Center for a New American Security

SEPTEMBER 2014

Bringing Liberty Online

Reenergizing the Internet Freedom Agenda in a Post-Snowden Era

POLICY BRIEF

By Richard Fontaine

The 2013 revelations of mass surveillance by the U.S. government transformed the global debate about Internet freedom. Where once Washington routinely chided foreign governments and their corporate collaborators for engaging in online censorship, monitoring and other forms of Internet repression, the tables have turned. Edward Snowden, a former National Security Agency (NSA) contractor, leaked thousands of documents revealing America's most secret electronic surveillance programs, unleashing a tidal wave of criticism and charges of hypocrisy, many directed at some of the very U.S. officials who have championed online freedom.

America's Internet freedom agenda – the effort to preserve and extend the free flow of information online – hangs in the balance.[1] Already a contested space, the Internet after the Snowden revelations has become even more politically charged, with deep international divisions about its governance and heated battles over its use as a tool of political change. With 2.8 billion Internet users today, and several billion more expected over the next decade, the contest over online freedom grows more important by the day.[2] As an ever-greater proportion of human activity is mediated through Internet-based technologies, the extent of online rights and restrictions takes on an increasingly vital role in political, economic and social life.[3]

Despite the many complications arising from the Snowden disclosures, America still needs a comprehensive Internet freedom strategy, one that tilts the balance in favor of those who would use the Internet to advance tolerance and free expression, and away from those who would employ it for repression or violence.[4] It will need to pursue this strategy while drawing a sharp distinction between surveillance for national security purposes (in which all governments engage) and monitoring as a means of political repression (which democracies oppose). This is not an easy task, but it is an important one. More than a year after the first Snowden revelations emerged, now is the time to reenergize the Internet freedom agenda.

Internet Freedom before Snowden

The U.S. government's explicit pursuit of Internet freedom began during the Bush administration's second term. Among other steps, the establishment of the State Department's Global Internet Freedom Task Force aimed to coordinate efforts to promote Internet freedom and to respond to online

censorship.[5] Building on this foundation, Secretary of State Hillary Rodham Clinton made the expansion of online rights a major focus of U.S. foreign policy in the first Obama term. Speaking in 2010, she cited Franklin Delano Roosevelt's Four Freedoms and added a fifth, the "freedom to connect – the idea that governments should not prevent people from connecting to the Internet, to websites or to each other."[6] A year later, she pledged America's "global commitment to Internet freedom, to protect human rights" – including the rights to expression, assembly and association – "online as we do offline."[7] And after the Arab Spring, the United States in 2011 established the Freedom Online Coalition, a collaboration of 23 countries to coordinate efforts to expand global Internet freedom.[8]

The U.S. government has backed up its words with resources. Since 2009, the State Department and other government agencies have spent more than $125 million on Internet freedom programming.[9] In addition to the State Department's efforts, other government agencies, including the Broadcasting Board of Governors, the U.S. Agency for International Development, the Defense Advanced Research Projects Agency and others, fund the development and deployment of tools aimed at expanding Internet freedom. These programs invest in technologies that allow users to circumvent firewalls so as to access censored material, communicate outside the watchful eye of autocratic regimes, secure their websites and data, link computers in decentralized mesh networks, and establish new Internet connections when existing ones have been cut.[10] It supplements the provision of technology with training programs in dozens of countries.

The Obama administration also took regulatory steps to promote Internet freedom, particularly after technology demonstrably facilitated the 2009 Green Revolution in Iran and the 2011 Arab Spring. The Treasury Department relaxed restrictions on the export of Internet-related software and services to Iran, explicitly to "foster and support the free flow of information to individual Iranian citizens."[11] Two years later, the White House issued an executive order that imposed sanctions on individuals who engaged in computer and network disruption, monitoring and tracking on behalf of the governments of Iran or Syria.[12]

The U.S. government has backed up its words with resources. Since 2009, the State Department and other government agencies have spent more than $125 million on Internet freedom programming.

