes becomes extraordinarily difficult if not impossible. In fact, it can't be done.

There is a deep irony here. Brandeis thought that the way to ensure the strength of his new right to privacy was to enforce it just like state copyright law. If you don't like the way "your" private information is distributed, you can sue everyone who publishes it. One hundred years later, the owners of federal statutory copyrights in popular music and movies followed this prescription to a T. They began to use litigation to protect their data rights against "the possessor[s] of any other modern device for … reproducing scenes or sounds,"[9] a class that now included many of their customers. The Recording Industry Association of America (RIAA) sued consumers by the tens of thousands for using their devices to copy and distribute songs.

Unwittingly, the RIAA gave a thorough test to Brandeis's notion that the law could simply stand in front of new technology and bring it to a halt through litigation. There aren't a lot of people who think that that has worked out well for the RIAA's members, or for their rights.

Brandeis wanted to protect privacy by outlawing the use of a common new technology to distribute "private" facts. His approach has fared no better than the RIAA's. Information that is easy to gather, copy and distribute will be gathered, copied, and distributed, no matter what the law says.

It may seem a little bit odd for me to criticize Brandeis and other privacy campaigners for resisting the spread of technology. After all, we can't simply accept the world that technology and commerce serve up.

It's one thing to redirect the path of technological change by a few degrees. It's another to insist that it take a right angle. Brandeis wanted it to take a right

---

8 Warren & Brandeis, *supra* note 1 at 206.

9 *Id.*

angle; he wanted to defy the changes that technology was pressing upon him. So did the RIAA.

Both were embracing a kind of Luddism—a reactionary spasm in the face of technological change. They were doomed to fail. The new technologies, after all, empowered ordinary citizens and consumers in ways that could not be resisted. If the law tries to keep people from enjoying the new technologies, in the end it is the law that will suffer.

But just because technologies are irresistible does not mean that they cannot be guided, or cannot have their worst effects offset by other technologies. The solutions I'm advocating will only work if they allow the world to keep practically all the benefits of the exponential empowerment that new technology makes possible.

## Privacy for the Real World: Proposed Solutions

So what's my solution to the tension between information technology and our current sense of privacy? The short answer is that we should protect privacy, but not by defying the course of technology or by crippling government when it investigates crimes. We can do it by working *with* technology, not against it. In particular, we can use information technology to make sure that government officials lose their privacy when they misuse data that has been gathered for legitimate reasons. Information technology now makes it easier to track every database search made by every user, and then to follow any distribution of that data outside the system. In other words, it can make misuse of the data in government files much more difficult and much more dangerous.

But before talking about what *might* work, let's take a closer look at some of the ideas that don't.

### Ownership of Personal Data

The first privacy solution is one we've already seen. It's the Brandeisian notion that we should all "own" our personal data. That has some appeal, of course. If I have a secret, it feels a lot like property. I can choose to keep it to myself, or I can share it with a few people whom I trust. And I would like to believe that sharing a secret with a few trusted friends doesn't turn it into public property. It's like my home. Just because I've invited one guest home doesn't mean the public is welcome.

But in the end, information is not really like property. Property can only be held by one person at a time, or at most by a few people. But information can be shared and kept at the same time. And those with whom it is shared can pass it on to others at little or no cost. If you ever told a friend about your secret crush

in junior high, you've already learned that information cannot be controlled like property. As Ben Franklin is credited with saying, "Three may keep a secret if two of them are dead."[10] The redistribution of information cannot be easily controlled in the best of times, and Moore's Law is making the control of information nearly impossible.[11]

The recording and movie industries discovered the same thing. If these industries with their enormous lobbying and litigation budgets cannot control information that they own as a matter of law, the rest of us are unlikely to be able to control information about ourselves. Gossip is not going to become illegal simply because technology amplifies it.

That's why Brandeis's proposal never really got off the ground, at least not as he envisioned it. Buoyed by Brandeis's prestige, the idea that private facts are private property lingered on in the courts for years, but what survived of his proposal is scarcely recognizable today.

In fact, so transformed is Brandeis's privacy doctrine that it is now described, accurately, as a "right of publicity," which surely would have him turning in his grave. Currently, most states honor Brandeis by allowing lawsuits for unauthorized commercial use of a person's likeness, either by statute or judge-made law.

Over time, courts lost sight of Brandeis's purpose. They began to take the analogy to property literally. Brandeis wanted to treat private information like property because that was the only way to give a remedy for the "mental pain and distress, far greater than could be inflicted by mere bodily injury," that he thought a man suffered when his photo was published without permission. But as people got used to having their pictures taken, the mental pain and distress slowly drained out of the experience.

All that was left was the property analogy. And so judges began shrinking the right until it only had bite in the one set of circumstances where the right to control one's image actually feels like a property right—when the image is worth real bucks. Thus, the courts require disgorgement of profits made when a celebrity's name, face, voice, or even personal style is used without permission to sell or endorse products. As a result, the right to exploit a celebrity's image really is property today; it can be sold, transferred, and even inherited.

---

10 Benjamin Franklin, POOR RICHARD'S ALMANAC, July 1735.

11 Moore's Law describes the long-term trend that the number of transistors that can be placed inexpensively on an integrated circuit has doubled approximately every two years. It is named after Intel's co-founder Gordon E. Moore, who described the trend in the essay *Cramming More Components Onto Integrated Circuits*, ELECTRONICS MAGAZINE 4, 1965.

There's only one problem with this effort to turn privacy into property: it hasn't done much for privacy. It simply protects the right of celebrities to make money off their fame. In fact, by monetizing things like celebrity images, it rewards those who have most relentlessly sacrificed their privacy to gain fame.

The right of publicity is well named. It is the right to put your privacy up for sale. Not surprisingly, a lot of people have been inspired to do just that. Ironically, Brandeis's doctrine has helped to destroy the essence of what he hoped to preserve.

Oh, and in the process, Brandeis's approach has stifled creativity and restricted free speech—muzzling artists, social commentators, and businesspeople who want to make creative use of images that are an essential part of our cultural environment. It's a disaster. Slowly, courts are waking up to the irony and limiting the right of publicity.

The same "private information as property" approach has also made a modest appearance in some consumer privacy laws, and it's worked out just as badly. At bottom, consumer privacy protection laws like the Right to Financial Privacy Act[12]treat a consumer's data like a consumer's money: You can give your data (or your money) to a company in exchange for some benefit, but only if you've been told the terms of the transaction and have consented. Similarly, the Cable Communications Policy Act of 1984 prevents cable providers from using or releasing personal information in most cases unless the providers get the customer's consent. The fruit of this approach is clear to anyone with a bank account or an Internet connection. Everywhere you turn, you're confronted with "informed consent" and "terms of service" disclosures; these are uniformly impenetrable and non-negotiable. No one reads them before clicking the box, so the "consent" is more fiction than reality; certainly it does little to protect privacy. Indeed, it's turning out a lot like the right of publicity. By treating privacy as property, consumer privacy protection law invites all of us to sell our privacy.

And we do. Only for most of us, the going price turns out to be disconcertingly cheap.

## Mandatory Predicates for Information Access

The second way of protecting privacy is to require what's called a "predicate" for access to information. That's a name only a lawyer could love. In fact, the whole concept is one that only lawyers love.

---

12 The Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3695 (1978) (codified as amended at 12 U.S.C. § 3401 *et seq.*).

Simply put, the notion is that government shouldn't get certain private information unless it satisfies a threshold requirement—a "predicate" for access to the data. Lawyers have played a huge role in shaping American thinking about privacy, and the predicate approach has been widely adopted as a privacy protection. But its value for that purpose is quite doubtful.

The predicate approach to privacy can be traced to the Fourth Amendment, which guarantees that "no Warrants shall issue, but upon probable cause." Translated from legalese, this means that the government may not search your home unless it has a good reason to do so. When the government asks for a search warrant, it must show the judge "probable cause"—evidence that the search will likely turn up criminal evidence or contraband. Probable cause is the predicate for the search.

When a flap arose in the 1970s over the FBI practice of assembling domestic security dossiers on Americans who had not broken the law, the attorney general stepped in to protect their privacy. He issued new guidelines for the FBI. He was a lawyer, so he declared that the FBI could not do domestic security investigations of Americans without a predicate.

The predicate wasn't probable cause; that was too high a standard. Instead, the attorney general allowed the launching of a domestic security investigation only if the bureau presented "specific and articulable facts giving reason to believe" that the subject of the investigation may be involved in violence.[13]

Actually, the story of the FBI guidelines shows why the predicate approach often fails. The dossiers being assembled by the FBI were often just clippings and other public information. They usually weren't the product of a search in the classic sense; no federal agents had entered private property to obtain the information. Nonetheless, the FBI guidelines treated the gathering of the information itself as though it were a kind of search.

In so doing, the guidelines were following in Brandeis's footsteps—treating information as though it were physical property. The collection of the information was equated to a physical intrusion into the home or office of the individual. Implicitly, it assumes that data can be locked up like property.

But that analogy has already failed. It failed for Brandeis and it failed for the RIAA. It failed for the FBI guidelines, too. As clippings became easier to

---

13 The Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3695 (1978) (codified at 12 U.S.C. § 3414(a)(5)(A)), amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107–56, 115 STAT. 272, § 505(b), **www.law.cornell.edu/uscode/pdf/uscode12/lii_usc_TI_12_CH_35_SE_3401.pdf**.

retrieve, clippings files became easier to assemble. Then Google made it possible for anyone to assemble an electronic clips file on anyone. There was nothing secret about the clippings then. They were about as private as a bus terminal.

But the law was stuck in another era. Under the guidelines, only the FBI and CIA needed a predicate to do Google searches. You have to be a pretty resilient society to decide that you want to deny to your law enforcement agencies a tool that is freely available to nine-year-old girls and terrorist gangs. Resilient, but stupid. (Not surprisingly, the guidelines were revised after 9/11.)

That's one reason we shouldn't treat the assembling of data as though it were a search of physical property. As technology makes it easier and easier to collect data, the analogy between doing that and conducting a search of a truly private space will become less and less persuasive. No one thinks government agencies should have a predicate to use the White Pages. Soon, predicates that keep law enforcement from collecting information in other ways will become equally anachronistic, leaving law enforcement stuck in the 1950s while everyone else gets to live in the twenty-first century.

I saw this lawyerly affinity for predicates up close at DHS. The issue was laptop searches at the border. The government has always had the right to search anything crossing the border without probable cause. Smugglers are smart and highly motivated; they would find a way to exploit any limitations on the authority to conduct searches. The first Congress knew that quite well, and in 1789, two months before it sent the Fourth Amendment to the states for approval, Congress gave the customs service "full power and authority" to search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed."[14]

Obviously, DHS and its border predecessors didn't search laptops in 1789. But they *did* search books, papers, correspondence, and anything else that could store information. That was the law for two hundred years, with one exception. The Supreme Court has ruled that a few extraordinarily intrusive techniques—body cavity searches and forced x-rays—require a "reasonable suspicion."[15]

Laptops are treated like books and papers. They are searched whenever border officials think that such a search is likely to be productive. Even the famously

---

14 An Act to Regulate the Collection of Duties, 1st Cong. 1st Sess., Stat.1, Ch. V, Sec. 24 at 43 (July 31, 1789).

15 U.S. v. Flores-Montano, 541 U.S. 149 (2004).

liberal Ninth Circuit, the court of appeal that includes California, has had no trouble approving that practice,[16] and for good reason—laptop searches pay off.

In 2006, for example, border officials at the Minneapolis-St. Paul airport referred a suspect traveler to secondary inspection. There they found that his computer contained video clips of IEDs being used to kill soldiers and destroy vehicles and a video on martyrdom. He was also carrying a manual on how to make improvised explosive devices, or IEDs—a weapon of choice for terrorists in Afghanistan and Iraq.

Despite two hundred years of history and precedent, as well as the proven value of searching electronic media, privacy groups launched a campaign against laptop searches toward the end of the Bush administration. This was a strange and unhappy era in the debate over privacy. By 2005, privacy advocates had found a growing audience for claims that the Bush administration had abandoned all limits in pursuing terrorism—that it had swung the pendulum violently away from privacy and in favor of government authority.

The privacy advocates' solution to the laptop issue was the lawyer's favorite—a predicate requirement. Laptops should not be searched at the border, they argued, unless the border official could articulate some specific reason for conducting the search. That argument was rejected by both the Bush and the Obama administrations after careful consideration.

We rejected it for two reasons. It wouldn't have protected privacy in any meaningful way, and it would have helped criminals like pedophiles and terrorists defeat our border defenses. Other than that, it was jim-dandy.

Why wouldn't it help protect privacy? Because, as a practical matter, no border official today searches a laptop without some reasonable suspicion about the traveler. The exponential increase in commercial jet travel and the unforgiving thirty-second rule mean that only one traveler in two hundred is sent to secondary inspection for a closer look. Once there, many travelers quickly satisfy the officials that they don't deserve more detailed inspection.

Everyone at the border is busy; border officers don't have the luxury of hooking up the laptops of random travelers for inspection without a good reason. Officers who waste their time and DHS's resources that way are going to hear from their supervisors long before they hear from the travelers' lawyers.

If border officials only search laptops today when they have a good reason to do so, why not make that a requirement? What harm can it do to make reasonable suspicion a predicate for laptop searches at the border? Plenty.

---

16 U.S. v. Arnold, 523 F.3d 941 (9th Cir. 2008).

Requiring reasonable suspicion before a laptop search will open every border search to litigation. And in court, it may be hard to justify even some very reasonable judgments.

Inevitably, enforcement of a predicate requirement for border searches will produce litigation. The litigation will focus on the motives of the border officials. The courts will tell those officials that some reasons are not good enough. Defense lawyers will want to see the personnel records of border officials, hoping to show that they've inspected a disproportionate number of laptops belonging to minorities, or to Saudis, or to men, or any other pattern that might get the case thrown out. Border officials will have to start keeping detailed records justifying each laptop search. New paperwork and new procedures will clog the inspection process, backing up travelers and penalizing any inspector who searches a laptop.

Wait a minute, you might ask, what if those officials are racists or sexists?

Let's assume that this concern is legitimate, at least sometimes, and that there are biased officials at work on the border. Surely there's a better way to find them and get them off the job than to count on criminal defense lawyers exposing them on the witness stand years after the event.

By now, notice, we're not even talking about privacy anymore. The "predicate" solution has, in effect, changed the subject. We're talking about the motives of border officials, or ethnic profiling, or something—but it isn't privacy. We're also moving the whole discussion into territory that lawyers find comfortable but that ordinary people might question.

The Fourth Amendment approach to privacy assumes that privacy is best protected by letting criminals challenge the search that produced the evidence against them, but before adopting that solution, we ought to be pretty sure that we're going to get benefits that match the cost of letting guilty defendants go free, something that isn't obvious here.

## Limits on Information Use

That leaves the third approach to privacy, one we've already seen in action. If requiring a predicate is the lawyer's solution; this third approach is the bureaucrat's solution. It is at heart the approach adopted by the European Union: Instead of putting limits on when information may be collected, it sets limits on how the information is used.

The European Union's data protection principles cover a lot of ground, but their unifying theme is imposing limits on how private data is used. Under those principles, personal data may only be used in ways that are consistent with the

purposes for which the data were gathered. Any data that is retained must be relevant to the original purposes and must be stored securely to prevent misuse.

The EU's negotiating position in the passenger name records conflict was largely derived from this set of principles. The principles also explain Europe's enthusiasm for a wall between law enforcement and intelligence. If DHS gathered reservation data for the purpose of screening travelers when they cross the border, why should any other agency be given access to the data? This also explains the EU's insistence on short deadlines for the destruction of PNR data. Once it had been used to screen passengers, it had served the purpose for which it was gathered and should be promptly discarded.

There is a core of sense in this solution. It focuses mainly on the consequences of collecting information, and not on the act of collection. It doesn't try to insist that information is property. It recognizes that when we give information to others, we usually have an expectation about how it will be used, and as long as the use fits our expectations, we aren't too fussy about who exactly gets to see it. By concentrating on how personal information is used, this solution may get closer to the core of privacy than one that focuses on how personal information is collected.

It has another advantage, too. In the case of government databases, focusing on use also allows us to acknowledge the overriding importance of some government data systems while still protecting against petty uses of highly personal information.

Call it the deadbeat-dad problem, or call it mission creep, but there's an uncomfortable pattern to the use of data by governments. Often, personal data must be gathered for a pressing reason—the prevention of crime or terrorism, perhaps, or the administration of a social security system. Then, as time goes on, it becomes attractive to use the data for other, less pressing purposes—collecting child support, perhaps, or enforcing parking tickets. No one would support the gathering of a large personal database simply to collect unpaid parking fines; but "mission creep" can easily carry the database well beyond its original purpose. A limitation on use prevents mission creep, or at least forces a debate about each step in the expansion.

That's all fine. But in the end, this solution is also flawed.

It, too, is fighting technology, though less obviously than the predicate and property approaches. Data that has already been gathered is easier to use for other purposes. It's foolish to pretend otherwise. Indeed, developments in information technology in recent years have produced real strides in searching unstructured data or in finding relationships in data without knowing for sure that the data will actually produce anything useful. In short, there are now good

reasons to collate data gathered for widely differing purposes, just to see the patterns that emerge.

This new technical capability is hard to square with use limitations or with early destruction of data. For if collating data in the government's hands could have prevented a successful terrorist attack, no one will congratulate the agency that refused to allow the collation because the data was collected for tax or regulatory purposes, say, and not to catch terrorists.

What's more, use limitations have caused great harm when applied too aggressively. The notorious "wall" between law enforcement and intelligence was at heart a use limitation. It assumed that law enforcement agencies would gather information using their authority, and then would use the information only for law enforcement purposes. Intelligence agencies would do the same. Or so the theory went. But strict enforcement of this use limitation was unimaginably costly. In August 2001, two terrorists were known to have entered the United States. As the search for them began, the government's top priority was enforcing the wall -- keeping intelligence about the terrorists from being used by the "wrong" part of the FBI. Government lawyers insisted that law enforcement resources could not be used to pursue intelligence that two known al Qaeda agents were in the United States in August 2001.

This was a fatal blunder. The criminal investigators were well-resourced and eager. They might have found the men. The intelligence investigators, in contrast, had few resources and did not locate the terrorists, at least not until September 11, when the terrorists' names were discovered on the manifests of the hijacked planes. It was a high price to pay for the modest comfort of "use" limitations.

Like all use limitations, the "wall" between law enforcement sounded reasonable enough in the abstract. While no one could point to a real privacy abuse arising from cooperation between the intelligence and law enforcement agencies in the United States, it was easy to point to the Gestapo and other totalitarian organizations where there had been too much cooperation among agencies.

What was the harm in a little organizational insurance against misuse of personal data, the argument ran. The rules allowed cooperation where that was strictly necessary, and we could count on the agencies to crowd right up to the line in doing their jobs. Or so we thought. In fact, we couldn't. As the pressure and the risk ratcheted up, agents were discouraged from pushing for greater communication and cooperation across the wall. All the Washington-wise knew that the way to bureaucratic glory and a good press lay in defending privacy. Actually, more to the point, they knew that bad press and bureaucratic disgrace were the likely result if your actions could be characterized as hurting privacy. Congress would hold hearings; appropriators would zero out your office; the second-guessing arms of the Justice Department, from the inspectors general to

the Office of Professional Responsibility, would feast on every detail of your misstep. So, what might have been a sensible, modest use restriction preventing the dissemination of information without a good reason became an impermeable barrier.

That's why the bureaucratic system for protecting privacy so often fails. The use restrictions and related limits are abstract. They make a kind of modest sense, but if they are enforced too strictly, they prevent new uses of information that may be critically important.

And often they are enforced too strictly. You don't have to tell a bureaucrat twice to withhold information from a rival agency. Lawsuits, bad press, and Congressional investigations all seem to push against a flexible reading of the rules. If a use for information is not identified at the outset, it can be nearly impossible to add the use later, no matter how sensible the change may seem. This leads agencies to try to draft broad uses for the data they collect, which defeats the original point of setting use restrictions.

It's like wearing someone else's dress. Over time, use restrictions end up tight where they should be roomy—and loose where they should be tight. No one is left satisfied.

## The Audit Approach: Enforced Accountability

So what will work? Simple: accountability, especially electronically-enforced accountability.

The best way to understand this solution is to begin with Barack Obama's passport records—and with "Joe the Plumber." These were two minor flaps that punctuated the 2008 presidential campaign. But both tell us something about how privacy is really protected these days.

In March of 2008, Barack Obama and Hillary Clinton were dueling across the country in weekly primary showdowns. Suddenly, the campaign took an odd turn. The Bush administration's State Department announced that it had fired or disciplined several contractors for examining Obama's passport records.

Democrats erupted. It wasn't hard to jump to the conclusion that the candidate's files had been searched for partisan purposes.[17] After an investigation, the flap slowly deflated. It soon emerged that all three of the main presidential candidates' passport files had been improperly accessed. Investigators reported that the State Department was able to quickly identify

---

17 Karen Tumulty, *Snooping Into Obama's Passport*, TIME, Mar. 21, 2008, **http://www.time.com/time/politics/article/0,8599,1724520,00.html**.

who had examined the files by using its computer audit system. This system flagged any unusual requests for access to the files of prominent Americans. The fired contractors did not deny the computer record. Several of them were charged with crimes and pleaded guilty. All, it turned out, had acted purely out of "curiosity."

Six months later, it was the Republicans' turn to howl about privacy violations in the campaign. Samuel "Joe" Wurzelbacher, a plumber, became an overnight hero to Republicans in October 2008 after he was practically the only person who laid a glove on Barack Obama during the campaign. The candidate made an impromptu stop in Wurzelbacher's Ohio neighborhood and was surprised when the plumber forced him into a detailed on-camera defense of his tax plan. Three days later, "Joe the Plumber" and his taxes were invoked dozens of times in the presidential debates.

The price of fame was high. A media frenzy quickly stripped Wurzelbacher of anonymity. Scouring the public record, reporters found that the plumber had been hit with a tax lien; they also found government data that raised doubts about the status of his plumbing license.

Reporters weren't the only ones digging. Ohio state employees also queried confidential state records about Wurzelbacher. In all, they conducted eighteen state records checks on Wurzelbacher. They asked whether the plumber owed child support, whether he'd ever received welfare or unemployment benefits, and whether he was in any Ohio law enforcement databases. Some of these searches were proper responses to media requests under Ohio open records laws; others looked more like an effort to dig dirt on the man.

Ohio's inspector general launched an investigation and in less than a month was able to classify all but one of the eighteen records searches as either legitimate or improper.[18] Thirteen searches were traced and deemed proper, but three particularly intrusive searches were found improper; they had been carried out at the request of a high-ranking state employee who was also a strong Obama supporter. She was suspended from her job and soon stepped down. A fourth search was traced to a former information technology contractor who had not been authorized to search the system he accessed; he was placed under criminal investigation.

What do these two flaps have in common? They were investigated within weeks of the improper access, and practically everyone involved was immediately caught. That's vitally important. Information technology isn't just taking away your privacy or mine. It's taking away the privacy of government workers even

---

[18] *See* State of Ohio, Office of Inspector General, *Report of Investigation, File ID Number 2008299*, Nov. 20, 2008, **www.judicialwatch.org/documents/2009/IGReport.pdf**.

faster. Data is cheap to gather and cheap to store. It's even getting cheap to analyze.

So it isn't hard to identify every official who accessed a particular file on a particular day. That's what happened here. And the consequences for privacy are profound.

If the lawyer's solution is to put a predicate between government and the data and the bureaucrat's solution is to put use restrictions on the data, then this is the auditor's solution. Government access to personal data need not be restricted by speed bumps or walls. Instead, it can be protected by rules, so long as the rules are enforced.

What's new is that network security and audit tools now make it easy to enforce the rules. That's important because it takes the profit motive out of misuse of government data. No profit-motivated official is going to take the risk of stealing personal data if it's obvious that he'll be caught as soon as people start to complain about identity theft. Systematic misuse of government databases is a lot harder and more dangerous if good auditing is in place.

Take another look at why government officials accessed these files. It wasn't to steal identities. The reason most of these people accessed the data was simple curiosity. Even the one access that may have been for more reprehensible reasons—the woman who checked confidential child support and welfare records for Joe the Plumber—was quickly caught and the data never leaked.

The speed and nearly complete effectiveness of the audit process in these cases tells us that network auditing tools can transform the way we enforce the rules for handling data in government. For example, if we catch every error, we can improve compliance and at the same time reduce the penalties for mistakes. Harsh penalties are not the most effective way to enforce rules. In fact, they're usually a confession of failure.

When we catch every offender, we can afford to lower the penalty. Lighter, more certain penalties for privacy violations serve another purpose, too. We've talked a lot about the oddly protean nature of privacy. Not causing harm in unexpected ways is at the core of the concept, but it's nearly impossible to write detailed rules spelling out what is and is not a violation of privacy. Indeed, the effort to write such rules and stick to them is what gave us the wall, and thousands of American dead. So something must be left to discretion. Government employees must use good sense in handling personal data. If they don't, they should be punished. But if we are confident that we can identify any questionable use of personal data and correct it quickly, the punishments can be smaller. They can be learning experiences rather than penological experiences.

So why did we criminally prosecute the poor schlubs whose hobby was looking at the passport pictures of famous people? The election happened. Everything that touched on the election was put under a microscope. Evil motives were always ascribed to the other side. The State Department had to make a blood sacrifice to show that accessing the data was not part of an evil plot by one party against the other. Opening a criminal investigation was a way of condemning the access in the clearest possible fashion. That the poor schlubs probably only deserved demotions counted for little in the super-heated atmosphere of a presidential campaign.

That shows one of the problems with the audit approach. It is too easily turned into a phony privacy scandal. In both the Wurzelbacher and Obama cases, the audits did their job. With one possible exception, they caught the government staff that broke the rules. They prevented any harm to either Wurzelbacher or Obama. And they made sure that the officials who were responsible would never repeat their errors again.

The system worked. Privacy was protected. But that's certainly not the impression that was left by coverage of the affairs. Indeed, the chairman of the Senate Judiciary Committee, Senator Leahy, used the passport flap to tout new legislation strengthening privacy protections on government databases. From a political point of view, then, the system failed. There were no thanks for the government officials who put the system in place, who checked the audit logs, who confronted and disciplined the wrongdoers, and who brought the solved problem to public attention. To the contrary, they were pilloried for allowing the access in the first place—even though preventing such access is an impossible task unless we intend to re-erect walls all across government.

How's that for irony? Audits work. But they work too well. Every time they catch someone and put a stop to misuse of personal data they also provide an opening for political grandstanding. In the end, the finger pointing will discourage audits. And that will mean less privacy enforcement. So, the more we turn every successful audit into a privacy scandal, the less real privacy we're likely to have.

That would be a shame, because the auditor's solution to the problem is the only privacy solution that will get more effective as technology advances. And we're going to need more solutions that allow flexible, easy access to sensitive databases while still protecting privacy.

If the plight of government investigators trying to prevent terrorist attacks doesn't move you, think about the plight of medical technicians trying to keep you alive after a bad traffic accident.

The Obama administration has launched a long-overdue effort to bring electronic medical records into common use. But the privacy problem in this

area is severe. Few of us want our medical records to be available to casual browsers. At the same time, we can't personally verify the bona fides of the people accessing our records, especially if we're lying by the side of the road suffering from what looks like brain or spine damage.

But the electronic record system won't work if it can't tell the first responders that you have unusual allergies or a pacemaker. It has to do that quickly and without a lot of formalities. Auditing access after the fact is likely to be our best answer to this problem, as it is to the very similar problem of how to let law enforcement and intelligence agencies share information smoothly and quickly in response to changing and urgent circumstances. The Markle Foundation has done pioneering work in this area, and its path-breaking 2003 report on privacy and security in the war on terror recommends embracing technologies that watch the watchers.[19] A unique mix of security, privacy, and technology experts managed to reach agreement in that report; they found that one key to protecting privacy without sacrificing security was a network that included "access control, authentication, and full auditing capability."[20]

The Markle report urges that large databases with personal information use emerging technologies that can identify all users of the system with certainty and then give them access that depends on their roles at any particular time. This includes "the ability to restrict access privileges so that data can be used only for a particular purpose, for a finite period of time, and by people with the necessary permissions."[21] The technologies they cited are not pie in the sky. They exist today: "smart cards with embedded chips, tokens, biometrics, and security circuits" as well as "[i]nformation rights management technologies."[22] The Markle task force later did a thoughtful paper on one of those technologies, which would preserve audit logs even if high-ranking officials seek to destroy or modify them later.[23]

These technologies can be very flexible. This makes them especially suitable for cases where outright denial of data access could have fatal results. The tools can be set to give some people immediate access, or to open the databases in certain situations, with an audit to follow. They can monitor each person with access to

---

19 Markle Foundation Task Force, *Creating a Trusted Network for Homeland Security*, Dec. 2003, **http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf**.

20 *Id.* at 15.

21 *Id.*

22 *Id.*

23 MARKLE FOUNDATION TASK FORCE, IMPLEMENTING A TRUSTED INFORMATION SHARING ENVIRONMENT: USING IMMUTABLE AUDIT LOGS TO INCREASE SECURITY, TRUST, AND ACCOUNTABILITY (2006), available at **http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf**.

the data and learn that person's access patterns—what kinds of data, at what time, for how long, with or without copying, and the like. Deviations from the established pattern can have many consequences. Perhaps access will be granted but the person will be alerted that an explanation must be offered within twenty-four hours. Or access could be granted while a silent alarm sounds, allowing systems administrators to begin a real-time investigation.

There's a kind of paradox at the heart of this solution. We can protect people from misuse of their data, but only by stripping network users of any privacy or anonymity when they look at the data. The privacy campaigners aren't likely to complain, though. In our experience, their interest in preserving the privacy of intelligence and law enforcement officers is pretty limited.

When I was general counsel of the National Security Agency, a well-known privacy group headed by Marc Rotenberg filed a Freedom of Information Act request asking the NSA to assemble all documents and emails sent "to or from Stewart Baker." Then as now, the NSA was forbidden to assemble files on American citizens who were not agents of a foreign power. Even so, Rotenberg was asking NSA to assemble a dossier on me. Since NSA and I were locked in a battle with Rotenberg over encryption policy at the time, the purpose of the dossier was almost certainly to look for embarrassing information that might help Rotenberg in his political fight. Indeed, Rotenberg claimed when I confronted him that he was planning to scrutinize my dossier for evidence of misconduct.

Had the FBI or NSA assembled a dossier on their political adversaries, it would have been a violation of law. In fact, it would have caused a privacy scandal. But Rotenberg saw no irony in his request. It wasn't a privacy problem, in his view, because government officials deserve no privacy.

I still think Rotenberg's tactics were reprehensible: He had singled me out for a selective loss of privacy because he didn't like my views. But I've come to appreciate that there's a core of truth to his view of government. Anyone who has access to government files containing personal data has special responsibilities. He should not expect the same privacy when he searches that data as he has while he's surfing the net at home. And now that technology makes it easy to authenticate and track every person, every device, and every action on a network, perhaps it's time to use that technology to preserve everyone else's privacy.

In the end, that's the difference between a privacy policy that makes sense and one that doesn't. We can't lock up data that is getting cheaper every day. Pretending that it's property won't work. Putting "predicates" between government and the data it needs won't work, and neither will insisting that they may only be used for purposes foreseen when it was collected.

What we *can* do is use new information technology tools to deter government officials from misusing their access to that data.

As you know by now, I think that some technology poses extraordinary risks. But we can avoid the worst risks if we take action early. We shouldn't try to stop the trajectory of new technology. But we can bend it just a little. Call it a course correction on an exponential curve.

That's also true for privacy. The future is coming—like it or not. Our data will be everywhere. But we can bend the curve of technology to make those who hold the data more accountable. Bending the exponential curve a bit—that's a privacy policy that could work. And a technology policy that makes sense.

# A Market Approach to Privacy Policy

By Larry Downes*

## Privacy: The Problem

What happens when the cost of deleting information is higher than the cost of retaining it?

The answer is that nothing gets deleted. In the age of cloud computing, mobile devices, and social networking, what that really means is that more and more data—some of it enterprise data, some of it personal information, and more and more of it something that merges the two—is being saved.

Soon, perhaps already, much of it will be consolidated, aggregated, reorganized, and mined for valuable patterns, behaviors, and insights. Privacy has become an unintended casualty of Moore's Law—collateral damage from friendly fire.

That, at least, is one way of thinking about privacy in the digital age, one that has been on my mind for the last several months. I wrote about the privacy problem in my recent book, *The Laws of Disruption*, in which I argued that the real solution to concerns about privacy in the digital age would be the emergence of robust markets for private information, where consumers would be able to trade personal information with other individuals and enterprises when doing so generated mutual benefit.[1]

The privacy problem has morphed since then into the latest terror of the digital age, surpassing earlier shibboleths, such as copyright piracy, identity theft, cyber war and net neutrality.[2] Daily media coverage of the latest privacy policy

---

* **Larry Downes** is an Internet analyst and consultant, helping clients develop business strategies in an age of constant disruption caused by information technology. He is the author of **UNLEASHING THE KILLER APP: DIGITAL STRATEGIES FOR MARKET DOMINANCE** (Harvard Business School Press 1998) and, most recently, of **THE LAWS OF DISRUPTION: HARNESSING THE NEW FORCES THAT GOVERN LIE AND BUSINESS IN THE DIGITAL AGE** (Basic Books 2009) [hereinafter THE LAWS OF DISRUPTION].

1 *See* LARRY DOWNES, THE LAWS OF DISRUPTION, *Law Two: Privacy*.

2 As I've written elsewhere, all of these problems share a common core. Each raises the fundamental question about the nature of digital life and by whom and how its basic infrastructure is to be governed. In some sense, each is another view of the same regulatory problem, seen through lenses that are equally unfocused, but in different ways. *See* Larry Downes, *After the Deluge, More Deluge*, THE TECHNOLOGY LIBERATION FRONT, July 22, 2010, **http://techliberation.com/2010/07/22/after-the-deluge-more-deluge/**.

change, hacking incident, stolen government laptop or inadvertent disclosure has raised the stakes and the tension in a problem that, it seems, people react to with such strong emotions that rational discussion of any solution is now impossible.[3]

The privacy crisis is very much on the mind of regulators around the world, who see the emergence of privacy fears among consumers as the latest and perhaps the best opportunity to gain a toehold in regulating (and perhaps taxing) content on the web. Nearly all of the earlier efforts—including outright censorship, imposition of protectionist laws on global e-commerce, and enforcement of strict copyright, trademark and patent regimes onto the evolving collaborative ethos of digital life—have failed utterly.[4] By aligning themselves with consumer interests (and perhaps helping to stoke the fires of anxiety), regulators may have at last found their point of entry into the market for Internet regulation.

That certainly seems to be the attitude adopted by the once-moribund U.S. Federal Trade Commission (FTC), which began a series of workshops in late 2009 aimed at exploring "the privacy challenges posed by the vast array of 21st century technology and business practices that collect and use consumer data."[5]

On January 28th, 2010, which was also dubbed Data Privacy Day by the non-profit group The Privacy Projects,[6] the second workshop in the FTC's three-part[7] series took place at the University of California, Berkeley campus. Attendees heard from government, business, and public interest speakers on

---

3 Recent examples include the Google Maps drive-by, see Robert Graham, *Technical Details of the Street View WiFi Payload Controversy,* ERRATA SECURITY, May 19, 2010, **http://erratasec.blogspot.com/2010/05/technical-details-of-street-view-wifi.html**, Facebook's on-going changes to its privacy policy and user options, Twitter's FTC settlement, see Press Release, Federal Trade Commission, Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program, June 24, 2010, **http://www.ftc.gov/opa/2010/06/twitter.shtm**, the botched launch of Google Buzz, see Danny Goodwin, Google to Pay $8.5 Million in Buzz Privacy Class Action Settlement, SEARCHENGINEWATCH.COM, Nov. 3, 2010, **http://blog.searchenginewatch.com/101103-081738**, shocking behavior on Chatroulette, the conviction of Google executives in an Italian court over a video showing the bullying of a minor with disabilities by a Google Video user, see Reuters, Italy Convicts Google Execs for Down Syndrome Video, Feb. 24, 2010, **http://www.wired.com/epicenter/2010/02/google-executive-convicted-in-italy-for-downs-video/**, and the launch of "social shopping" websites such as Blippy and Swipely.

4 *See generally*, THE LAWS OF DISRUPTION, *supra* note 1.

5 *See Exploring Privacy: A Roundtable Series*, Fed. Trade Comm'n, **www.ftc.gov/bcp/workshops/privacyroundtables/** [hereinafter *FTC Roundtable Series*].

6 For more information on Data Privacy Day, visit **http://dataprivacyday2010.org**.

7 *See FTC Roundtable Series*, *supra* note 5.

whether and how the FTC should regulate the private collection and use of data to protect consumer privacy interests. The conversation that day, characterized by histrionic rhetoric, self-congratulatory moralizing, and an utter lack of focus, reflects well the current state of the so-called "privacy problem."

Why is the FTC holding such hearings in the first place? The agency's charter, which has evolved over its long history, includes policing anticompetitive behavior[8] and enforcing a Congressional ban on "unfair and deceptive acts or practices." So far, the FTC's main contribution to the debate about digital privacy has been the drafting of non-binding guidelines for consumer notice of online services' privacy policies, the so-called "Fair Information Practice Principles (FIPs)."[9] In the United States, the adoption of the FIPs is voluntary, but failure to abide by them can lead to FTC enforcement.[10]

The limits of the so-called "notice" regime are pretty obvious. Consumers don't read privacy policies. Even if they did, they would find them to be absurdly long, most of them written in some of the worst legalese I've ever seen.

Notice is also difficult to achieve in practice. During the last few years, Facebook has repeatedly landed in trouble for its mostly-admirable efforts to craft a working privacy regime for its now 500 million users. The generally poor response to these efforts, I think, stems from a growing privacy paranoia fueled by the media and governments, kindled by the growing pains of a company that by its nature deals with very personal, even intimate, information and whose growth rate challenges pretty much everything.

At the same time, the company's founder, Mark Zuckerberg, has demonstrated remarkably poor timing and nearly perfect political tone deafness. Even as the company dug itself out of criticism of a new set of privacy tools in the fall, Zuckerberg told an audience in January 2010 that "the social norm" for sharing private information had "evolved."[11] Well, he is only 25 years old, and many of

---

8 The FTC recently reached a settlement with Intel on a broad regulatory action brought against the company. *See* Press Release, Fed. Trade Comm., *FTC Settles Charges of Anticompetitive Conduct Against Intel*, Aug. 4, 2010, **http://www.ftc.gov/opa/2010/08/intel.shtm**.

9 For more information on the Fair Information Practice Principles, visit **http://www.ftc.gov/reports/privacy3/fairinfo.shtm**.

10 The FTC can take action if a website violates its own policy on the basis of its jurisdiction over deceptive practices. But there is no requirement for a website to have a privacy policy, and no explicit privacy protection in U.S. law for most categories of personally-identifiable information.

11 *See* Marshall Kirkpatrick, *Facebook's Zuckerberg Says Age of Privacy is Over*, READWRITEWEB, Jan. 9, 2010, **http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php**.

his comments, including these, have been unfairly taken out of context by mainstream, business, and technology media companies.[12]

The limits of notice become acute when the data collection device is not a computer. Cell phones, in addition to taking on more and more data functions, collect a great deal of information about the location and movements of their users—they have to in order to function. But many applications such as Loopt[13] and Foursquare[14] take advantage of GPS data to offer services not possible on a fixed computing device, including locating friends or providing location-specific ads. On the smaller screen of a cell phone, reading any document is difficult enough. What consumer in any case is going to read a separate privacy policy for every application they download?

Even as it continues to refine and promote FIPs, the FTC has held hearings, workshops and other information-gathering sessions regarding emerging technologies that seem to raise new and worrisome privacy concerns. These have included Radio Frequency ID tags, targeted or "behavioral" advertisements, cookies and now Flash-based "super cookies."[15]

There was plenty of evidence at the Berkeley session of these and more of what Microsoft's Peter Cullen called "anxiety-based conversations." [16] This year's themes include the dangers of mobile computing, social networking, and cloud-based computing, as well as continuing hand-wringing over targeted or contextual advertising.