The United States has aimed to promote the free flow of online information through diplomatic action as well. State Department diplomats pressure repressive regimes to loosen their Internet restrictions, free imprisoned bloggers and ensure that citizens can express themselves online without fear of punishment. U.S. government officials have engaged in significant dialogue with U.S. and multinational technology companies about their involvement in aiding Internet repression and in establishing transparency standards. American diplomats have also pressed for Internet freedom in the proliferating international fora that have taken up the issue. In 2012, for instance, the United States won approval of a U.N. Human Rights Council resolution affirming that freedom of expression and other rights that people have offline must also be protected online.[13] Trade agreements have provided yet another vehicle for the U.S. Internet freedom agenda with, for example, hortatory language in the U.S.-Korea Free Trade Agreement calling for the free flow of online information.[14]

A key element of U.S. action has been aimed at preventing fundamental changes to the multistakeholder model of Internet governance, which brings together individuals, governments, civil society organizations, private firms and others for transparent and consensus-based decisionmaking.[15] One such challenge arose at the December 2012 World Conference on International Telecommunications, when 89 countries – a majority of ITU members in attendance – supported an attempt by Russia, China, Iran and others to give governments greater control over the Internet.[16] Despite opposition from the United States and others, the session ended with 89 countries signing the revised treaty; 55 other countries did not. As a sign of what may come in future international treaty negotiations, such numbers did not favor the multistakeholder model, and this was so even before the Snowden revelations emerged to complicate U.S. efforts.

The Snowden Fallout and the Internet Freedom Agenda

The dramatic revelations about NSA spying that began to emerge in June 2013 provoked a storm of international reaction.[17] Political leaders expressed outrage at American surveillance practices and threatened a raft of retaliatory measures. President Dilma Rousseff of Brazil cancelled a planned state visit to the United States and the Brazilian government later organized an international meeting (NetMundial) to discuss the future of Internet governance.[18] German Chancellor Angela Merkel was deeply affronted by the alleged monitoring of her personal cellphone. Chinese and other officials charged America with blatant hypocrisy. The fallout affected the private sector as well; where previously the focus of many observers had been on the aid given by U.S. companies to foreign governments engaged in Internet repression, the gaze shifted to the role American corporations play – wittingly or not – in enabling U.S. surveillance. Countries that had been the target of American reproaches rebuked the U.S. government for what they saw as hypocrisy.

The United Nations and other international venues became platforms for international criticism of the United States. Germany and Brazil together sponsored a resolution adopted by the U.N. General Assembly in late 2013 backing a "right to privacy" in the digital age.[19] In June 2014, the U.N. High Commissioner for Human Rights issued a report that endorsed digital privacy as a human right and criticized mass surveillance as "a dangerous habit rather than an exceptional measure."[20] Some European officials began to question the existing Internet governance model itself. In a statement, the European Commission said, "Recent revelations of large-scale surveillance have called into question the stewardship of the US when it comes to Internet Governance. So given the US-centric model of Internet Governance currently in place, it is necessary to broker a smooth transition to a more global model."[21]

Nongovernmental groups that might otherwise be partners with the U.S. government in promoting Internet freedom reacted sharply as well. Reporters Without Borders, for instance, listed the NSA as an "Enemy of the Internet" in its 2014 report on entities engaged in online repression. Drawing no distinction between surveillance aimed at protecting national security and surveillance intended to suppress free expression and political dissent, the organization declared the NSA "no better than [its] Chinese, Russian, Iranian or Bahraini counterparts."[22] Mass surveillance methods used by democracies like the United States, it added, are "all the more intolerable" as they "are already being used by authoritarian countries such as Iran, China, Turkmenistan, Saudi Arabia and Bahrain to justify their own violations of freedom of information."[23] Tim Berners-Lee, the inventor of the World Wide Web, said, "Mass surveillance is the most immediate threat to the open Internet and the most

insidious because we can't see it."[24] The Electronic Frontier Foundation asserted that "mass surveillance is inherently a disproportionate measure that violates human rights,"[25] and officials with Human Rights Watch observed that the surveillance scandal would render it more difficult for the U.S. government to press for better corporate practices and for companies to resist overly broad surveillance mandates. "Now," its chief researcher said, "the vision and credibility of the U.S. and its allies on Internet freedom is in tatters."[26]

As former NSA general counsel Stewart Baker warned, "The Snowden disclosures are being used to renationalize the Internet and roll back changes that have weakened government control of information."

The reactions to the Snowden disclosures threatened to go beyond verbal denunciations, diplomatic protests and critical press. The most serious commercial fallout came in the rising support for data localization requirements. Russia in July 2014 approved legislation that requires data operators to store the personal data of its citizens within the country's borders.[27] Indonesia, Brazil and Vietnam have also called for their citizens' data held by companies such as Facebook to be stored domestically.[28] Data localization has been debated in the European Parliament and elsewhere on the continent as well.[29] Apart from the chilling effect on innovation and the loss of business to America companies, Internet freedom itself could become a casualty of such mandates. If a user's data must be held within the borders of a repressive country, its government will have new opportunities to censor, monitor and disrupt online information flows.