The structure of these conversations doesn't change much over time. The new technology is discussed by law professors, company representatives, and FTC

---

12 Caroline McCarthy, *Facebook Follies: A Brief History*, CNET NEWS.COM, May 13, 2010, **http://news.cnet.com/8301-13577_3-20004853-36.html**; Guilbert Gates, *Facebook Privacy: A Bewildering Tangle of Options*, N.Y. TIMES, May 12, 2010, **http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html**.

13 Loopt is a mobile mapping service that allows users to find local information using the geographic location of their mobile phones. For more information, visit **http://www.loopt.com**.

14 Foursquare is a location-based social networking application that allows users to connect with friends in their geographic location. For more information, visit **http://foursquare.com**.

15 The super cookie "problem," piled on by many speakers at the Berkeley workshop, turned out to be a red herring, easily controlled by engineered fixes to major browsers. It's hard not to read too much into that example. *See* Berin Szoka, *Privacy Innovation: Adobe Flash Supports Private Browsing & Deletes Flash Cookies*, THE TECH. LIBERATION FRONT, Feb. 17, 2010, **http://techliberation.com/2010/02/17/privacy-innovation-adobe-flash-supports-private-browsing-deletes-flash-cookies/**.

16 Private Conversation with Peter Cullen, Jan. 28, 2010 (notes on file with author).

staff (everybody but the engineers who know how the technology works), who try to point out the benefits and mostly dangers of the technology.

Extremists on either end of the spectrum call for the FTC to either ban or ignore the development. In typical fashion, satisfied that all sides have been heard, the agency takes the problem under advisement, and then waits for the next crisis du jour to emerge. No legislation or regulations are enacted.

Well, that's probably just as well—assuming there is no real privacy crisis that needs to be addressed, or rather that needs to be addressed by an organization with the FTC's institutional limitations. I mean no disrespect to the FTC's hard-working staff. By institutional limits, I am thinking of the inherent constraints on a U.S. regulatory agency. These include the mismatch of a national regulator supervising behavior that is natively global, problems in revising rules and jurisdictions for an environment that is evolving at accelerating speeds using a process designed to be slow and deliberative, and the dangers of solving what are largely engineering problems with staff whose expertise is policy—and offline policy at that.

It's probably clear that I don't think there is a crisis. But I admit that it's difficult to know. Both sides in this non-debate have an unfortunate habit of relying on unscientific survey data and anecdotal evidence, the latter of which, on closer inspection, turns out to be highly incomplete if not urban myth. Pam Dixon of the World Privacy Forum, for example, told a story about grocer Whole Foods using facial recognition software in stores to collect data from the tomato aisle for what Dixon called "direct marketing purposes." But according to the Forum's own report, *The One Way Mirror Society*, (whose investigation of the Whole Foods story was limited to parsing company press releases) the software could at best distinguish gender, not specifically identify customers.[17] Direct marketing is targeted to an individual (or their likely interests) rather than demographic characteristics such as gender. So whatever Whole Foods was doing, it wasn't direct marketing.

The surveys that purportedly show a privacy panic are, for the most part, poorly constructed and unscientifically executed. For some reason law professors and their students, who have at best a casual acquaintance with the methods and rigors of any social science, are the ones called on by private and public actors to conduct these studies.

Consider, for example, two questions about the same technical feature of cell phones. If you ask for an emotional response to the statement, "My cell phone

---

17 Pam Dixon, *The One-Way-Mirror Society: Privacy Implications of the New Digital Signage Networks*, WORLD PRIVACY FORUM, Jan. 27, 2010, **http://www.worldprivacyforum.org/pdf/onewaymirrorsocietyfs.pdf**.

tracks where I go" you'll get one answer, but if you phrase it, "My cell phone can tell me where I am," you'll get a very different result. It's the same feature. The "findings" are useless. The choice and wording of the questions are the only valuable information, in that it reveals a great deal about the authors of the survey. But the surveys tell us nothing about the respondents or the choices they would make when faced with real-world tradeoffs between restricting data and the benefits that flow from it—such as getting more relevant ads or a greater quality and quantity of "free" online content and services supported by advertising revenue.

## Privacy: Defining the Problem

There's a bigger problem here, and that is with the terms of the debate. In most conversations, no one knows what anyone else means by "privacy," or what information is included in the term "personally-identifiable information," which drives much of the privacy regulations in the European Union. The discussion at the FTC's Berkeley roundtable, as with all privacy discussions, conflated several different information problems into one, freely mixing and matching issues and regulatory solutions that don't actually go together. Until we separate the problems and solve them individually, the chances for meaningful policy solutions are nil.

To start with, it's essential to understand the unique properties of information as an economic good. Information has very different properties from traditional commodities such as farm products, timber, and oil. Information can be used simultaneously by everyone, for one thing, and when we're done using it, it's still there, potentially more valuable because of the use. These remarkable features make information what economists call a non-rivalrous or "public" good, and they are the main reason that information now drives economic activity in much of the developed world. (The other is the continued decline in the cost of computing power.)

So rather than talking about who "owns" private information or who is "stealing" data (words that make more sense when talking about traditional commodities), I find it much more constructive to talk about whether any particular use of information is "productive" or "destructive" A productive use of information is one that makes it more valuable, including collaboration, remixing, and validation. Destructive uses leave the information less valuable, and include misrepresentation, misidentification, and dilution.[18]

---

[18] Some information uses include both productive and destructive elements. Arguably, remixing and other information sampling adds value to information protected by copyright and trademark law while potentially diluting markets the law protects on behalf of the information producer. *See* Larry Downes, *Viacom v. YouTube: The Principle of Least Cost Avoidance*, The Tech. Liberation Front, June 26, 2010,

As I argue in my book, *The Laws of Disruption*, privacy laws are best understood as legal protections against destructive uses of information by different categories of users. Seen that way, there is not one overarching and overwhelming privacy problem, but several very different privacy problems, each deserving of particular analysis and, one hopes, its own resolution. Here are the main categories of destructive information uses:

| Information User | Destructive Uses |
|---|---|
| Criminals | Identity theft, phishing, malware and other forms of fraud |
| Commercial enterprises | Surreptitious collection of consumer information for sale or use in marketing, often without adequate compensation or revenue sharing with the consumer |
| Other consumers, friends, family | Stalking, bullying, accidental or intentional disclosure of embarrassing or secret information |
| Government and other state actors | Unlawful search and seizure, accidental disclosure |
| News media | Publication of defamatory or erroneous information that damages reputation |
| Employers and business associates | Eavesdropping and other monitoring to identify poor performance, violation of employer rules, or business secrets |
| Insurers and health care professionals | Collection and use of known and potential risks to determine coverage or the danger of accidental disclosure |

Though many of these destructive uses were discussed at the FTC hearing, it should be noted at the outset that the agency's charter only extends to the first and second category.[19] (To be fair, FTC staff frequently reminded the speakers to limit their discussion to topics over which the agency had jurisdiction.) Why, then, did the speakers repeatedly bring up all the others? For one thing, some

---

**http://techliberation.com/2010/06/26/viacom-v-youtube-the-principle-of-least-cost-avoidance/**. For now, I'll stick to the "easier" problems of uses that are almost purely destructive.

19 *See* Fed. Trade Comm'n, *Privacy Initiatives*, *Introduction*, http://**www.ftc.gov/privacy**. As the agency explains the scope of its privacy initiatives, "The Federal Trade Commission is educating consumers and businesses about the importance of personal information privacy, including the security of personal information. Under the FTC Act, the Commission guards against **unfairness and deception** by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information. Under the **Gramm-Leach-Bliley Act**, the Commission has implemented rules concerning **financial privacy** notices and the administrative, technical and physical **safeguarding** of personal information, and it aggressively enforces against **pretexting**. The Commission also protects consumer privacy under the **Fair Credit Reporting Act** and the **Children's Online Privacy Protection Act**."

of the most lurid stories suggesting a privacy crisis come from the other categories, making them irresistible to those arguing for a crisis response. Unfortunately, most parties in the privacy "debate" so far have shown little interest in cabining the discussion to manageable and discrete problems when an emotional point is there to be scored.

Indeed, one important reason to evaluate the categories of destructive information use separately is to help us see that some goals of the privacy movement are mutually exclusive. In the abstract, for example, most people are uncomfortable with the proliferation of surveillance cameras in urban locations. But listen to the indignation that erupts the minute a serious crime or terrorist act occurs and the police turn out not to have caught it on film.

Or take the often-repeated example of the victim of domestic violence, used as a stalking horse for the proposition that search engines, cell phone carriers, and other service providers, who collect bits and pieces of information that might be used to identify and locate an individual, should immediately purge their databases, lest they fall into the wrong hands.

Turn the problem around, however, and you can make the exact opposite case. For the victim, it's important to erase all traces of their online activity. But for the perpetrator, effective law enforcement requires as much information as possible.[20] Optimally, we'd like to tell information collectors to purge data about victims but retain it for criminals, but of course, we don't know who is who until after the fact. What's a data collector to do?[21]

This isn't a hypothetical problem. Lawmakers in the United States and the European Union are simultaneously putting pressure on phone companies, search engines and social networking sites to both purge and retain the same data, a kind of whipsaw that has led these providers uncharacteristically to call for new laws—laws that would give them a straight answer on what is expected of them.

It's also worth noting that in the United States in particular, most of the existing legal protections for private information are squarely aimed at deterring destructive uses by criminals and by governments themselves. Every year I have to convince another batch of students that the right to privacy recognized by U.S. courts and grounded in the U.S. Constitution does not apply to conflicts

---

20 Declan McCullagh, *Web Searches Lead to Murder Conviction*, CNET NEWS.COM, Feb. 12, 2010, **http://news.cnet.com/8301-13578_3-10452471-38.html**.

21 *See* Miguel Helft, *For Data, Tug Grows Over Privacy vs. Security*, N. Y. TIMES, Aug. 2, 2010, **http://www.nytimes.com/2010/08/03/technology/03blackberry.html**. *See also* Lance Whitney, *German Court Rules Against Data Retention Policy*, CNET NEWS.COM, March 2, 2010, **http://news.cnet.com/8301-13578_3-10462117-38.html**.

with commercial enterprises, parents, friends, or the news media. (Indeed, the latter are strongly protected by the First Amendment against such regulation.)

With at least a whiff of First Amendment rationale, even the common law torts that deal with conflicts between individuals over information use—including rights of publicity, defamation, and "false light" claims—have fallen into disrepute during the last fifty years.[22]

Here there are also economic forces at work: information technology has erased the temporary mask of anonymity created by 19th century urban life, reviving a social goal of transparency as old as Hawthorne's *The Scarlet Letter*.[23] American life, built of equal parts frontier necessity and Puritan aspiration, calls for complete and accurate information about each other. That goal increasingly weighs more heavily in private disputes over what Warren and Brandeis in 1890 famously termed "the right to be left alone."[24] More about that in a moment.

Why the focus on state actors? The principal fear of the drafters of the Constitution, obviously informed by the experience of the colonies, was with potential tyranny from government. The government, after all, practically holds a monopoly on the coercive power of the military and the ability to incarcerate.

For historical reasons, the focus is very different in Europe and many parts of Asia, which have enacted strong privacy laws that align citizens and democratic governments against everybody else. The difference between U.S. and European law, in particular here, is perhaps the broadest effort to apply terrestrial laws to digital life generally.[25]

In the United States, distrust of government evolved to include a fear that private information could be misused to achieve the same ends as more overt repression. These fears were underscored by the late 20th century scandals,

---

22 *See* Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222 (7th Cir. 1993) (opinion by Posner).

23 NATHANIEL HAWTHORNE, THE SCARLET LETTER (Ticknor, Reed & Fields 1850).

24 Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890), (discussed below). *See also* Peggy Noonan, *The Eyes Have It*, WALL ST. J., May 21, 2010, **http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748703559004575256732042885638.html**.

25 *See* Adam Liptak, *When American and European Ideas of Privacy Collide*, N.Y. TIMES, Feb. 26, 2010, **http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html**; Kevin J. O'Brien, *Europe Says Search Firms Are Violating Data Rules*, N.Y. TIMES, May 26, 2010, **http://www.nytimes.com/2010/05/27/technology/27data.html**; Jessica E. Vascellaro, *Ten Countries Ask Google to do More to Protect Privacy*, WALL ST. J., April 20, 2010, **http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748704671904575194992879579682.html**.

including The Pentagon Papers and later Watergate, which led to the first comprehensive anti-wiretapping law at the federal level.[26]

So, with notable exceptions, all existing U.S. privacy laws afford limited—and perhaps inadequate—protection to citizens *against their governments*. That fact is often whitewashed in the furor of the privacy debate. The ACLU of Northern California, for example, recently published a white paper called *Cloud Computing: Storm Warnings for Privacy?*[27] The paper points out the mismatch between existing privacy law and the reality of cloud computing, where personal information is turned over for storage and processing to a variety of third parties and often to their unnamed and changing business partners.

The report never quite says so directly, but all the proposed reforms are aimed at curbing the ability of state actors, not private parties, to gain access and make use of data in the cloud. It is not "consumers" as the report characterizes them, who need to be worried about their "privacy protections" in the cloud. It is citizens. I think the ACLU is right to be worried about government access to cloud data sources, but I wish it wouldn't pretend to have a broader agenda than it does.

Though the right to privacy against government is now firmly established, it's also worth remembering that this is a relatively new right. Despite all the talk of one's right to privacy, you will scour the Bill of Rights in vain for any reference to privacy even against state actors.

It wasn't until the 1960s that the Supreme Court began to interpret the First Amendment's free speech provisions, along with the Fourth Amendment's prohibition against unreasonable searches and seizures of people and their property, as implying a more general right to privacy enforceable against state actors.[28] In key cases, including *Griswold v. Connecticut* (birth control), *Roe v. Wade* (abortion), and more recently *Lawrence v. Texas* (homosexuality), the Court struggled to reign in government intrusions into the private lives of citizens, intrusions the Founders would never have imagined possible. Lacking a

---

26 *See* The Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 et. seq.

27 Am. Civil Liberties Union of N. Cal., *Cloud Computing: Storm Warnings for Privacy?*, Jan. 2010, **http://www.dotrights.org/sites/default/files/Cloud%20Computing%20Issue%20Paper.pdf**.

28 *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 483 (1965) ("In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion."); Roe v. Wade, 410 U.S. 113, 152 (1973) ("The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as [1891], the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution.").

Constitutional provision that guaranteed the right to privacy for basic human activities, the Court more-or-less invented one.

At the same time, as 20th century society came to recognize that information was a kind of property (something with value, in any case), the perception of a right to privacy emerged. It was found, to use Justice Douglas's famous but unfortunate phrase, in "the penumbras and emanations" of the Bill of Rights.[29] But to reiterate, the right to privacy, as it is currently understood, is a right to be free of unreasonable interference from government, not from each other or the businesses with which we interact.

Some of today's most vocal privacy advocates are calling for a broader right of privacy, one that could be asserted against any or all of the destructive information uses and perhaps against many of the productive uses as well.

An earlier effort to create such a right, it is worth noting, failed. In 1890, Samuel Warren and Louis Brandeis wrote a famous article for the *Harvard Law Review* in which they called for the creation of a general right of privacy, defined as the "right to be left alone."[30] The article was inspired by Warren's personal experience. Warren's wife was the daughter of a U.S. Senator, and Warren was appalled to discover that their daughter's wedding was reported, with photographs, in *The Washington Post*.[31]

Warren and Brandeis's proposal led to some experimentation, mostly at the state level and mostly through judge-made law. Common law courts invented new tort injuries for damage to reputation, rights of publicity, and more expanded forms of defamation, including the portrayal of someone in a "false light." Many of these rights are no longer recognized, or have become nearly impossible to enforce.

Under the Supreme Court's 1964 decision in *New York Times v. Sullivan*,[32] for example, public officials must prove actual malice to recover damages for defamation. Extending that decision, the Court held in the *Florida Star*[33] case that a rape victim could not prevent a newspaper from publishing information from a police report about the crime committed against her. More recently,

---

29 *Griswold*, 381 U.S. at 484. Justice Thomas, a strict constructionist, has a sign on his desk asking visitors to kindly keep their penumbras off his emanations.

30 Warren & Brandeis, *supra* note 24.

31 What would Warren think of today's celebrity media, or reality TV, in which non-celebrities volunteer to give themselves the celebrity treatment?

32 376 U.S. 254 (1964).

33 Florida Star v. B.J.F., 491 U.S. 524 (1989).

homeowners have been rebuffed in efforts to prohibit Google maps from photographing their homes.[34]

The Warren and Brandeis experiment failed for a good reason, at least from an economic standpoint. Many of the uses of private information that Warren and Brandeis sought to outlaw are in fact productive uses, generating substantial social value that outweighs the costs to the individuals of keeping such information public.

It may be very important for you to keep secret the fact that you have a criminal record, a communicable disease, a Swiss bank account or a secret liaison with an employee. But it is more valuable to the rest of us to know these things about you, if only to know how many others have the same attribute so we can take appropriate actions—quarantine the sick, pass stricter banking laws, etc. The benefits of disclosure, the courts have determined, generally outweigh the costs of secrecy.

Warren and Brandeis weren't entirely wrong, however. It's important to note that the same "private" information can also be used destructively. I might overestimate the risks of hiring a former felon, for example, or even exclude potential tenants for my apartments based on an irrational reliance on personal traits and associated stereotypes. That's why we have anti-discrimination laws, one of the notable exceptions where protections for misuse of personally-identifiable information extend to commercial and other non-governmental users. But it is an exception, narrowly focused on a particular abuse.

Generally speaking, in fact, privacy legislation in the U.S. has only been enacted when legislators find particular and persistent market failures—failures, that is, to use personally-identifiable information in rational ways. Along with anti-discrimination laws, we have laws that control private information use in credit reporting, medical records, and identity theft and other forms of financial fraud.[35] In each of these cases, the law is focused on a particular destructive use in a particular context, with remedies for consumers narrowly-tailored to leave as much information unprotected as possible.

## Privacy: The Solution

Particular solutions to particular information use failures are, I believe, a model lawmakers ought to be encouraged to continue following.

---

34 *See* Steven Musil, *Google Wins Street View Privacy Suit*, CNET NEWS.COM, Feb. 18, 2009, **http://news.cnet.com/8301-1023_3-10166532-93.html**.

35 *See* Larry Downes, *If Feds Fail, What Can Stop Identity Theft?* CIO INSIGHT, July 2005, http://**www.cioinsight.com/c/a/Past-Opinions/If-Feds-Fail-What-can-Stop-Identity-Theft/**.

But maybe it's time to revisit Warren and Brandeis's call for broader privacy protections against non-state actors. The argument in favor would go something like this: Now that the cost of information retention is less than the cost of information deletion, commercial enterprises may soon wield the same kind of coercive power that until now has usually been the domain of governments.

Perhaps the same kinds of risks to society that led the courts to recognize a "zone of privacy" for information collection and use now justify extending that zone to the complicated web of enterprises that collect, consolidate, and resell information about a wide range of consumer behaviors—as well as to companies that by design collect intimate information, including social networking sites and anything mobile.

But note that even if this argument carries the day—that is, if the benefits of reducing destructive uses of private information in some of the other categories exceed the costs (including inadvertent limits on some productive uses, such as the advertising that supports so much "free" media), it doesn't necessarily follow that the FTC or any other government entity is the right institution to define, enact, and enforce those new legal rights.

Again, the FTC's authority is limited to investigating anticompetitive behavior and "unfair" or "deceptive" trade practices—terms that have clear meanings under the agency's statute, its previous decisions and policy statements, and court cases interpreting the law.

Moreover, there is the agency's tendency simply to react with dismay to new technologies and then to move on when the technology soon after resolves its own problems. This habit—not limited to the FTC by any means—leads me to doubt its institutional capacity to define what kind of new privacy rights consumers should have, independent of always-changing technological capacities. The FTC's staff invokes the phrase "privacy by design" like a mantra in conversation with policy representatives and consumer advocates. The hope behind that phrase is that future technologies can be engineered to protect privacy interests. But the phrase is meaningless without first defining what interests are to be protected.

There are bigger reasons to question whether federal or state government is well-suited to the role of privacy cop. For one thing, competing government interests in effective law enforcement create a kind of regulatory schizophrenia over the use of privacy-enhancing technologies. As an example, consider encryption. Given that one common theme of destructive information use in several categories, as noted in the chart above, involves accidental disclosure (including access gained illegally by hackers or by fraud), it might be thought that more widespread use of encryption technology would reduce those risks. But the federal government has been ambiguous at best about encouraging

enterprises to adopt encryption. In the 1990s, basic encryption methods were classified as a "munition" by the Department of State (and later, the Department of Commerce). Phil Zimmerman, the inventor of an open source encryption protocol known as Pretty Good Privacy, was the subject of a lengthy criminal investigation for exporting "weapons" without a license. Only under intense pressure from the courts in a series of First Amendment decisions did the Commerce Department finally liberalize these export controls.

There was also the memorable fight in the early 1990s over the Clipper Chip, a government-developed encryption technology for use in cell phones.[36] Had the chip been made mandatory or even widely deployed (opponents, including the Electronic Frontier Foundation (EFF), successfully prevented that outcome), it would have given law enforcement a back door into mobile phone calls and might have led to the prohibition of other encryption technologies.[37]

Federal and state governments also receive failing grades at adopting and using the kinds of safe data handling practices some think these governments should enforce against everyone else. That failure is evidenced by numerous embarrassing breaches and stolen unsecured laptops containing millions of records of sensitive citizen data. Government in this sense offers a good example (several, actually) of how *not* to manage privacy and the worst, not best, safe handling practices. Finally, a general problem of state, as opposed to federal, legislation is the potential for fifty different definitions of privacy, all imposed on what is a global information economy.

More broadly, there's a disturbing irony to handing privacy enforcement over to governments, an argument I have also made with regard to enforcement of net neutrality principles. Enforcement powers would require the agency to examine the information and how it was disclosed. For agencies to investigate and punish banned uses of private information, they would necessarily need to have access to the data sources in question.

If I complain, to the FTC, for example, that a social networking enterprise is selling my information in violation of some future privacy protection law, how else will the agency evaluate my claim without looking deeply into the company's information practices? Like any good audit, they will need to follow the flow of information from beginning to end to determine what, if any, violations of law occurred.

---

[36] For more information on the Clipper Chip, including government documents and public response, visit **http://epic.org/crypto/clipper**.

[37] The Clipper Chip fight was instrumental in the formation of EFF, proving once again the law of unintended consequences. The government lost the battle, but more importantly, it inadvertently helped to organize a permanent and effective opposition.

Yet state actors, as noted above, are currently the most restricted from seeing this information. In a bitter irony, enforcement of privacy rights against enterprises would have the effect of exposing data to the government that it otherwise would be forbidden to see. As a result, there is the potential for abuse of that privilege in the name of law enforcement or other government priorities (e.g., terrorism or tax fraud).[38]

Who else can define, let alone enforce, new privacy protections against enterprises and other non-state actors? One obvious alternative is self-regulation by the enterprises themselves, perhaps encouraged by the threat of government intervention if the market fails.

There's already a good deal of self-regulation, including voluntary adoption of the FIPs and certification from third parties such as TRUSTe[39] and the Better Business Bureau.[40] Much of this self-regulation, however, presumes the usefulness of the notice regime which, as noted, no one presumes any more.

The potential is there, however, for more effective self-regulation. Even companies who make money from information collection and its use are worried about the privacy problem, or at least the perception of one. Some are even calling for new legislation, in part to solve the whipsaw problem described above.

Microsoft and other companies who are counting on cloud computing as the next major computer architecture are eager for regulatory frameworks that will both allay consumer anxiety and give cloud-based service providers safe harbors in which to develop their offerings.

An emerging consensus among a wide range of technology companies and information service providers would move the discussion from guidelines about private information notice to rules about information use. The "use" approach would develop acceptable principles for how collected and retained data (private or otherwise) can be used, by whom, and with what controls reserved to consumers to limit or block those uses.

As part of the Business Forum for Consumer Privacy (BFCP), Microsoft and others are calling for a legislated framework for use-based rules.[41] What does

---

38 *See* Declan McCullaugh, *Amazon Fights Demand for Customer Records*, CNET NEWS.COM, April 19, 2010, **http://news.cnet.com/8301-13578_3-20002870-38.html**.

39 *See* **http://www.truste.com**.

40 *See* **http://www.bbb.org/us/Business-Accreditation**.

41 The Business Forum for Consumer Privacy, *A Use and Obligations Approach to Protecting Privacy: A Discussion Document*, Dec. 7, 2009,

that mean? According to a 2009 BFCP white paper, a "use-and-obligations" model requires all organizations to be transparent, offer and honor appropriate choice, ensure that risks to consumers related to use are assessed and managed, and implement security for the information they maintain.[42] The white paper describes a taxonomy of use types (for example, marketing, internal operations) within the enterprise category, and tries to define an appropriate set of default rules that should apply for each.

The BFCP approach is certainly more productive than the anxiety-based conversations. Focusing on use, for one thing, moves the conversation away from the emotional subject of privacy to the more rational subject of propriety, by which I mean the recognition that both enterprises and consumers participate in the creation of valuable new sources of data and both should have rights to monetize that value. Consumers ought to be able to buy out enterprises for productive uses they don't want, and vice-versa.

In this scenario, privacy policy evolves from self-regulation by the market to actually becoming a market for private and other data. Assuming this market works, data will be put to the most highly-valued productive uses, and those uses that are not valued or are destructive will not be implemented.[43] As with any market, the government will stand in the background to ensure the rules are obeyed and to intervene when market failures occur.

One immediate concern about the creation of a privacy market is that consumers will have no voice in its creation or operation. Consumers, after all, are individuals, easily overwhelmed by the economic might of large corporations, who can be expected to develop rules that give consumers an unfair disadvantage in the information marketplace.

That would have been an entirely reasonable concern in the pre-digital age, and one of the principal justifications for the creation of private and public consumer watchdog groups such as the FTC in the first place (the agency is nearly 100 years old). Such groups, at least in theory, lobby and sue on behalf

---

**http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf**.

42 *See* Hunton & Williams LLP, *Business Forum for Consumer Privacy Introduces New Data Protection Model*, Dec. 21, 2009, **http://www.huntonprivacyblog.com/2009/12/articles/events/business-forum-for-consumer-privacy-introduces-new-data-protection-model/**.

43 This emerging privacy market, operating with minimal transaction costs or "friction," could present a wonderful opportunity to test Ronald Coase's theory that absent transaction costs, stakeholders will necessarily bargain to the most productive use of a given resource. See Ronald Coase, "The Problem of Social Cost," 3 Journal of Law & Economics 1 (1960) (the so-called "Coase Theorem").

of large groups of consumers to ensure their interests are fairly represented in a wide variety of market activities. (The class-action mechanism is another example.) To use the economic terminology, these legal constructs overcome the collective action problem of individual users whose individual losses may be too small to justify the expense of enforcing or even negotiating rights.

But the same technologies that create the privacy problem are also proving to be the source of its solution. Even without government intervention, consumers increasingly have the ability to organize, identify their common demands, and enforce their will on enterprises.[44]

Facebook's journey to a fair privacy policy continues to be instructive here. The company's ongoing privacy crisis actually started in early 2009, when Facebook announced what was in fact a modest change to its terms of service. Some users who read the modification objected to it, and used the very tools Facebook provides for group formation to create a "People Against the New Terms of Service" page, which quickly signed up 100,000 fans.[45] (Still a relatively small number given Facebook's size: now over 500 million users worldwide.)

The revolt and (perhaps more influential) the ensuing bad publicity led Facebook to withdraw the changes—no lawsuit or legislation necessary. Even more, the company soon announced that it was changing its entire approach to governance. In the future, the company said, it would rewrite its user agreement to be understandable to lay readers, and circulate future changes as proposals to the entire population of users.

If enough users objected to a proposed change, the changes would be put to a vote. (The changes to privacy settings that set off the firestorm in the fall of 2009 were circulated ahead of time, but didn't qualify for a vote, perhaps suggesting that Facebook's "constitution" still needs some tweaking.)

So assuming that buyers and sellers have equal access and power, how would a market for private data work in practice?[46] There are already some good

---

44 Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. TIMES, July 16, 2010, **http://www.nytimes.com/2010/07/18/business/18unboxed.html**; L. Gordon Crovitz, *Privacy Isn't Everything on the Web*," WALL ST. J., May 24, 2010, **http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748704546304575260470054326304.html**.

45 To view the Facebook page, visit **http://www.facebook.com/group.php?gid=77069107432**.

46 Venture capitalists have begun to recognize the potential of privacy markets and are investing accordingly. *See* Pui-Wing Tam & Ben Worthen, *Funds Invest in Privacy Start-ups*, WALL ST. J., June 20, 2010,

prototypes in place in the form of consumer loyalty and affinity programs that have been around for decades. The grocery store scanner data can already determine what items have been bought at the same time, but in order to tie that collection to particular demographic characteristics (gender and zip code are the most important for marketing purposes), it requires the cooperation of the customer.

So, in exchange for using a club card and giving the store permission to connect purchases to a particular customer, the consumer gets special discounts. In effect, the store recognizes the value of the identifying information and pays the consumer for it.

That approach is attractive for several reasons. For one thing, it is entirely voluntary—consumers make the decision to sign up for the programs or not, or even whether or not to participate in any individual transaction. This proto-market also operates under very low transaction costs. Instead of negotiating for the purchase of each individual data element with each individual consumer, a framework is established that allows both parties to opt out at will. Discounted prices become a new form of currency requiring no oversight. No lawyers and no regulators are involved.

The loyalty program also makes explicit what I think is the most important feature of the privacy debate, one that is usually lost in the extreme rhetoric of both sides. Information only attains its true monetizable value when every participant in the transaction has an incentive to provide it, authenticate it and protect it. Retail data is of limited use to the supply chain without demographic linkages. Individual data is not marketable unless someone is able to collect and analyze large volumes of it. As with all information exchanges, the whole is greater than the sum of its parts.

Today, even fifty years into the computer revolution, most aspects of retail engineering, including production planning, pricing and promotions, product design, forecasting, and marketing, operate with precious little real information. Most are more black arts than science. With the potential capture of complete life-cycle transaction data, there is at last the hope of discipline, and with it great increases in efficiency.

And in the next digital decade, we now have the potential for information to be collected post-sale: How did you like the product? Did it perform as expected? What other products did you use it with? It becomes even clearer that without

---

**http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748703438604575315182025721578.html**.

cooperation from the consumer, no real value will come from vast data warehouses that enterprises have built but rarely use effectively.[47]

The privacy marketplace is already here, and there is every indication that as technology continues to evolve, an increasingly robust and valuable set of institutions will develop alongside of it. As new forms of data enter the digital domain, new tools and techniques will emerge to harness their value and allocate it among those who develop it.

In order for the technology of information processing to reach its potential, however, the histrionics of the privacy debate must stop. Instead, consumers must be encouraged and educated to think about information use in terms of productive and destructive costs and benefits. In short, we must learn to think rationally about information value. If the FTC and other regulators are looking for a role in solving the problems of online privacy, a good starting point would be to contribute constructively to the emergence of this organic, elegant solution.

---

47 *See* LARRY DOWNES, THE STRATEGY MACHINE: BUILDING YOUR BUSINESS ONE IDEA AT A TIME, (Harper Business 2002), Chapter 3, *The Information Supply Chain*. *See also* Jules Polontesky & Christopher Wolf, *Solving the Privacy Dilemma*, THE HUFFINGTON POST, July 27, 2010, **http://www.huffingtonpost.com/jules-polonetsky/solving-the-privacy-dilem_b_660689.html**.

# CHAPTER 9

## CAN SPEECH BE POLICED IN A BORDERLESS WORLD?

# The Global Problem of State Censorship & the Need to Confront It

By John G. Palfrey, Jr.*

Speech is policed through technical Internet filtering in more than three dozen states around the world. This practice is increasingly widespread. States including China, Iran, Syria, Tunisia, and Uzbekistan have extensive Internet filtering regimes in place. Censorship using technological filters is often combined with restrictive laws related to what the press can publish, opaque surveillance practices, and severe penalties for people who break the state's rules of using the Internet. This trend has been emerging, and documented with precision, for nearly a decade.[1]

An empirical study of technical Internet filtering tells only part of the story, however. Speech is policed actively in parts of the world with regimes that are substantially more democratic than China or Iran. Through mechanisms that include surveillance, "encouraging" self-censorship, intellectual property restrictions, and defamation laws, virtually every state in the world polices online speech through multiple means.[2] As more and more of everyday life moves onto the Internet, so has regulation of that activity. These forms of regulation are driven by the same types of concerns that animate the regulation of speech in traditional environments.

---

* John Palfrey is the Henry N. Ess III Professor of Law at Harvard Law School and Faculty Co-director of the Berkman Center for Internet & Society at Harvard University. This chapter draws upon research by the OpenNet Initiative, which is a collaboration that joins researchers at the Citizen Lab at the Munk Centre, University of Toronto (Prof. Ron Deibert, principal investigator), the SecDev Group (formerly the University of Cambridge where Rafal Rohozinski is principal investigator), and the Berkman Center (where the author and Jonathan Zittrain are co-principal investigators). The author is grateful to the large number of researchers who have participated in gathering, over nearly a decade, the data on which this chapter draws. Parts, though not all, of this argument have been published in other volumes.

1 *See* **www.opennet.net** for the results of the OpenNet Initiative's research since 2002. *See also* Ronald Deibert, John Palfrey, Rafal Rohozinski, & Jonathan Zittrain, eds., ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING (MIT Press, 2008) and Ronald Deibert, John Palfrey, Rafal Rohozinski, & Jonathan Zittrain, eds., ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE (MIT Press, 2010), in which variations on these themes appear throughout.

2 Like technical Internet filtering, this is not a new phenomenon. *See* Adam D. Thierer, *190 Internet Censors? Rising Global Threats to Online Speech*, 38 TechKnowledge, July 26, 2002, **www.cato.org/pub_display.php?pub_id=11535**.

The social, political, and cultural issues that give rise to online speech restrictions are familiar. Child safety is one of the primary drivers of online speech regulation, most commonly related to pornography. Police use surveillance to track the misdeeds of wrong-doers, in turn causing a chilling effect on online activities. Business people, authors, musicians, and others want their intellectual property rights vindicated to the fullest extent, prompting extensive intellectual property restrictions online. Those who perceive harm to their reputations seek the extension of defamation laws to the digital world. In each of these instances, speech restrictions cross traditional and digital environments more or less seamlessly.

## Is It True that "All Politics Is Local" in the Digitally-Mediated World?

The problem of policing speech on the Internet arises at every level of government, from local political conversations about community norms to the international debate over Internet governance. The principal difference at these multiple levels of governance is the willingness to address the difficult problems of when to regulate speech online and the ramifications that flow from doing so. State legislatures fight over whether to constrain speech in schools when young people engage in cyber-bullying.[3] In the United States, Congress takes up the same issue from the perspective of federal law enforcement and funding for schools and education. At the same time, the topic of speech-based controls is an important aspect of global Internet regulation. However, it rarely makes it into the agenda at the international level as a genuine, openly-discussed matter.

At the local level, there is often substantial appetite to regulate speech online, primarily as a response to fears about child safety. The clearest example at the local level in the United States is the effort to curb cyber-bullying through school environments, which states, regional, and municipal governments seek to regulate.[4] Speech, largely online in social network environments, is policed by local regulation that bars young people from expression that may harm their peers psychologically. While the debate rages as to the appropriateness of these regulations, dozens of states in the United States have enacted, or have considered enacting, these types of laws at the local level. Courts have split as to the constitutionality of such provisions. In short, intense local concerns,

---

3 The First Amendment Center published a fine series of essays and research materials related to the speech restrictions associated with the anti-bullying efforts, with special attention paid to state legislative activities. *See* First Amendment Ctr., *Online Symposium: Cyberbullying & Public Schools*, **www.firstamendmentcenter.org/collection.aspx?item=cyberbullying_public_schools**.

4 Sameer Hinduja, & Justin W. Patchin, Cyberbullying Research Center, *State Cyberbullying Laws: A Brief Review of State Cyberbullying Laws and Policies*, July 2010, **www.cyberbullying.us/Bullying_and_Cyberbullying_Laws_20100701.pdf**.

such as about how young people treat one another, are driving legislative attempts to regulate online speech through school-based enforcement.[5]

At the federal level, online speech restrictions have arisen repeatedly as proposals and as enacted law, in the United States and around the world. Twenty-five years after the creation of the .COM top-level domain, it is apparent that national governments can, and often do, assert sovereignty over the acts of their citizens in the online environment, including limitations on their speech. At a basic level, in the United States and in many other jurisdictions, speech that is deemed to be harmful in the offline world is considered equally unlawful in the online environment. For the speaker, there is no free pass simply because the utterance in question appears online.

The primary difference between the policing of speech online and offline lies in terms of how intermediaries are treated. Under United States federal law, and the national law of many other jurisdictions, intermediaries that enable people to publish speech online are exempt from liability in most cases, for example, from claims of defamation under Section 230 of the Communications Decency Act.[6] There are exceptions to this rule, even in the United States: Criminal matters and copyright violations fall outside of the statute's safe harbor provisions.[7] In other jurisdictions, regulation of intermediaries may soon be the law. For instance, in Sweden, the Data Inspection Board issued a report in July 2010 asserting that companies offering social media services, such as blogs, Facebook, or Twitter, have a legal obligation to monitor personal data posted to the pages on their site.[8]

At the international level, we observe extensive policing of speech online, but discussion of the issues involved is largely invisible—or else not happening at all. While there is extensive and healthy debate about many aspects of the problem of Internet governance, the discussion does not reach the hard problems of when online speech regulation should be permitted. There are many issues worthy of the attention of the many capable minds focused on Internet governance, but the topic of speech regulation rarely makes the list of what is, in fact, publicly discussed and vetted seriously.[9] The primary focus for

---

5 *See* Ronald Collins, *A Look at "Cyber-bullying and Public Schools*," March 31, 2009, **www.firstamendmentcenter.org/analysis.aspx?id=21410**.

6 47 U.S.C. § 230.

7 *See id.*

8 *See* Swedish Data Inspection Board Report, July 5, 2010, **www.datainspektionen.se/in-english/** (on intermediary liability); *see also Companies Responsible for Social Media Content*, THE LOCAL: SWEDEN'S NEWS IN ENGLISH, July 5, 2010, **www.thelocal.se/27606/20100705/**.

9 The International Telecommunication Union (ITU), official host of the World Summit on the Information Society (WSIS) in Geneva, has held several events designed to refine the debate further. Through these events, the ITU has convinced dozens of observers to

Internet governance discussions continues to be issues related to the management of Internet resources, including the domain name system and related policy issues. Discussion of the non-profit Internet Corporation for Assigned Names and Numbers (ICANN) continues to play a central role. ICANN occupies an arcane bit of turf—essentially, the port allocation business. That is important in some respects but does not appear to concern most users of the Internet, particularly in a world in which most people find Internet resources through search engines and, increasingly, mobile devices and applications.[10] As an example, within the context of the Internet Governance Forum 2009 meeting in Egypt, the first substantive panel of the event was devoted to traditional ICANN-related matters such as the transition from Internet Protocol version 4 (IPv4) to IPv6 and the addition of new top-level domains (TLDs).[11] Possible topics for consideration, other than ICANN reform and these highly specific technical issues, each more important to the end-users of the Internet and their sovereigns, have included a fund for developing countries to build Internet infrastructure, the quandary of what to do about spam, and a cluster of intellectual property concerns.

Internet speech restrictions should serve as the focal point for the world's heads of state and their designees when Internet governance is on the table. While online speech restrictions raise a wide array of issues, a discussion of Internet filtering would hone in on whether states actually *want* their citizens to have full access to the Internet or not. It would help guide a public conversation about what is truly most important about having access to the Internet and the extent to which states place a premium, if at all, on the global flow of information. Without collective action, the Internet will likely continue to become balkanized into a series of local networks, each governed by local laws, technologies, markets, and norms. As Jonathan Zittrain argued in *Who Rule the Net?*, the predecessor of this collection, we may be headed toward a localized version of the Internet, governed in each instance by local laws.[12] If such a version of the Internet is inevitably part of our future, there ought to be open and transparent

---

publish what comprises an extensive body of work on this topic on the ITU website. In addition, long-time experts in this field, such as Prof. Milton Mueller of Syracuse, and others, have constructed helpful models to structure the conversation. For suggestions on further information of this general nature, please see **www.netdialogue.org**, a joint project of Harvard Law School and Stanford Law School.

10 Witness the abysmal turnout for ICANN's election of 2000, in which a free and open election for five ICANN directors attracted fewer than 100,000 votes globally.