Such moves, combined with increasing questions about the multistakeholder approach to Internet governance (and possible support for a government-driven approach), together give rise to concerns about the potential "Balkanization" of the Internet, in which a constellation of national-level systems could take the place of the current global online infrastructure. As former NSA general counsel Stewart Baker warned, "The Snowden disclosures are being used to renationalize the Internet and roll back changes that have weakened government control of information."[30]

This is evident in other proposed steps as well. Brazil and the European Union have announced plans for an undersea cable that would route data transmissions directly between Europe and Latin America and bypass the United States.[31] The European Union threatened to suspend the Safe Harbor data-sharing agreement with the United States and promulgated new rules for it that EU officials said stemmed directly from worries after the Snowden disclosures.[32]

A cautionary note is in order when interpreting the reactions to the Snowden affair. Some developments – such as data localization requirements and worries about a splintering Internet – predated the revelations and have been accelerated rather than prompted by them. Autocratic governments also drew lessons from the technology-fueled Arab Spring, resulting in actions aimed at limiting Internet freedom. Other white-hot responses cooled when rhetoric turned to action. Brazil's new "Marco Civil" Internet law, approved in April 2014, left out a number of the strongest responses that had been widely debated in the run-up to its adoption. The EU did not go through with its threatened Safe Harbor data-exchange boycott. And for all of the worries about laws that would require the local storage of users' data, few countries have actually passed them. Nevertheless, the potential for such fallout remains.

The United States Reacts

Despite the international outrage, and both public and private criticism of U.S. surveillance policies, the U.S. government has continued its Internet freedom–related activities, albeit at a lower public volume. In early 2014, Secretary of State John Kerry, addressing the Freedom Online Coalition conference in Estonia, called for an "open, secure, and inclusive Internet."[33] U.S. Internet freedom programming continues: the State Department's Bureau of Democracy, Human Rights and Labor alone planned to expend roughly $18 million in 2014 on anti-censorship technology, secure communications, technology training and rapid response to bloggers under threat.[34] In June, the United States sponsored a successful U.N. Human Rights Council resolution reaffirming that the same rights that people have offline, including freedom of expression, must be protected online, regardless of frontiers.[35]

While continuing to execute the Internet freedom agenda, U.S. officials have attempted to reconcile their government's surveillance practices with its expressed desire for greater online freedom. This is challenging, to say the least. U.S. officials draw a critical distinction between monitoring communications for purposes of protecting national security and surveillance aimed at repressing political speech and activity. While this distinction is intuitive to many Americans, it is likely to be lost on many others, particularly where autocratic regimes consider domestic political dissent to be a national security threat. At its bluntest, the American position is that it is legitimate, for example, for the U.S. government, but not for the Chinese government, to surveil Chinese citizens. This is and will remain a tough sell.

Secretary Kerry has defended the Obama administration's reforms to signals intelligence collection, saying that they are based on the rule of law, conducted pursuant to a legitimate purpose, guided by proper oversight, characterized by greater transparency than before and fully consistent with the American vision of a free and open Internet.[36] In March 2014, Deputy Assistant Secretary of State Scott Busby addressed the linkage between surveillance and Internet freedom and added two principles to Kerry's – that surveillance should not be arbitrary but rather as tailored as possible, and that decisions about intelligence collection priorities should be informed by guidance from an authority outside the collection agency.[37] In addition, the U.S. government has taken other steps to temper the international reaction. For example, the Department of Commerce opted to relinquish its oversight of ICANN – the organization that manages domain name registries – to the "global Internet community."[38]

Such moves are destined to have only a modest effect on foreign reactions. U.S. surveillance will inevitably continue under any reasonably likely scenario (indeed, despite the expressions of outrage, not a single country has said that it would cease its surveillance activities). Many of the demands – such as for greater transparency – will not be met, simply due to the clandestine nature of electronic espionage. Any limits on surveillance that a government might announce will not be publicly verifiable and thus perhaps not fully credible. Nor will there be an international "no-spying" convention to reassure foreign citizens that their communications are unmonitored. As it has for centuries, state-sponsored espionage activities are likely to remain accepted international practice, unconstrained by international law. The one major possible shift in policy following the Snowden affair – a stop to the bulk collection of telecommunications metadata in the United States – will not constrain the activity most disturbing to foreigners; that is, America's surveillance of them. At the same time, U.S. officials are highly unlikely to articulate a global "right

to privacy" (as have the U.N. High Commissioner for Human Rights and some foreign officials), akin to that derived from the U.S. Constitution's fourth amendment, that would permit foreigners to sue in U.S. courts to enforce such a right.[39] The Obama administration's January 2014 presidential directive on signals intelligence refers, notably, to the "legitimate privacy interests" of all persons, regardless of nationality, and not to a privacy "right."[40]