11 Internet Governance Forum of 2009, Managing Critical Internet Resources, Transcript, Nov. 16, 2009, **www.intgovforum.org/cms/2009/sharm_el_Sheikh/Transcripts/Sharm%20El%20Sheikh%2016%20November%202009%20Managing%20Critical%20Internet%20Resources.pdf**.

12 Jonathan Zittrain, *Be Careful What You Ask For, in* WHO RULES THE NET? INTERNET GOVERNANCE AND JURISDICTION 13-30 (Adam Thierer et al. eds., Cato Inst. 2003).

consideration of ways to embrace it that can preserve elements of the network that are the most important.

## The Internet Filtering Problem

The world may appear borderless when viewed from cyberspace, but geopolitical lines are, in fact, well-established online. The fact that extensive Internet filtering occurs at a national level around the world is clearly documented. Through a collaborative research effort called the OpenNet Initiative,[13] the Citizen Lab at the University of Toronto, the Berkman Center for Internet and Society at Harvard University, and the SecDev Group are working together to compare Internet filtering practices of states in a systematic, methodologically rigorous fashion. In the past several years, OpenNet Initiative has sought to reach substantive conclusions about the nature and extent of Internet filtering in roughly 70 states and to compare practices across regions of the world. The OpenNet Initiative has released extensive reports that document and provide context for Internet filtering, previously reported anecdotally, in each of the states that it has studied closely. Reports released to date have focused on states in the Middle East and North Africa, Asia, and Central Asia, where the world's most extensive filtering takes place. OpenNet Initiative's research also covers states in every region of the world, including North America and Western Europe, where forms of speech regulation other than technical Internet filtering at the state level are the norm.

Filtering implementations (and their respective scopes and levels of effectiveness) vary widely among the countries OpenNet Initiative has studied. China continues to institute by far the most intricate filtering regime in the world, with blocking occurring at multiple levels of the network and covering content that spans a wide range of topic areas. Though its filtering program is widely discussed, Singapore, by contrast, blocks access to only a handful of sites, each pornographic in nature. Most other states that OpenNet Initiative is studying implement filtering regimes that fall between the poles of China and Singapore, each with significant variation from one to the next. These filtering regimes are properly understood only in the political, legal, religious and social context in which they arise.

Internet filtering occurs in different ways in different parts of the world. Some states implement a software application developed by one of a small handful of U.S.-based technology providers. Burma, in the first incarnation of its filtering regime, used an open source product for filtering, called DansGuardian.[14] Others rely less heavily on technology solutions and more extensively on "soft controls." Sometimes the filtering regime is supported explicitly by the state's

---

13 For more information, see **www.opennetinitiative.net/**.

14 For more information on the DansGuardian filtering product, see **dansguardian.org/**.

legal code; in other cases, the filtering regime is carried out through a national security authority. In yet other instances, the regulation is simply presumed to be permissible. The content blocked spans a wide range of social, religious, and political information. Studies by OpenNet Initiative have reviewed whether individual citizens could access sites in a "global basket" of bellwether sites, testing every jurisdiction across a variety of sensitive areas—akin to a stock index sorted by sector—as well as a list of websites likely to be sensitive in some categories, but only in some countries.

## Extent, Character & Locus of Filtering

More than three dozen states around the world practice technical Internet filtering of various sorts.[15] That number has grown over time. Those states that do filter the Internet have established a network of laws and technical measures to carry out substantial amounts of filtering that could allow the practice to become further embedded in their political and cultural environments. Web content is constantly changing, which poses a problem for the censors. Mobile devices and social networks have further complicated the task of speech regulation online. No state yet studied, even China, seems able to carry out its Web filtering in a comprehensive manner, *i.e.*, consistently blocking access to a range of sites meeting specified criteria. China appears to be the most nimble at responding to the shifting Web, likely reflecting a devotion of the most resources, not to mention political will, to the filtering enterprise.

A state wishing to filter its citizens' access to the Internet has several initial options: Domain Name System (DNS) filtering, Internet Protocol (IP) filtering, or Uniform Resource Locator (URL) filtering.[16] Most states with advanced filtering regimes implement URL filtering, as it can avoid even more drastic over-filtering or under-filtering situations presented by the other choices, discussed below.[17] To implement URL filtering, a state must first identify where to place the filters; if the state directly controls the Internet service provider(s) (ISP), the answer is clear. Otherwise, the state may require private or semi-private ISPs to implement the blocking as part of their service. The technical complexities presented by URL filtering become non-trivial as the

---

15 *See* Deibert et al., ACCESS DENIED, *supra* note 1.

16 Nart Villeneuve, *Why Block IP Addresses?*, NART VILLENEUVE: INTERNET CENSORSHIP EXPLORER, Feb. 14, 2005, **www.nartv.org/2005/02/14/why-block-by-ip-address/**.

17 For instance, IP filtering forces the choice of blocking all sites sharing an IP address. A recent OpenNet Initiative bulletin found more than 3,000 web sites blocked in an attempt to prevent access to only 31 sites. *See* Collateral Blocking: Filtering by South Korean Government of Pro-North Korean Websites**,** OpenNet Initiative Bulletin 009, Jan. 31, 2005, www.opennetinitiative.net/bulletins/009/. DNS blocking requires an entire domain and all subdomains to be either wholly blocked or wholly unblocked. *See* Villeneuve, *supra* note 16.

number of users grows to millions rather than tens of thousands. Some states appear to have limited overall access to the Internet in order to keep URL filtering manageable. The government of Saudi Arabia, for example, made filtering a pre-requisite for public Internet access, delaying any such access for a period of several years until the resources to filter were set in place.

Citizens with technical knowledge can generally circumvent filters that a state has put in place. Some states acknowledge as much: The overseer of Saudi Arabia's filtering program, via the state-run Internet Services Unit, admits that technically savvy users can simply not be stopped from accessing blocked content. Expatriates in China, as well as those citizens who resist the state's control, frequently find up-to-date proxy servers through which they can connect to the Internet while evading filters. While no state will ultimately win a game of cat-and-mouse with those citizens who are resourceful and dedicated enough to employ circumvention measures, many users will never do so—rendering filtering regimes at least partially effective despite the obvious workarounds.

Some of the earliest theorizing about control in the online environment, as discussed in *Who Rules the Net?*,[18] suggested that such state-run control of Internet activity would not work. It is important to note that states such as China have proven that an ambitious state can, by devoting substantial technical, financial, and human resources, exert a large measure of control over what their citizens do online. States, if they want, can erect certain forms of gates at their borders, even in cyberspace, and can render them effective through a wide variety of modes of control.[19] These controls have proven the claims of Jack L. Goldsmith and others who have emphasized the extent to which the online environment can be regulated and the ways in which traditional international relations theory will govern in cyberspace the same as they do in real-space.[20]

That does not mean that the issue is simple. For starters, states ordinarily need a great deal of help in carrying out filtering and surveillance regimes. Enter ISPs, many of which require a license from the government to lawfully provide Internet access to citizens. Much Internet filtering is effected by these private ISPs under respective states' jurisdictions, though some governments partially centralize the filtering operation at private Internet Exchange Points—topological crossroads for network traffic—or through explicit state-

---

18 *Supra* note 12.

19 *See* Jack L. Goldsmith and Tim Wu, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD 65-86 (Oxford University Press 2006).

20 *See* Jack L. Goldsmith, *Against Cyberanarchy*, *in* WHO RULES THE NET?: INTERNET GOVERNANCE AND JURISDICTION (Thierer et al., eds., Cato Inst. 2003).

run clearing points established to serve as gatekeepers for Internet traffic. Some governments implement filtering at public Internet access points such as the computers found within cybercafés. Such filtering can take the form of software used in many American libraries and schools for filtering purposes, or "normative" filtering—government-encouraged interventions by shop-owners and others as citizens surf the Internet in a public place.

Sometimes technical controls are not enough to constrain speech in the manner that the censors want. The exercise of more traditional state powers can have a meaningful impact on Internet usage that does not require the complete technical inaccessibility of particular categories of content. China, Vietnam, Syria, and Iran have each jailed "cyber-dissidents."[21] Against this backdrop, the blocking of Web pages may be intended to deliver a message to users that state officials monitor Internet usage—in other words, making it clear to citizens that "someone is watching what you do online." This message is reinforced by methods to gather what sites a particular user has visited after the fact, such as the requirement of passports to set up accounts with ISPs and tighter controls of users at cybercafés.

As we learn more and more about how Internet filtering takes place, the problems of "governing" the Internet come more sharply into relief—about how control is exerted, about how citizens in one state can or cannot connect to others in another state, about the relationship between each state and its citizens, and about the relationships between states.

## Types of Content Filtered

Around the world, states are blocking access to information online based upon its content—or what applications hosted at certain sites can do—for political, religious, cultural, security, and social reasons. Sensitivities within these categories vary greatly from country to country. These sensitivities often track, to a large extent, local conflicts. The Internet content blocked for social reasons—commonly child safety, pornography, information about gay and lesbian issues, and sex education—is more likely to be the same across countries than the political and religious information to which access is blocked.

---

21 Reporters Sans Frontières, *Internet Enemies: China*, **en.rsf.org/internet-enemie-china,36677.html** (last accessed Aug. 25, 2010) ("Thirty journalists and seventy-two netizens are now behind bars for freely expressing their views."); Reporters Sans Frontières, *Internet Enemies: Viet Nam*, **en.rsf.org/internet-enemie-viet-nam,36694.html** (last accessed Aug. 25, 2010) ("Vietnam is the world's second biggest prison for netizens: it now has seventeen of them behind bars."); Reporters Sans Frontières, *Internet Enemies: Syria*, **en.rsf.org/internet-enemie-syria,36689.html** (last accessed Aug. 25, 2010) ("At least four netizens are currently behind bars."); Reporters Sans Frontières, *Internet Enemies:Iran*, **http://en.rsf.org/internet-enemie-iran,36684.html** (last accessed Aug. 25, 2010) ("Some thirty netizens have been arrested since June 2009, and a dozen are still being detained.").

Several states carry out extensive filtering on certain topics. OpenNet Initiative testing has shown that 50% or more of the sites tested on a given topic (like sex education) or application (such as anonymization tools) are inaccessible. Very rarely does any state manage to achieve complete filtering on any topic/application. The only areas in which 100% filtering is approached are pornography and anonymizers (sites that, if left unfiltered, would defeat filtering of other sites by allowing a user to access any Internet destination through the anonymizers' gateways). States like Burma, which reportedly monitors e-mail traffic, also block a high percentage of free e-mail service providers. Such complete, or near-complete, filtering is additionally only found in countries that have outsourced the task of identifying pornographic sites to one of several for-profit American companies, and is inevitably accompanied by over-blocking. Outside of these three areas, OpenNet Initiative testers are consistently able to access some material of a similar nature to the sites that were blocked.

## Filtering & Over-breadth

Internet filtering is almost impossible to accomplish with any degree of precision. There is no way to stem the global flow of information in a consistently accurate fashion. A country that is deciding to filter the Internet must make an "over-broad" or "under-broad" decision at the outset. The filtering regime will either block access to too much or too little Internet content. Very often, this decision is tied to whether to use a home-grown system or whether to adopt a commercial software product, such as SmartFilter, WebSense, or an offering from security provider Fortinet, each of which are products made in the United States and are believed to be licensed to countries that filter the Internet. Bahrain, for instance, has opted for an "under-broad" solution for pornography; its ISPs appear to block access to a small and essentially fixed number of "black-listed" sites. Bahrain may seek to block access to pornographic material online, while actually blocking only token access to such material. The United Arab Emirates, by contrast, seem to have made the opposite decision by attempting to block much more extensively in similar categories, thereby sweeping into its filtering basket a number of sites that appear to have innocuous content by any metric. And Yemen was rebuked by the United States-based WebSense for allegedly using the company's filtering system to block access to material that was not pornographic in nature, contrary to the company's policies.[22]

Most of the time, states make blocking determinations to cover a wide range of Web content, commonly grouped around a second-level domain name or the IP address of a Web service (such as www.twitter.com or 66.102.15.100), rather

---

22 *See* Jillian C. York, *WebSense Bars Yemen's Government from Further Software Updates*, OpenNet Initiative, Aug. 12, 2009, **opennet.net/blog/2009/08/websense-bars-yemens-government-further-software-updates**.

than based on the precise URL of a given Web page (such as www.twitter.com/username), or a subset of content found on that page (such as a particular image or string of text). Iran, for instance, has used such an approach to block a cluster of weblogs that the state prefers not to reach its citizens. This approach means that the filtering process will often not distinguish between permissible and impermissible content so long as any impermissible content is deemed "nearby" from a network standpoint.

Because of this wholesale acceptance or rejection of a particular speaker or site, it is difficult to know exactly what speech was deemed unacceptable for citizens to access. It's even harder to ascertain why, exactly, the speech is blocked. Bahrain, a country in which we only found a handful of blocked sites at the outset of our first round of testing, blocked access to a discussion board at www.bahrainonline.org. The message board likely contains a combination of messages that would be tolerated independently as well as some that would appear to meet the state's criteria for filtering. Likewise, we found minimal blocking for internal political purposes in the United Arab Emirates, but the state did block a site that essentially acted as a catalog of criticism of the state. Our tests cannot determine whether it was the material covering human rights abuses or discussion of historical border disputes with Iran, but in as much as the discussion of these topics is taking place within a broad dissention-based site, the calculation we project onto the censor in the United Arab Emirates looks significantly different than that for a site with a different ratio of "offensive" to "approved" content.

For those states using commercial filtering software and update services to maintain a current list of blocked sites matching particular criteria, OpenNet Initiative has noted multiple instances where such software has mistaken sites containing gay and lesbian content for pornography. For instance, the site for the Log Cabin Republicans of Texas was blocked by the U.S.-based SmartFilter as pornography, and therefore, the apparent basis for its blocking by the United Arab Emirates. (OpenNet Initiative research shows that gay and lesbian content is itself often targeted for filtering, and even when it is not explicitly targeted, states may not be overly concerned with its unavailability.)[23]

As content changes increasingly faster on the Web and generalizations become more difficult to make by URLs or domains,—thanks in part to the rise of simpler, faster, and aggregated publishing tools, like those found on weblog sites and via other social networking applications—accurate filtering is getting trickier for filtering regimes to address unless they want to ban nearly everything. Mobile devices have further added to the complexity of the problem from the censor's viewpoint.

---

[23] OpenNet Initiative, INTERNET FILTERING IN THE UNITED ARAB EMIRATES IN 2004-2005: A COUNTRY STUDY, Feb. 2005, **opennet.net/studies/uae**.

For example, free web hosting domains tend to group an enormous array of changing content and thus provoke very different responses from state governments. In 2004, Saudi Arabia blocked every page on freespace.virgin.net and www.erols.com.[24] However, research indicated the www.erols.com sites had been only minimally blocked in 2002, and the freespace.virgin.net sites had been blocked in 2002, but were accessible in 2003 before being re-blocked in 2004. In all three tests, Saudi Arabia imposed URL blocking on www.geocities.com (possibly through SmartFilter categorization), but only blocked 3% of more than a thousand sites tested in 2004. Vietnam blocked all sites tested on the www.geocities.com and members.tripod.org domains. In OpenNet Initiative's recent testing, it has found that Turkey and Syria have been blocking all blogs hosted on the free Blogspot service.[25]

China's response to the same problem provides an instructive contrast. When China became worried about bloggers, they shut down the main blogging domains for weeks in the summer of 2004. When the domains came back online, the blogging systems contained filters that would reject posts containing particular keywords.[26] Even Microsoft's MSN Spaces blogging software prevented writers from publishing terms like "democracy" from China. In effect, China moved to a content-based filtering system, but determined that the best place for such content evaluation was not the point of Web page access, but the point of publication, and it possessed the authority to force these filters on the downstream application provider. This approach is similar to that taken with Google in response to the accessibility of disfavored content via Google's caching function. Google was blocked in China until a mechanism was implemented to prevent cache access.[27] These examples clearly demonstrate the length to which regimes will go to preserve "good" access instead of simply blocking an entire service.

These examples also demonstrate the increasing reliance by states on "just-in-time" filtering, rather than filtering that occurs in the same, consistent way over time. While the paradigmatic case of Internet filtering was initially the state that wished to block its citizens from viewing any pornography online at any time

---

24 Saudi Arabia blocked every page on **www.erols.com** except for the root page at **www.erols.com** itself, potentially indicating a desire to manage perceptions as to the extent of the blocking.

25 All data from OpenNet Initiative testing can be found in the country-by-country summaries at **www.opennet.net/**.

26 Filtering by Domestic Blog Providers in China, OpenNet Initiative Bulletin 008, Jan. 14, 2005, **www.opennetinitiative.net/bulletins/008/**.

27 This mechanism turned out to be extremely rudimentary, as outlined in a previous OpenNet Initiative bulletin. *See* Google Search & Cache Filtering Behind China's Great Firewall, OpenNet Initiative Bulletin 008, Sept. 3, 2004, **www.opennetinitiative.net/bulletins/006/**.

(for instance, Saudi Arabia), the phenomenon of a state blocking particular speech or types of speech at a sensitive moment has become commonplace. For instance, China blocked applications such as Twitter and YouTube at the time of the 20th anniversary of the Tiananmen Square demonstrations in June 2009. A few weeks later, Iran blocked similar applications, including Facebook, at the time of demonstrations in the streets of Tehran. These blocks are often lifted once the trouble has past. One means of tracking these changes in the availability of applications and websites is a project called Herdict.org, which enables people from around the world to submit reports on what they can and cannot access in real-time.[28]

Alternate approaches that demand a finer-grained means of filtering, such as the use of automated keywords to identify and expunge sensitive information on the fly, or greater manual involvement in choosing individual Web pages to be filtered, are possible, so long as a state is willing to invest in them. China in particular appears prepared to make such an investment, one mirrored by choices demonstrated through more traditional media. For example, China allows CNN to be broadcast within the country with a form of time delay, so the feed can be temporarily turned off as when, in one case, stories about the death of Zhao Ziyang were broadcast.[29] Online policing of speech, even in what appears to be a "borderless world," can be carried out through technical controls at many layers.

## Law, Surveillance & Soft Controls

Just as dozens of states use technical means to block citizens from accessing content on the Internet, most also employ legal and other soft controls. Surveillance practices are most commonly coupled with outright technical censorship. Many states that filter use a combination of media, telecommunications, national security, and Internet-specific laws and regulatory schemes to restrict the publication of and access to information on the Internet. States often require ISPs to obtain licenses before providing Internet access to citizens. Some states—China and Turkey, for instance, which have each enacted special regulations to this effect—apply pressure on cybercafés and ISPs to monitor Internet usage by their customers. With the exceptions of Saudi Arabia and Qatar, no country seems to explicitly communicate to the public about its process for blocking and unblocking content on the Internet. Most countries, instead, have a series of broad laws that cover content issues online, both empowering states that need these laws to carry out filtering

---

28 *See* **www.herdict.org**. The histories of reports of these just-in-time blocking patterns can be viewed from this website.

29 *See* Eric Priest, *Reactions to the Internet & Society 2004 Session on "Business" (December 11, 10:45-12:15)*, Spring 2005, **cyber.law.harvard.edu/blogs/gems/tka/EPriestReactionPaper2.pdf**.

regimes, and putting citizens on general notice not to publish or to access content online that violates certain norms.

Often these soft controls are exercised through social norms or through control at the far edges of the network. Sometimes the state requires non-governmental organizations and religious leaders to register before using the Internet to communicate about their work. In China and in parts of the former Soviet Union, very often the most fearsome enforcer of the state's will is the old woman on one's block, who may or may not be on the state's payroll. The control might be exercised, as in Singapore, largely through family dynamics. The call by the local police force to the Malaysian blogger to come and talk about his web publishing might have as much of an effect on expression as any law on the books or technical blocking system.

Whether through advanced information technology, legal mechanisms, or soft controls, a growing number of states around the world are seeking to control the global flow of information. Ordinarily, this control takes the form of blocking, through technical means, state's citizens from accessing certain information online. In other instances, the blocking stops the state's citizens from publishing information online, in effect disallowing people outside the state from hearing the voices of the state's citizens. As a result, most filtering regimes cause a chilling effect on the use of information technologies as a means of free expression, whether for political, religious, or cultural purposes.

## From "How to Police Speech Online" to "How to Limit Speech Restrictions Online"

It is commonplace to argue that states have generally regulated the Internet lightly, but it is increasingly untrue. The author of a chapter in an important recent book wrote, "governments exercise relatively little control over the Internet, even though it has a tremendous impact on society."[30] This statement misleads readers into thinking that the Internet might somehow be a freer, more open environment than traditional spaces are. Such a statement might have been true in the United States fifteen years ago. But as of today, it is inaccurate. From a global perspective, both the importance of digitally-mediated communications and the extent of regulation of speech continue to grow over time.

The policing of speech in a borderless world brings with it a series of problems that merit public discussion. The types of controls that take place at a local

---

30 Harold Kwalwasser, Internet Governance, *in* CYBERPOWER AND NATIONAL SECURITY, 491 (Franklin D. Kramer et al., eds., Nat'l Defense Univ. Press 2009).

level, about bullying or hate speech or any other issue that may arise, can be vetted in a public meeting of a school district or in a state legislature. The online speech issues that are consistently on federal agendas in the United States—intellectual property restrictions, child safety, network neutrality, defamation, and so forth—tend to play out in public forums like the legislatures or in the court system. Of course, there are instances where the debate about speech controls occurs behind closed doors at the local and national levels as well. Corporate-level filtering, which can affect millions of employees, is one example where the issues are rarely vetted in a meaningful way. But the place where the debate is most consistently and conspicuously absent is on the international stage. It ought to merit meaningful consideration in the Internet governance debate.

The practice of state-mandated Internet filtering, and related regulations like surveillance, is now a widely-known fact, but the hard problems that stem from this practice are infrequently discussed as a matter of public policy outside of human rights and academic circles and the occasional national-level hearing. The blocking and surveillance of citizens' activity on the Internet—by virtue of the network's architecture, an issue of international dimensions—calls for discussion at a multilateral level. Rather than fretting over the finer points of the domain name system, time would be better spent in Internet governance discussions on issues like transparency in Internet filtering or broad issues of interconnection of the global network. The Internet filtering problem offers much more to be gained—through frank discussion, if not action—and provides an exercise worthy of an extraordinary gathering of world leaders who want to talk about the global "Information Society."

On one level, Internet filtering is a private matter between a state and its citizens as to what information citizens may access online.[31] States that censor the Internet assert the right to sovereignty. From the state's perspective, the public interest, as defined in one state, such as Saudi Arabia, is different from the public interest as defined by the state in Uzbekistan, China, or the United Kingdom. States can and do exercise their sovereignty through control of the information environment.

But even if one accepts the state sovereignty argument, that viewpoint should not end the conversation about Internet filtering. The state-based censorship

---

[31] Some states make an effort to suggest that their citizens (in Saudi Arabia and the United Arab Emirates specifically) are largely in support of the filtering regime, particularly when it comes to blocking access to pornographic material. For instance, the agency responsible for both internet access and filtering in Saudi Arabia conducted a user study in 1999, and reported that 45% of respondents thought "too much" was blocked, 41% thought it "reasonable," and 14% found it "not enough." These studies stand for the proposition, in the context of our report, that some states that filter seek to make the case that their filtering regime enjoys popular support, not that such support necessarily exists.

and surveillance practices of any state affect the citizens and businesses of other states in the context of the interconnected global communications network. Increasingly, the censorship and surveillance practices of states reach past the web-browsing habits of their own citizens. High-profile debates between Canadian company Research in Motion, maker of BlackBerry smartphones, and the United Arab Emirates and Saudi Arabia about the ability of the state to intercept BlackBerry communications make this point clear.[32] The Internet blocking that takes place in one state can also affect the network at a technical level in other jurisdictions, as Pakistan found out when it brought down YouTube globally for two hours in early 2009.[33]

A global discussion about the relationship between these filtering and surveillance practices and human rights is necessary and could be extremely fruitful. Specifically, states might consider rules that relate to common standards for transparency in Internet filtering and surveillance practices as they relate to individuals and those corporations drawn into the process. On a broader level, the issue raised here is about interconnection between states and the citizens of those states—and ultimately about what sort of an Internet we want to be building and whether the global flow of information is a sustainable vision.

For instance, we have yet to join the ethical interests at play in filtering. States vary greatly in terms of how explicitly the filtering regime is discussed and the amount that citizens can come to know about it. No state OpenNet Initiative studied makes its block list generally available.[34] The world leaders who gather

---

32 *See* Adam Shreck, *UAE BlackBerry Crackdown Affects Visitors Too*, ASSOCIATED PRESS, August 3, 2010, **www.google.com/hostednews/ap/article/ALeqM5iJ1MLhAMIeRDhT4heu4LKw-xgH3QD9HBKDJO0**. *See also Anthony DiPaola & Vivian Salama*, *UAE to Suspend BlackBerry Service Citing Security*, BLOOMBERG, August 1, 2010, **www.businessweek.com/news/2010-08-01/u-a-e-to-suspend-blackberry-services-citing-security.html**.

33 *See* Declan McCullagh, *How Pakistan Knocked YouTube Offline (and how to make sure it never happens again)*," CNET, February 25, 2008, **news.cnet.com/8301-10784_3-9878655-7.html**.

34 Saudi Arabia publishes its rationale and its blocking practices on an easily accessible website, at **www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm** ("The Internet Services Unit oversees and implements the filtration of web pages in order to block those pages of an offensive or harmful nature to the society, and which violate the tenants of the Islamic religion or societal norms. This service is offered in fulfillment of the directions of the government of Saudi Arabia and under the direction of the Permanent Security Committee chaired by the Ministry of the Interior."). In Saudi Arabia, citizens may suggest sites for blocking or for unblocking, in either Arabic or English, via a public website. Most sites include a block-page, indicating to those seeking to access a website that they have reached a disallowed site. Most states have enacted laws that support the filtering regime and provide citizens with some context for why and how it is occurring, though rarely with any degree of precision. As among the states we have studied, China is one of the states that obscures the nature and extent of its filtering regime to the greatest extent through a long-running series of conflicting public statements about its practices in this respect.

periodically at United Nations-sponsored meetings and at the Internet Governance Forums could make the most of their leadership by seeking to establish a set of best practices related to Internet filtering and the transparency related to filtering regimes. They might also focus profitably on the difficult problems facing those multinational companies that do business in regimes that require filtering and surveillance of the network in ways that would not be legally permissible in the company's home jurisdiction, as the Global Network Initiative has in its private capacity.[35] The issue of speech regulation in a borderless world is too important to leave only to those handful of companies, right-minded though they may be, which are seeking to do the right thing in a geopolitically complex regulatory environment.

The critical question in the next digital decade is not whether speech can be policed in a borderless world, but whether we should set new limits on the extent and manner in which it is policed today. We should ask, too, whether it is today easier, in fact, than in the past to police speech in a digitally-mediated world, and what the ramifications are for civil liberties if so. The Internet is becoming larger and more fractured each day. We should not pretend the Internet is a "lightly regulated" medium as though the calendar on our kitchen wall reads "1985" at the top. Trends that support more speech from more people in more places around the globe—using mobile applications generally, such as blogs, wikis, Twitter, SMS, and so forth—are countered by the increasing sophistication and reach of Internet filtering and surveillance practices. A richer understanding of the complexities at play in Internet filtering and other speech restrictions would help develop a foundation that does not yet exist for building a sustainable, and truly global, network that will continue to bring with it the innovation, jobs, services, and other social benefits that it promises.

---

35 *See* **www.globalnetworkinitiative.org**.

# The Role of the Internet Community in Combating Hate Speech

By Christopher Wolf*

In less than twenty years, the Internet has evolved to become an unprecedented tool for information, communication, entertainment and commerce. Much of the progress was made possible by the protections of the First Amendment and the absence of legal constraints. But there is a growing dark side to the Internet, which raises the question of how to police harmful content. Online child predators are a well-known blight, a frequent focus of headlines and television news. Cyber-bullying also has received significant attention recently, especially in the wake of teen suicides.

Less reported but equally troubling is the fact that the Internet has become a technology embraced by racists, anti-Semites, homophobes and bigots of all kinds to spread their messages of hate. The online haters use all of the tools of the Internet, from static websites, to streaming audio and video, to social networking sites like Facebook.

No longer relegated to meeting in dark alleys and the basements of abandoned buildings, or to mailing their propaganda in plain brown wrappers, hate groups have a platform to reach millions around the world. They seek to victimize minorities, to embolden and mobilize like-minded haters, and to recruit followers. And in their wake, an online culture has developed—aided by the mask of anonymity—in which people who would never consider themselves members of hate groups employ racial, religious and other epithets as part of their vocabulary in posting comments to news stories on mainstream sites and in other aspects of online life. In turn, the common appearance of such epithets desensitizes readers, making hate speech and the denigration of minorities "normal."

---

* Christopher Wolf is a partner in the law firm Hogan Lovells LLP where he leads the Privacy and Information Management practice. He founded and chairs the Internet Task Force of the Anti-Defamation League, and is Past Chair of the International Network Against Cyber-Hate (INACH).

One recent example of how haters are using the Internet occurred on the Fourth of July in 2010. As Americans were celebrating that event, a new "Event" was announced on Facebook, entitled "Kill a Jew Day."[1] The Facebook "host" for the Event wrote, "You know the drill guys," and he urged followers to engage in violence "anywhere you see a Jew" between July 4 and July 22. A Nazi swastika adorned the Event page.

The posting of that sickening Event prompted a wave of anti-Semitic rants on Facebook in support of the targeting of Jewish people. But it also prompted a counter-event on Facebook entitled "One Million Strong Against Kill a Jew Day" (whose supporters actually numbered, more modestly, in the thousands).[2] And, pursuant to the Facebook Terms of Service, complaints about the "Kill a Jew Day" event to Facebook administrators resulted in the company disabling the Event page.

The outrage over the Facebook Event site was justified, not just because of the vile anti-Semitism underneath it or the glorified display of a swastika. People also objected to the site because they know that Internet messages can and do inspire violence. Online anti-Semitic hate speech has been implicated in real-world acts of violence, such as an attack on Nobel Laureate and Holocaust survivor Elie Wiesel by a Holocaust denier in 2007,[3] and the 2009 murder of a guard at the Holocaust Memorial Museum in Washington, D.C., by a white supremacist who maintained his own online hate site and who was egged-on by fellow haters.[4] Words have consequences, and indeed inspire acts of hate and violence.

This recent example of online hate provides another opportunity to examine what society's response to online hate speech should be. What

---

1 *See* Yaakov Lappin, *"Kill a Jew" Page on Facebook Sparks Furor*, THE JERUSALEM POST, July 5, 2010, **http://www.jpost.com/JewishWorld/JewishNews/Article.aspx?id=180456**.

2 *See* Amada Schwartz, *Anti-Semitism v. Facebook*, JEWISH JOURNAL, July 13, 2010, **http://www.jewishjournal.com/community/article/anti-semitism_vs_facebook_20100713/**.

3 Suzanne Herel, *Holocaust Survivor, Nobel Peace Prize Winner Elie Wiesel Attacked in S.F. Hotel*, S.F. CHRONICLE, Feb. 9, 2007, **http://www.sfgate.com/cgi-bin/blogs/nwzchik/detail?blogid=32&entry_id=13385**.

4 Michael E. Ruane, Paul Duggan & Clarence Williams, *At a Moment of Sorrow, A Burst of Deadly Violence*, THE WASHINGTON POST, June 11, 2009, **http://www.washingtonpost.com/wp-dyn/content/article/2009/06/10/AR2009061001768.html**.

is the best way to police sites like the "Kill a Jew Day" Event page on Facebook, and the thousands of hate-filled videos uploaded to YouTube, and the white supremacist websites designed to recruit young people, glorifying violence against minorities?

One visceral response to the proliferation of online hate is: "There ought to be a law." Legal rules are the way a society decrees what is right and what is wrong, and since hate speech is wrong, it seems logical that the law would be employed to police it. A legal ban on hate speech and the criminalization of its publication is indeed an alternative in some jurisdictions. But, of course, it is not an option in the United States where the First Amendment gives broad latitude to virtually all speech, even the most repugnant. (Only direct threats against identifiable targets are criminalized.)

Legislatures around the world have heeded the call for laws encompassing Internet hate speech. The hate speech protocol to the Cybercrime Treaty is a prime example of a heralded legal solution to the problem.[5] It was designed to eliminate racist sites from the Internet through criminal penalties.

From Brazil to Canada, and from South Africa to Great Britain, there are legal restrictions on hate speech, online and offline. In much of Europe, denial of the Holocaust (online or offline) is forbidden. In Germany, even displaying the swastika is a crime. The enforcement of laws against Holocaust deniers—given the bitterly sad history of those countries—serves as a message to all citizens (especially impressionable children) that it is literally unspeakable to deny the Holocaust given the horrors of genocide inflicted in those countries.

Still, there are many who believe that prosecutions, such as that of Holocaust denier David Irving in Austria,[6] promoted his visibility and stirred up his benighted supporters, rather than quelling future hate speech and enlightening the public.

Moreover, laws against hate speech have not demonstrably reduced hate speech or deterred haters. The hate speech protocol to the Cybercrime

---

5 The Convention on Cybercrime Nov. 23, 2001, Europ. T.S. No. 185, **http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm**.

6 *See Austria Holds "Holocaust Denier,"* BBC NEWS, Nov. 17, 2005, **http://news.bbc.co.uk/2/hi/europe/4446646.stm**.

Treaty, for example, has not reduced online hate. The shield of Internet anonymity and the viral nature of online hate make legal policing an unrealistic challenge, except in cases where authorities want to "set an example." And since the U.S., with its First Amendment is essentially a safe-haven for virtually all web content, shutting down a website in Europe or Canada through legal channels is far from a guarantee that the contents have been censored for all time. The borderless nature of the Internet means that, like chasing cockroaches, squashing one does not solve the problem when there are many more waiting behind the walls—or across the border.

Many see prosecution of Internet speech in one country as a futile gesture when the speech can re-appear on the Internet almost instantaneously, hosted by an Internet service provider (ISP) or social networking site in the United States. Moreover, in the social networking era, the ability of people to upload far outpaces the ability of the police to track and pursue offending speech.

Like the prosecution in Austria of David Irving, the prosecutions in Germany of notorious Holocaust deniers and hate site publishers Ernst Zundel[7] and Frederick Töben[8] sent messages of deterrence to people that make it their life's work to spread hate around the world that they may well go to jail as well. And, again, such prosecutions expressed society's outrage at the messages. But all one need do is insert the names of those criminals in a search engine, and you will find websites of supporters paying homage to them as martyrs and republishing their messages.

Even some free speech advocates around the world applaud the use of the law to censor speech when it is *hate* speech because of the pernicious effects of hate speech on minorities and children, and because of its potential to incite violence. But many of those same people object to the use of the law by repressive regimes like China to censor speech it deems to be objectionable as hate directed towards the Chinese government. It is not easy to draw the line between good and bad state use of censorship because defining what is hate speech can be quite subjective. Giving the state the power to censor is problematic, especially given the potential for abuse.

---

7 *See Zundel Gets Five Years from German Count*, WINNIPEG FREE PRESS, Feb. 16, 2007, **http://www.winnipegfreepress.com/historic/32115694.html**.

8 *See* Steve Kettmann, *German Hate Law: No Denying It*, WIRED, Dec. 15, 2000, **http://www.wired.com/politics/law/news/2000/12/40669#ixzz0jTf5lnLh**.

This is not to say that law has no role to play in fighting online hate speech—far from it. But countries with speech codes intended to protect minorities should make sure that the proper discretion is employed to use those laws against Internet hate speech, lest the enforcement be seen as ineffectual and result in a diminished respect for the law. And, again, the realities of the Internet are such that shutting down a website through legal means in one country is far from a guarantee that the website is shuttered for all time.

Thus, the law is but one, albeit limited, tool in the fight against online hate.

Counter-speech—exposing hate speech for its deceitful and false content, setting the record straight, and promoting the values of tolerance and diversity, has an important role to play in the policing of online hate speech. That is the thrust of the First Amendment. To paraphrase U.S. Supreme Court Justice Brandeis, sunlight is still the best disinfectant—it is always better to expose hate to the light of day than to let it fester in the darkness. One answer to hate speech is more speech. The Facebook event "One Million Strong Against Kill a Jew Day," even if far short of a million members, is a vivid example of the power of counter-speech as a vehicle for society to stand up against hate speech. And, of course, education from an early age on Internet civility and tolerance would go far to stem the next generation of online haters.

An equally important and powerful tool against hate speech is the voluntary cooperation of the Internet community, including Internet Service Providers, social networking companies and others. When Facebook enforced its Terms of Service (which requires users not to "post content that: is hateful, threatening, or … incites violence…"[9]) and disabled the "Kill Jew Day" event site,[10] that was a powerful example of an Internet company exercising its own First Amendment rights to ensure that it remained an online service with standards of decency. That voluntary act was quick and effective. A legal action against Facebook for hosting the site—impossible in the U.S. but viable elsewhere around the world—would have been expensive, time-consuming and no more

---

9 Statement of Rights and Responsibilities, Facebook, **http://www.facebook.com/terms.php**.

10 Lappin, *supra* note 1.

effective. The chilling effect of a legal action against Facebook may have resulted in undue restrictions by Facebook on future user postings.

Voluntary enforcement by Internet companies of self-established standards against hate speech is effective. If more Internet companies in the U.S. block content that violate their Terms of Service, it will at least be more difficult for haters to gain access through respectable hosts. The challenge, of course, is with social media sites where postings occur constantly and rapidly. Social media companies normally wait for a user complaint before they investigate hate speech posted on their service, but the proliferation of hate-filled postings outpaces the effectiveness of such a "notice and take down" arrangement. New monitoring techniques to identify hate speech as it is posted may be in order.

In the era of search engines as the primary portals for Internet users,[11] cooperation from the Googles of the world is an increasingly important goal. The example of the Anti-Defamation League[12] and Google with the site "Jew Watch" is a good one.[13] The high ranking of Jew Watch in response to a search inquiry was not due to a conscious choice by Google, but was solely a result of an automated system of ranking. Google placed text on its site that explained the ranking, and gave users a clear explanation of how search results are obtained, to refute the impression that Jew Watch was a reliable source of information, and linked to the ADL site for counter-speech.[14]

In short, vigilance and voluntary standards are more effective than the law in dealing with the increasing scourge of online hate speech. Hate speech can be "policed" in a borderless world, but not principally by the traditional police of law enforcement. The Internet community must continue to serve as a "neighborhood watch" against hate speech online,

---

11 A study by Nielsen found that 37 percent of respondents used search engines when looking for information, as compared to 34 percent using portals and only 18 percent using social media. *See* Jon Gibs, *Social Media: The Next Great Gateway for Content Discovery?*, NIELSEN, Oct. 5, 2009, **http://blog.nielsen.com/nielsenwire/online_mobile/social-media-the-next-great-gateway-for-content-discovery/**.

12 The Anti-Defamation League was founded to combat anti-Semitism. For more information, see **http://www.adl.org/**.

13 *See Google Responds to Jew Watch Controversy*, WEBPRONEWS, April 15, 2004, **http://www.webpronews.com/topnews/2004/04/15/google-responds-to-jew-watch-controversy**.

14 Google, *An Explanation of Our Search Results*, **http://www.google.com/explanation.html**.

"saying something when it sees something," and working with online providers to enforce community standards.

# CHAPTER 10

## WILL THE NET LIBERATE THE WORLD?

# Can the Internet Liberate the World?

By Evgeny Morozov*

It may be useful to start by laying out the basics. Anyone pondering the question posed in the title of this essay most likely assumes that there exists some powerful forces of oppression from which the world could and should be liberated. A list of such problems is as infinite as it is intuitive: From poverty to racism and from pollution to obesity, "oppressive forces" seem to be all around us.

Yet, for some reason, these are rarely the kind of problems that one wants to fight with the help of technology, let alone the Internet. It's in solving political rather than socio-economic problems that the Internet is presumed to hold the greatest promise. Most specifically, it is its ability to undermine repressive governments that is widely discussed and admired, even more so as Internet companies like Google find themselves struggling with the likes of the Chinese government.

Two features of the Internet are often praised in particular: 1) its ability to quickly disseminate any kind of information—including the information that authoritarian governments may not like—and 2) its ability to allow like-minded individuals to find each other, to mobilize supporters and to collectively pursue future goals—including democratization. The hype surrounding Iran's Twitter Revolution of 2009 was probably the strongest public manifestation of high hopes for the transformative potential of the Internet; only a rare pundit did not predict the eventual collapse of the Iranian regime under the barrage of angry tweets from its citizens.

Still, such praise is not without merit. Even the hardest skeptics would grant these two features to the Internet; to deny that it does enhance the citizens' ability to inform (and get informed) and to mobilize—what the Internet theorist Clay Shirky calls "ridiculously easy group forming"[1]—would be to deny the obvious. The skeptics would also have no trouble acknowledging that both of these features are constantly under threat, as governments keep implementing new systems of censorship and control.

---

* Evgeny Morozov is the author of THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM (Public Affairs, 2011). He's also a visiting scholar at Stanford University, a fellow at the New America Foundation and a contributing editor to Foreign Policy magazine.

1 CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS 54 (Penguin Press 2008), quoting social scientist Sébastien Paquet.

Nor does anyone really contest the fact that the Internet has proved quite resilient against such attacks, giving rise to numerous tools to circumvent government censorship. For many, the fact that an institution as powerful as the U.S. government has trouble reining in a fluid and mostly virtual organization like WikiLeaks is a testament to the power of the Internet, even though the morality of WikiLeaks' actions (in publishing leaked information about the U.S. military occupation of Afghanistan) is still widely disputed.

However, conceding that the Internet helps to disseminate information and mobilize campaigners around certain causes is not quite the same as conceding that authoritarian regimes are doomed or that democracy is inevitable. There may be good independent reasons to campaign for greater freedom of expression on the Internet—but one shouldn't presume that such freedoms would necessarily translate into democratization.

For the Net—and its two powerful features discussed above—to be able to "liberate the world" from authoritarianism, one needs to make a few further assumptions. First, one needs to assume that modern authoritarian regimes derive their power primarily by suppressing the activities that the Internet helps to amplify: *i.e.*, dissemination of information and popular mobilization around specific causes. Second, one also needs to assume that the Internet won't have any other political and social effects that may—if only indirectly—create new modes of "oppression," entrenching authoritarianism as a result. In other words, the Internet can only deliver on its liberating promise as long as the things it offers are also the things that the fight against authoritarianism requires—and as long as it doesn't produce any other regime-strengthening effects that may inadvertently undermine that fight.

On initial examination, the first assumption seems to hold. There is no shortage of suppression of both information and mobilization opportunities in modern authoritarian states. Their rulers have not lost the desire to guard their secrets or regulate how their citizens participate in public life. The fact that some forms of censorship persist even in democratic societies suggests that governments do not really aspire to lift all the digital gates and let information flow freely. The urge, then, is to find ways to break through those gates—and the Internet seems to excel at the job. If there is one thing that techies and hackers know how to do well, it's to build tools to pierce firewalls.

But suppose that such tools can be found and can even achieve the kind of scale where all Internet users in China or Iran have access to them. What would the effect be on their populations and their governments? I'd like to propose that one's answer to this question depends mostly on one's views about the sources of legitimacy of modern authoritarianism.

Those who believe that such legitimacy is derived primarily through the brainwashing of their citizens are justifiably very excited about the Internet.

Moreover, they are usually very quick to predict the inevitable fall of authoritarian governments. After all, their theoretical conception of authoritarianism posits that once the information gates are open, brainwashing loses much of its effectiveness; people realize they have been lied to all along—and they rebel as a result.

At first sight, the contemporary global situation may seem to vindicate such views. Many modern authoritarian governments—and here cases like Belarus, China, Russia come to mind—enjoy strong levels of support from vast swathes of their populations. One may quibble about the ways by which the Kremlin has solidified its power in the last decade—many of those ways are far from democratic—but virtually all opinion polls reveal that the Kremlin's policies are genuinely popular. Ditto China, where the government is one of the most trusted institutions in the country, enjoying a level of trust that the U.S. Congress could only dream of.

Is it all because of brainwashing? If the answer is "yes," then there are, indeed, good reasons to be optimistic about the power of the Internet. The moment the authoritarian governments' monopoly over information disappears, any manipulations of truth that were possible in an age of information scarcity would be impossible.

This, I'd like to propose, may be a very simplistic reading of the situation—and a reading that is also extremely insensitive to historical and social forces. There is much more to the legitimacy of modern authoritarian states than just their skillful manipulation of information. Many authoritarian regimes—Belarus, China and Russia are again excellent examples but one could also add Azerbaijan, Kazakhstan, and Vietnam to the list—have made genuine advances in economic development, many of them thanks to their embrace of technology in general and the Internet in particular. Furthermore, in many of these countries, the once extremely contentious political life has stabilized as well, allowing their populations to enjoy a rare period of peace and prosperity—even it came at the hefty price of having their governments tighten the valves on freedom of expression or freedom of assembly.

It seems disingenuous to argue that modern Russians or Chinese do not appreciate the fact that today they purchase considerably more commodities—including luxurious ones—than they could 20 years ago; or that they can travel the world much more freely; or that they—at least online—can consume any kind of entertainment they want, regardless of its origins. Placed in the historical context and compared against other possible scenarios of where these two countries may have been had their rulers not embarked on a series of reforms, such achievements look even more impressive.

Should it turn out that large segments of the populations of authoritarian states are well aware of the kind of human rights violations that are needed in order to

sustain the impressive rates of economic progress—or, even more shockingly, that they are actually supportive of such violations—a strategy of "un-brainwashing" simply would not work. If modern authoritarianism is as much a product of a social contract as modern democracy is, then changing the attitudes of those who have long given up the fight for freedom would take much more than just exposing them to facts.

The big question that Western do-gooders should be asking themselves here is not whether the Internet can liberate the world but whether the world actually *wants* to be liberated. Above all, this is a question of whether capitalism unburdened by democratic norms and ideals is sustainable in the long term—a possibility that goes directly against the theory that the logic of capitalism inevitably leads to democracy, a view that was extremely popular in the early 1990s.[2]

If capitalism can get by without democracy, the ability to spread subversive information that might reveal the horrors of the regime looks considerably less impressive, for the populations that the West seeks to liberate are already well-aware of what's going on and many of them may have simply chosen to look the other way in expectation of a better life for their children.

Granted, it's not just facts that may help change their attitudes. One may use the Net to distribute subversive poetry and fiction that would reawaken (or, in most cases, create from scratch), the political consciousness of those living under authoritarianism. Technology would certainly be of great help here, both in terms of helping to distribute such materials but also in terms of protecting those who access them. But the ability of such materials to incite people to democratic change is not just a function of how many people read them; rather, it's a function of how well-argued such materials are.

It seems that even if the West succeeded in distributing *1984*, *Darkness at Noon*, or *Brave New World* to every single citizen of an authoritarian state, this might not lead to a revolution, simply because those books offer a poor critique of the actually existing modern-day authoritarianism, which has come to terms with both Western popular culture and globalization.

---

2 *See, e.g.*, Commission on Security & Cooperation in Europe (U.S. Helsinki Commission), Briefing on *Twitter Against Tyrants: New Media In Authoritarian Regimes*, Oct. 22, 2009, available at **http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewDetail&ContentRecord_id=462&Region_id=0&Issue_id=0&ContentType=H,B&ContentRecordType=B&CFID=32177263&CFTOKEN=96274551**; Nicholas Kristof, *Tear Down This Cyberwall!*, N.Y. TIMES, June 17, 2009, *available at* **http://www.nytimes.com/2009/06/18/opinion/18kristof.html?_r=1**; L. Gordon Crovitz, *Mrs. Clinton, Tear Down this Cyberwall*, WALL ST. JOURNAL, May 3, 2010, available at **http://online.wsj.com/article/SB10001424052748704608104575219022492475364.html**; FRANCIS FUKUYAMA, THE END OF HISTORY AND THE LAST MAN (1992).

If support for modern authoritarianism is not the product of ignorance and brainwashing but rather of a rational calculation that, under the present conditions, authoritarianism is the best way to generate and preserve economic growth, the Internet's ability to disseminate and mobilize, while very impressive in itself, may not deliver the kind of benefits that so many in the West expect. To put it simply, citizens of authoritarian states may not be *uninformed*—so getting them *informed* is going to be of only limited value. As such, the Net's ability to liberate the world is severely constrained by the absence of a strong intellectual vision for how a liberated Russia or China would look (and work) like.

Now, if the Soviet experience is anything to judge by, revolutions don't need the absolute majority of the population to be successful. In other words, it may be possible that a small group of politically active citizens could take advantage of political openings at the right moment and push for significant reform—or the overthrow of a government altogether. In situations like this, the Internet's ability to mobilize may indeed come very handy.

Several caveats are in order here. First, obviously, this doesn't mean that the Internet can help create such political openings—those are usually created by structural factors. As much as it is tempting to believe that it was fax machines and photocopiers that brought down communism in Eastern European countries, one would probably be better off studying their dismal economic record in the late 1980s. So far, it seems that the information revolution—which many have taken to mean the end of authoritarianism everywhere—has, overall, had a positive impact on the rates of economic growth in modern authoritarian regimes—and, to this extent, that revolution may actually have *strengthened* these regimes.

The second caveat is that there is little certainty that the group with the best ability to mobilize will also be the group with the most impressive democratic agenda. Once again, the Soviet example—with a tiny group of Bolsheviks gaining control of a country as massive as Russia—is quite instructive. Not all revolutions are democratic in character, and more than one of them ended up with the least democratic groups gaining power. Al-Qaeda is far better at using technology to mobilize the masses than the liberal voices of the Middle East; the Russian nationalists, likewise, are far more creative online than the democratic and pro-Western opposition.

Third—and, perhaps, most important—what happens in between political openings matters a great deal as well. It's simply not true that, from the perspective of an authoritarian state, all social mobilization is harmful. Take the case of China. Thanks to the extremely vibrant nationalist sector of the country's blogosphere, the Chinese government is often pushed to adopt a much more aggressive posture—towards Taiwan, Japan, South Korea—than

they might otherwise have done. Such hawkishness in their foreign policy may or may not bolster their legitimacy; the short answer is that we have to look at the context. For our purposes, it seems clear that we won't be able to understand the role of the Internet—even if one concedes that it is, indeed, conducive to more mobilization and contestation—if we study that role outside of the socio-political environment in which it is embedded. The assumption that "greater opportunities for social mobilization equals greater odds that democracy will prevail in the long run" simply is not true.

This last point highlights the problem with the second grand assumption that we still need to examine—namely, that the Net won't have any other primary or secondary effects on the quality and sustainability of authoritarianism. The account that prioritizes the role of information dissemination and mobilization usually rests on a very simplistic, even reductionist, theory of authoritarianism. It presumes the existence of an authoritarian chimera—the government—which controls its citizens through a combination of surveillance and coercion. Citizens, the theory goes, would take immediate advantage of the Internet and use it to push against the government.

But why wouldn't the government do the same to push against the citizens? In order to understand the overall impact of the Net on the "struggle for liberation," one must study how it may have also facilitated government monitoring and control of what their citizens do. Even the most optimistic observers of the Net would concede that social networking, fun as it is, may not necessarily be the best way to protect one's data—both because no social networking site is secure from occasional data leaks and because secret police around the world have now, inadvertently, obtained the ability to map the connections between different activists, see how they are related to foreign funders, and so on.

Furthermore, there is a vibrant and rapidly-expanding global market in activities like face recognition, which makes the identification of those who participate in anti-government protests much easier—often this actually happens by comparing party photos they themselves upload to social networking sites with the photos taken at the protest rallies. Seasoned activists may, of course, be smart enough to steer away from social networking sites, but this hardly applies to the rest of the population.

But conceding that it's not just anti-government activists who have been empowered by the Net is only part of the story. The truth is that we simply can't easily classify all social forces into "pro-" and "anti-government" simply based on the location of their offices (*e.g.*, the secret police are in; the unions are out). In reality, modern authoritarian regimes derive their power from a much more diverse pool of resources than sheer brute force or surveillance. To understand what makes modern authoritarian regimes tick, one thus needs to

look at a whole range of other political, social, and cultural factors: religion, history, nationalism, geography (*e.g.*, the relations between the federal center and the periphery), rates of economic growth, corruption, government efficiency, fear of a foreign invasion and so forth. Many of these factors have successfully been co-opted by modern authoritarian rulers to justify and prolong their rule.

It's easy to imagine an authoritarian regime that would become stronger as a result of (a) an increase in religious sentiment among its population, (b) the promotion of a particular interpretation of recent history that would justify the current political regime as inevitable and an unambiguous improvement over its predecessors, and (c) impressive rates of economic growth, with little corruption or government bureaucracy. Likewise, it's easy to imagine how all of these developments would be amplified if (d) the Internet ends up providing more access to more religious materials to more believers (*e.g.*, through mobile phones), (e) governments find a way to hire and compensate loyal bloggers for touting a particular reading of history, and (f) governments set up websites that allow citizens to report on corrupt officials, problems with existing infrastructure, or government waste.

That last development may seem like a good thing—until one realizes that an authoritarian government with less government waste is not necessarily a weaker authoritarian government. It may actually be more effective and the country may enjoy faster rates of economic growth—but that, alas, still does not always translate into a more democratic government.

All of this is to say that the only way to understand how the Internet influences authoritarianism is to first define a theory of authoritarianism itself—preferably, a theory that goes beyond Manichean theories of "the totalitarian state" versus "the dissidents"—and then use it to closely investigate how the Internet affects each of its components.

As such, our ability to harvest the potential of the Net to "liberate the world" depends not so much on our ability to understand the Net but on our ability to understand the world itself. It's much easier to understand how the Internet affects government efficiency than to understand how government efficiency affects government legitimacy under conditions of capitalism-friendly authoritarianism.

Political scientists, unfortunately, don't have much to boast of on this front: their understanding of this completely new breed of authoritarianism is at best rudimentary—and their understanding of how such a fluid and complex technology as the Internet can affect it is even worse. Given the immense poverty of our current conceptual apparatus, even if the Net does end up liberating the world, most likely we won't know it for quite some time.

# Internet Freedom: Beyond Circumvention

By Ethan Zuckerman*

U.S. Secretary of State Hillary Clinton's January 2010 speech on Internet Freedom signaled a strong interest from the State Department in encouraging the use of the Internet to promote political reforms in closed societies.[1] It makes sense that the State Department would look to support existing projects to circumvent Internet censorship. *The New York Times* reports that a group of senators subsequently urged the Secretary to apply existing funding to support the development and expansion of censorship circumvention programs.[2]

My colleagues Hal Roberts, John Palfrey and I have studied the development of Internet circumvention systems over the past five years, and released a study last year that compared the strengths and weaknesses of different circumvention tools.[3] Some of my work at The Berkman Center for Internet & Society at Harvard University is funded by a U.S. State Department grant that focuses on the continuing study and evaluation of these sorts of tools. As a result, I spend a lot of time coordinating efforts between tool developers and people who need access to circumvention tools to publish sensitive content.

I strongly believe that we need strong, anonymized and useable censorship circumvention tools. But I also believe that we need lots more than censorship circumvention tools, and I fear that both funders and technologists may over-focus on this one particular aspect of Internet freedom at the expense of other avenues. I wonder whether we're looking closely enough at the fundamental limitations of circumvention as a strategy and asking ourselves what we're hoping Internet freedom will do for users in closed societies.

---

* Senior Researcher at the Berkman Center for Internet and Society at Harvard University. Thanks to Hal Roberts, Janet Haven and Rebecca MacKinnon for help editing and improving this essay. They're responsible for the good parts. You can blame the rest on me.

1 Hillary Rodham Clinton, Secretary of State, Remarks on Internet Freedom at the Newseum (Jan. 21, 2010), **http://www.state.gov/secretary/rm/2010/01/135519.htm**.

2 Brad Stone, *Aid Urged for Groups Fighting Internet Censors*, N.Y. TIMES, Jan. 20, 2010, **http://www.nytimes.com/2010/01/21/technology/21censor.html?_r=1**. For more information on Tor, see **http://www.torproject.org**. For more information on Psiphon, see **http://psiphon.ca**. For more information on Freegate, see **http://www.dit-inc.us/freegate**.

3 HAL ROBERTS, ETHAN ZUCKERMAN & JOHN PALFREY, 2007 CIRCUMVENTION LANDSCAPE REPORT: METHODS, USES, AND TOOLS (March 2009), **http://dash.harvard.edu/bitstream/handle/1/2794933/2007_Circumvention_Landscape.pdf?sequence=2**.

So here's a provocation: **We can't circumvent our way around Internet censorship.**

I don't mean that Internet censorship circumvention systems don't work. They do—our research tested several popular circumvention tools in censored nations and discovered that most can retrieve blocked content from behind the Chinese firewall or a similar system.[4] There are problems with privacy, data leakage, the rendering of certain types of content, and particularly with usability and performance, but the systems we tested can indeed circumvent censorship. What I mean is this: We couldn't afford to scale today's existing circumvention tools to "liberate" all of China's Internet users even if they all wanted to be liberated.

Circumvention systems share a basic mode of operation—they act as proxies to let users retrieve blocked content. A user is blocked from accessing a website by her Internet Service Provider (ISP) or that ISP's ISP. She may want to read a page from Human Rights Watch's (HRW) website, which is accessible at IP address 70.32.76.212. But that IP address is on a national blacklist, and she's prevented from receiving any content from it. So, she points her browser to a proxy server at another address—say, 123.45.67.89—and asks a program on that server to retrieve a page from the HRW website. Assuming that 123.45.67.89 isn't on the national blacklist, she should be able to receive the HRW page via the proxy.

During the transaction, the proxy is acting like an Internet service provider. Its ability to provide reliable service to its users is constrained by bandwidth—bandwidth to access the destination site and to deliver the content to the proxy user. Bandwidth is costly in aggregate, and it costs real money to run a proxy that's heavily used.

Some systems have tried to reduce these costs by asking volunteers to share them—the first release of Citizen Lab's Psiphon used home computers hosted by volunteers around the world as proxies, and then used their consumer bandwidth to access the public Internet. Unfortunately, in many countries, consumer Internet connections are optimized to download content and are much slower when they are uploading content. These proxies could access the Human Rights Watch website pretty quickly, but they took a very long time to deliver the page to the user behind the firewall. As a result, Psiphon is no longer primarily focused on trying to make proxies hosted by volunteers work. Tor, on the other hand, is, but Tor nodes are frequently hosted by universities and companies that have access to large pools of bandwidth. Still, available bandwidth is a major constraint of the Tor system. The most usable circumvention systems today—virtual private network (VPN) tools like

---

4 *See, generally*, ROBERTS, ZUCKERMAN & PALFREY, *supra* note 3.

Relakks[5] or WiTopia[6]—charge users between $3 and $6 per month to defray bandwidth costs.

Assume that systems like Tor, Psiphon and Freegate receive additional funding from the U.S. State Department. How much would it cost to provide proxy Internet access for … well, China? China reports 384 million Internet users,[7] meaning we're talking about running an ISP capable of serving more than 25 times as many users as the largest U.S. ISP.[8] According to the China Internet Network Information Center (CNNIC), China consumes 998,217 Mbps of international Internet bandwidth.[9] It's hard to get estimates for what ISPs pay for bandwidth, though conventional wisdom suggests prices between $0.05 and $0.10 per gigabyte. Using $0.05 as a cost per gigabyte, the cost to provide the uncensored Internet to China would be $13,608,000 per month, or $163.3 million a year in pure bandwidth charges, not including the costs of proxy servers, routers, system administrators and customer service. Faced with a bill of that magnitude, the $45 million U.S. senators are asking Secretary Clinton to spend quickly looks pretty paltry.[10]

There's an additional complication—we're not just talking about running an ISP—we're talking about running an ISP that's very likely to be abused by bad actors. Spammers, fraudsters and other Internet criminals use proxy servers to conduct their activities, both to protect their identities and to avoid systems on free webmail providers, for instance, which prevent users from signing up for dozens of accounts by limiting an IP address to a certain number of signups in a limited time period. For example, Wikipedia found that many users used open proxies to deface their system and now reserve the right to block proxy users from editing pages.[11] Proxy operators have a tough balancing act—for their proxies to be useful, people need to be able to use them to access sites like Wikipedia or YouTube, but if people use those proxies to abuse those sites, the proxy will be blocked. As such, proxy operators can find themselves at war with their own users, trying to ban bad actors to keep the tool useful for the rest of the users.

---

5 For more information on Relakks, see **http://www.relakks.com**.

6 For more information on WiTopia, see **http://www.witopia.net**.

7 Chris Buckley, *China Internet Population Hits 384 million*, REUTERS, Jan. 15, 2010, **http://www.reuters.com/article/idUSTOE60E06S20100115**.

8 *See Top 23 U.S. ISPs by Subscriber: Q3 2008*, ISP Planet, **http://www.isp-planet.com/research/rankings/usa.html**.

9 *See* China Internet Network Info. Ctr., *Internet Fundamental Data*, **http://www.cnnic.net.cn/en/index/0O/index.htm** (last visited July 29, 2010).

10 Brad Stone, *Aid Urged for Groups Fighting Internet Censors*, N.Y. TIMES, Jan. 20, 2010, **http://www.nytimes.com/2010/01/21/technology/21censor.html**.

11 *See Open Proxies*, WIKIPEDIA, **http://en.wikipedia.org/wiki/Wikipedia:Open_proxies**.

I'm skeptical that the U.S. State Department can or wants to build or fund a free ISP that can be used by millions of simultaneous users, many of whom may be using it to commit click fraud or send spam.[12] I know—because I've talked with many of them—that the people who fund blocking-resistant Internet proxies don't think of what they're doing in these terms. Instead, they assume that proxies are used by users only in special circumstances, to access blocked content.

Here's the problem: A government like China is blocking a lot of content. As Donnie Dong notes in a recent blog post, five of the ten most popular websites worldwide are blocked in China.[13] Those sites include YouTube and Facebook, sites that eat bandwidth through large downloads and long sessions. Perhaps it would be realistic to act as an ISP to China if we were just providing access to Human Rights Watch—but it's not realistic if we're providing access to YouTube, too.

Proxy operators have dealt with this question by putting constraints on the use of their tools. Some proxy operators block access to YouTube because it's such a bandwidth hog. Others block access to pornography, both because it uses bandwidth and to protect the sensibilities of their sponsors. Others constrain who can use their tools, limiting access to people coming from Iranian or Chinese IP addresses, trying to reduce bandwidth use by American high school kids whose schools have blocked YouTube. In deciding who or what to block, proxy operators are offering their personal answers to a complicated question: *What parts of the Internet are we trying to open up to people in closed societies?* As we'll address in a moment, that's not such an easy question to answer.

Imagine for a moment that we could afford to proxy China, Iran, Myanmar and others' international traffic. We figure out how to keep these proxies unblocked and accessible (it's not easy—the operators of heavily used proxy systems are engaged in a fast-moving cat and mouse game) and determine how to mitigate the abuse challenges presented by open proxies. We still have problems.

Most Internet traffic is domestic. In China, we estimate that, at minimum, 95% of total traffic is within the country. Domestic censorship matters a great deal, and perhaps a great deal more than censorship at national borders. As Rebecca

---

12 Matthew Broersma, *Researchers Eye Open Proxy Attacks*, TECHWORLD, Nov. 15, 2007, **http://news.techworld.com/security/10663/researchers-eye-open-proxy-attacks**.

13 Donnie Dong, *Google's Angry, Sacrifice and the Accelerated Splitting Internet*, BLAWGDOG, Jan. 13, 2010, **http://english.blawgdog.com/2010/01/googles-angry-sacrifice-and-accelerated.html**.

MacKinnon documented in *China's Censorship 2.0*,[14] Chinese companies censor user-generated content in a complex, decentralized way. As a result, a good deal of controversial material is never published in the first place, either because it's blocked from publication or because authors decline to publish it for fear of having their blog account locked or cancelled. We might assume that if Chinese users had unfettered access to Blogger, they'd publish there. Perhaps not—people use the tools that are easiest to use and that their friends use. A seasoned Chinese dissident might use Blogger, knowing she's likely to be censored—an average user, posting photos of his cat, would more likely use a domestic platform and not consider the possibility of censorship until he found himself posting controversial content.

In promoting Internet freedom, we need to consider strategies to overcome censorship inside closed societies. We also need to address "soft censorship": the co-opting of online public spaces by authoritarian regimes, which sponsor pro-government bloggers, seed sympathetic message board threads, and pay for sympathetic comments. Evgeny Morozov offers a thoroughly dark view of authoritarian use of social media in "How Dictators Watch Us on the Web."[15]

We also need to address a growing menace to online speech—attacks on sites that host controversial speech. When Turkey blocks YouTube[16] to prevent Turkish citizens from seeing videos that defame Ataturk, they prevent 20 million Turkish Internet users from seeing everything on YouTube. When someone—the Myanmar government, patriotic Burmese, mischievous hackers—mount a distributed denial of service attack on *The Irrawaddy*,[17] an online newspaper highly critical of the Myanmar government, this temporarily prevents everyone everywhere from seeing it.

Circumvention tools help Turks who want to see YouTube get around a government block, but they don't help Americans, Chinese or Burmese see *The Irrawaddy* if the site has been taken down by a Distributed Denial of Service (DDoS)[18] or hacking attack. Publishers of controversial online content have begun to realize that they're not just going to face censorship by national

---

14 Rebecca MacKinnon, *China's Censorship 2.0: How Companies Censor Bloggers*, 14 FIRST MONDAY (Feb. 2009), **http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089**.

15 Evgeny Morozov, *How Dictators Watch Us on the Web*, PROSPECT, Nov. 18, 2009, **http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web**.

16 Nico Hines, *YouTube Banned in Turkey After Video Insults*, THE TIMES, Mar. 7, 2007, **http://www.timesonline.co.uk/tol/news/world/europe/article1483840.ece**.

17 Aung Zaw, *The Burmese Regime's Cyber Offensive*, THE IRRAWADDY, Sept. 18, 2008, **http://www.irrawaddy.org/opinion_story.php?art_id=14280** .

18 A DDoS attack uses multiple computer systems to target and attack a single system, or website, thus preventing users from accessing the targeted system.

filtering systems—they're going to face a variety of technical and legal attacks that seek to make their servers inaccessible.

There's quite a bit publishers can do to increase the resilience of their sites to DDoS attack and to make their sites more difficult to filter. To avoid blockage in Turkey, YouTube could increase the number of IP addresses that lead to the web server and use a technique called "fast-flux DNS"[19] to give the Turkish government more IP addresses to block. They could maintain a mailing list to alert users to unblocked IP addresses where they could access YouTube, or create a custom application that disseminates unblocked IPs to YouTube users who download the application. These are all techniques employed by content sites that are frequently blocked in closed societies.

YouTube doesn't utilize these anti-blocking measures for two reasons. One, it has historically preferred to negotiate with nations who filter the Internet to make YouTube sites accessible again, rather than to work against these nations by fighting filtering. (This may be changing, now that Google has decided to disengage from China due to censorship and hacking issues.) Second, YouTube doesn't really have an economic incentive to be unblocked in Turkey. If anything, being blocked in Turkey, and perhaps even in China, may even be to its economic advantage, since serving these countries is likely to be unprofitable.

Sites that enable distribution of user-created content are supported by advertising traffic. Advertisers are generally more excited about reaching users in the U.S. who have credit cards, more disposable income and are inclined to buy online than users in China or Turkey. Some suspect that the introduction of "lite" versions of services like Facebook is designed to serve users in the developing world at lower cost, since those users rarely create income for the sites.[20] In economic terms, it may be hard to convince Facebook, YouTube and others to continue providing services to closed societies, where they have a tough time selling ads. We also may need to ask more of them to take steps to ensure that they remain accessible and useful in censorious countries.

In short:

- Internet circumvention is difficult and expensive. It can make it easier for people to send spam and steal identities.
- Circumventing censorship through proxies gives people access to international content, but doesn't address domestic censorship, which likely affects the majority of people's Internet behavior.

---

19 Fast-flux DNS prevents the identification of a host server's IP address.

20 Brad Stone & Miguel Helft, *In Developing Countries, Web Grows Without Profit*, N.Y. TIMES, April 26, 2009, **http://www.nytimes.com/2009/04/27/technology/start-ups/27global.html?_r=1**.

- Circumventing censorship doesn't offer a defense against DDoS or other attacks that target publishers.

To figure out how to promote Internet freedom, we need to start addressing the question: "How do we think the Internet changes closed societies?" In other words, do we have a "theory of change"[21] behind our desire to ensure people in Iran, Burma, China, etc., can access the Internet? Why do we believe this is a priority for the U.S. State Department or for public diplomacy as a whole?

Much work on Internet censorship isn't motivated by a theory of change—it's motivated by a deeply-held conviction—one that I share—that the ability to share information is a basic human right. Article 19 of the Universal Declaration of Human Rights states that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[22] The Internet is the most efficient system we've ever built to allow people to seek, receive and impart information and ideas, and therefore, we need to ensure everyone has unfettered Internet access. The problem with the Article 19 approach to censorship circumvention is that it doesn't help us prioritize. It simply makes it imperative that we solve what may be an unsolvable problem.

If we believe that access to the Internet will change closed societies in a particular way, we can prioritize access to those aspects of the Internet. Our theory of change helps us figure out what we must provide access to. The four theories I list below are rarely explicitly stated, but I believe they underlie much of the work behind censorship circumvention.

> **The Suppressed Information Theory**: If we can provide certain suppressed information to people in closed societies, they'll rise up, challenge their leaders and usher in a different government. We might choose to call this the "Hungary '56 theory"[23]—reports of struggles against communist governments around the world, reported into Hungary via Radio Free Europe, encouraged Hungarians to rebel against their leaders. (Unfortunately, the U.S. didn't support the revolutionaries militarily—as many in Hungary had expected—and the revolution was brutally quashed by a Soviet invasion.)

---

21 Mark Schmitt, *The "Theory of Change" Primary*, THE AMERICAN PROSPECT, Dec. 21, 2007, **http://www.prospect.org/cs/articles?article=the_theory_of_change_primary**.

22 The Universal Declaration of Human Rights, art. 19, G.A. Res. 217A(III), U.N. GAOR, 3d Sess., U.N. Doc. A/810 (Dec. 10, 1948), **http://www.un.org/en/documents/udhr/index.shtml**.

23 For more information on the Hungarian Revolution of 1965, see *Hungarian Revolution of 1956*, WIKIPEDIA, **http://en.wikipedia.org/wiki/Hungarian_Revolution_of_1956**.

Or we could term this the "North Korea theory," because a state as closed as North Korea might be a place where unsuppressed information—about the fiscal success of South Korea, for instance—could provoke revolution. Barbara Demick's beautiful piece in the New Yorker, "The Good Cook," gives a sense of how little information most North Koreans have about the outside world and how different the world looks from Seoul.[24] Nonetheless, even North Korea is less informationally isolated than we think—*The Dong-A Ilbo*, a South Korean newspaper, reports an "information belt" along the North Korea/China border where calls on smuggled mobile phones are possible between North and South Korea.[25] Other nations are far more open—the Chinese tend to be extremely well informed about both domestic and international politics, both through using circumvention tools and because Chinese media reports a great deal of domestic and international news.

It's possible that access to information is a necessary, though not sufficient, condition for political revolution. It's also possible that we overestimate the power and potency of suppressed information, especially as information is so difficult to suppress in a connected age.

**The Twitter Revolution Theory:** If citizens in closed societies can use the powerful communications tools made possible by the Internet, they can unite and overthrow their oppressors. This is the theory that led the U.S. State Department to urge Twitter to postpone a period of scheduled downtime during the Iran election protests.[26] While it's hard to make the case that technologies of connection are going to bring down the Iranian government,[27] good examples exist, like the role of the mobile phone in helping to topple President Estrada in the Philippines.[28]

There's been a great deal of enthusiasm in the popular press for the Twitter revolution theory, but careful analysis reveals some limitations. The communications channels opened online tend to be compromised quickly,

---

24 Barbara Demick, *The Good Cook*, THE NEW YORKER, Nov. 2, 2009, at 58, **http://www.newyorker.com/reporting/2009/11/02/091102fa_fact_demick**.

25 *North Koreans Directly Connect with South Koreans via Chinese Cell Phones*, ASK A KOREAN!, Jan. 17, 2010, **http://askakorean.blogspot.com/2010/01/excellent-article-on-dong-ilbo-about.html**.

26 Sue Pleming, *U.S. State Department Speaks to Twitter Over Iran*, REUTERS, June 16, 2009, **http://www.reuters.com/article/idUSWBT01137420090616**.

27 *See* Cameron Abadi, *Iran, Facebook, and the Limits of Online Activism*, FOREIGN POLICY, Feb. 12, 2010, **http://www.foreignpolicy.com/articles/2010/02/12/irans_failed_facebook_revolution**.

28 *See Joseph Estrada Controversies*, WIKIPEDIA, **http://en.wikipedia.org/wiki/Joseph_Estrada#Controversies**.

used for disinformation and monitoring activists. And when protests get out of hand, governments of closed societies don't hesitate to pull the plug on networks—China has blocked Internet access in Xinjiang for months, and Ethiopia turned off SMS on mobile phone networks for years after they were used to organize street protests. And it's worth noting that prophesied "twitter revolutions" in Moldova and Iran both failed in the face of authoritarian governments.

**The Public Sphere Theory**: Communication tools may not lead to revolution immediately, but they provide a new rhetorical space where a new generation of leaders can think and speak freely. In the long run, this ability to create a new public sphere, parallel to the one controlled by the state, will empower a new generation of social actors, though perhaps not for many years.

Marc Lynch made a pretty persuasive case for this theory in a talk last year about online activism in the Middle East.[29] In the former Soviet Union, samizdat (self-published, clandestine media) was probably more important as a space for free expression than it was as a channel for disseminating suppressed information.[30] The emergence of leaders, like Vaclav Havel, whose authority was rooted in cultural expression as well as political power, makes the case that simply speaking out is powerful. But the long timescale of this theory makes it hard to test.

The theory we accept shapes our policy decisions. If we believe that disseminating suppressed information is critical—either to the public at large or to a small group of influencers—we might focus our efforts on spreading content from Voice of America or Radio Free Europe. Indeed, this is how many government forays into censorship circumvention began—national news services began supporting circumvention tools so their content, painstakingly created in languages like Burmese or Farsi, would be accessible in closed societies. This is a very efficient approach to anti-censorship—we can ignore many of the problems associated with abusing proxies and focus on prioritizing news over other less-important bandwidth-hogging uses, like the video of the cat flushing the toilet. Unfortunately, we've got a long track record that shows that this form of anti-censorship doesn't magically open closed regimes, which suggests that increasing our reliance on this strategy might be a poor idea.

---

29 Ethan Zuckerman, *Marc Lynch Asks Us to be Realistic About Digital Activism in the Middle East*, April 27, 2009, **http://www.ethanzuckerman.com/blog/2009/04/27/marc-lynch-asks-us-to-be-realistic-about-digital-activism-in-the-middle-east**.

30 *See generally*, Peter Steiner, *Introduction: On Samizdat, Tamizdat, Magnitizdat, and Other Strange Words*, 29 POETICS TODAY 613 (2008) **http://poeticstoday.dukejournals.org/cgi/reprint/29/4/613.pdf**.

If we adopt the Twitter Revolution theory, we should focus on systems that allow for rapid communication within trusted networks. This might mean tools like Twitter or Facebook, but it probably means tools like LiveJournal and Yahoo! Groups, which gain their utility through exclusivity, allowing small groups to organize outside the gaze of the authorities. If we adopt the public sphere approach, we want to open any technologies that allow public communication and debate—blogs, Twitter, YouTube, and virtually anything else that fits under the banner of Web 2.0. This, unfortunately, presents technical challenges that are proving extremely difficult to solve.

What does all this mean in terms of how the U.S. State Department should allocate their money to promote Internet Freedom? My goal was primarily to outline the questions they should be considering, rather than offering specific prescriptions. But here are some possible implications of these questions:

If we believe the U.S. government should be exporting "Internet freedom"—and there are good reasons to argue that a government, and particularly the US government, shouldn't take on this task—we need to continue supporting circumvention efforts, at least in the short term. But we need to disabuse ourselves of the idea that we can "solve" censorship through circumvention. We should support circumvention until we find better technical and policy solutions to censorship, not because we can tear down the Great Firewall by spending more on proxies, *etc.*

Second, if we want more people using circumvention tools, we need to find ways to make these systems fiscally sustainable. Sustainable circumvention is becoming an attractive business for some companies.[31] It needs to be part of a comprehensive Internet freedom strategy, and we need to develop strategies that are sustainable and provide low- to zero-cost access to users in closed societies.

Third, as we continue to fund circumvention, we need to address usage of these tools to send spam, commit fraud and steal personal data. We might do this by relying less on IP addresses as an extensive, fundamental means of regulating bad behavior, but we have to find a solution that protects networks against abuse while maintaining the possibility of anonymity, a difficult balancing act.

Additionally, we need to shift our thinking from helping users in closed societies access blocked content to helping publishers reach all audiences. In doing so, we may gain those publishers as a valuable new set of allies as well as opening a new class of technical solutions.

---

[31] Lara Farrar, *Cashing in on Internet Censorship*, CNN, Feb. 19, 2010, **http://www.cnn.com/2010/TECH/02/18/internet.censorship.business/?hpt=Sbin**.

Furthermore, if our goal is to allow people in closed societies to access an online public sphere or to use online tools to organize protests, we need to bring the administrators of these tools into the dialog. Secretary Clinton suggests that we make free speech part of the American brand identity—let's find ways to challenge companies to build blocking resistance into their platforms and to consider Internet freedom as a central part of their business mission. We need to address the fact that making platforms unblockable has a cost for content hosts and that their business models currently don't reward companies for providing services to blocked users.

The U.S. government should treat Internet filtering—and more aggressive hacking and DDoS attacks—as a barrier to trade. The U.S, should strongly pressure governments in open societies like Australia and France to resist the temptation to restrict Internet access, as this behavior helps China and Iran make the case that their censorship is in line with international norms. And we need to fix U.S. treasury regulations that make it difficult and legally ambiguous for companies like Microsoft and projects like SourceForge[32] to operate in closed societies. If we believe in Internet Freedom, the first step is rethinking these policies so they don't hurt ordinary Internet users.

Finally, if attempts to export Internet freedom are to be met with something other than cynicism or skepticism, the U.S. government needs to do a better job of protecting free speech domestically. The pressure exerted by individual Senators and by the State Department on companies like Amazon and PayPal to terminate services to WikiLeaks calls into question the U.S. government's commitment to online free speech. If the U.S. wants countries like China to consider a more free and open Internet, control of the Internet in the U.S. must also follow the rule of law, and not fall victim to political expediency.

If we take seriously Secretary Clinton's call, the danger is that we increase our speed marching in the wrong direction. As we embrace the goal of Internet Freedom, now is the time to ask what we're hoping to accomplish and to shape our strategy accordingly.

---

[32] SourceForge is an open source code depository from which software can be developed and downloaded. For more information, see **http://sourceforge.net/**.

## THE BEST THINKING ABOUT THE FUTURE OF DIGITAL POLICY

This unique collection brings together 26 thought leaders on Internet law, philosophy, policy and economics to consider what the next digital decade might bring. Has the Internet been good for our culture? Is the Internet at risk from the drive to build more secure, but less "open" systems and devices? Is the Internet really so "exceptional?" Has it fundamentally changed economics? Who—and what ideas—will govern the Net in 2020? Should online intermediaries like access providers, hosting providers, search engines and social networks do more to "police" their networks, increase transparency, or operate "neutrally?" What future is there for privacy online? Can online free speech be regulated? Can it really unseat tyrants? These 31 thought-provoking essays tackle these questions and more. This book is essential reading for anyone gazing toward the digital future.

## CONTRIBUTORS

Rob Atkinson
Stewart Baker
Ann Bartow
Yochai Benkler
Larry Downes
Josh Goldfoot
Eric Goldman
James Grimmelman
H. Brian Holland
David Johnson
Andrew Keen
Hon. Alex Kozinski
Mark MacCarthy
Geoff Manne
Evgeny Morozov
Milton Mueller
John Palfrey
Frank Pasquale
Paul Szynol
Adam Thierer
Hal Varian
Christopher Wolf
Tim Wu
Michael Zimmer
Jonathan Zittrain
Ethan Zuckerman

**TechFreedom**
techfreedom.org
1899 L ST NW, 12th Floor
Washington, D.C. 20036

**NextDigitalDecade.com**