A Snapshot of Internet Freedom Today

The scrambled Internet freedom narrative and its complicated consequences are discouraging, not least because the need for an active online freedom agenda has never been more pressing. It is today estimated that roughly half of Internet users worldwide experience online censorship in some form.[41] Freedom House observes a deterioration in global Internet freedom over the three consecutive years it has issued reports; its 2013 volume notes that Internet freedom declined in more than half of the 60 countries it assessed. Broad surveillance, new legislation controlling online content and the arrest of Internet users are all on the increase; over the course of a single year, some 24 countries passed new laws or regulations that threaten online freedom of speech.[42]

A glance at the past 12 months reveals a disturbing trend. In Turkey, for example, after its high court overturned a ban on Twitter, the government began demanding that the company quickly implement orders to block specific users. Ankara also blocked YouTube after a surreptitious recording of the country's foreign minister surfaced, and it has dramatically increased its takedown requests to both Twitter and Google.[43] Russia has begun directly censoring the Internet with a growing blacklist of websites, and under a new law its government can block websites that encourage people to participate in unauthorized protests.[44] Chinese social media censorship has become so

It is today estimated that roughly half of Internet users worldwide experience online censorship in some form.

pervasive that it constitutes, according to one study, "the largest selective suppression of human communication in the history of the world."[45] China has also begun assisting foreign countries, including Iran and Zambia, in their efforts to monitor and censor the Internet.[46] Vietnam has enacted a new law making it illegal to distribute digital content that opposes the government.[47] Venezuela has blocked access to certain websites and limited Internet access in parts of the country.[48] A robust, energetic American Internet freedom agenda is most needed at the very moment that that agenda has come under the greatest attack.

Reenergizing the Agenda

Precisely because the Internet is today such a contested space, it is vitally important that the United States be actively involved in promoting online freedom. America's Internet freedom efforts accord with the country's longstanding tradition of promoting human rights, including freedoms of expression, association and assembly. And it represents a bet: that access to an open Internet can foster elements of democracy in autocratic states by empowering those who are pressing for liberal change at home. While the outcome of that bet remains uncertain, there should be no doubt about which side the United States has chosen.

Reenergizing the Internet freedom agenda begins with acknowledging that the United States must promote that agenda even as it continues to engage in electronic surveillance aimed at protecting national security. The U.S. government will simply have to endure some significant amount of

continuing criticism and opposition. At the same time, it should continue to draw a sharp distinction between surveillance for national security purposes (in which all governments engage) and monitoring as a means of political repression (which democracies oppose). To those who see no distinction between American surveillance and that of autocracies, government officials should point out that key legal guarantees matter: the U.S. Constitution's first amendment protects against censorship and political repression at home, while in autocratic systems such safeguards are nonexistent or not enforceable.[49]

As the United States continues its significant efforts, described above, to further the Internet freedom agenda, there are additional steps it should take to refocus and reenergize the effort:

CALL ON FOREIGN GOVERNMENTS TO EMBRACE SURVEILLANCE PRINCIPLES

While an international convention regulating electronic spying is nearly inconceivable, the principles already articulated by U.S. government officials represent an important effort to distinguish between American surveillance and the efforts of repressive governments. Given the active surveillance programs of democracies and autocracies alike, the United States should call on other governments to embrace similar principles, or to explain why they are unwilling to do so.

ENSURE THAT THE U.S. GOVERNMENT CONDUCTS COMPREHENSIVE COST/BENEFIT ANALYSES OF SURVEILLANCE DECISIONS

It is now clear that decisions made in the intelligence community about surveillance can have profound implications for the Internet freedom agenda as executed by other agencies. Government officials should ensure that all costs – including the costs if clandestine efforts are discovered – are considered when making surveillance decisions, with input from all relevant stakeholders. Given the linkages between surveillance and Internet freedom, a more unified interagency deliberation process is required.

ENHANCE THE TRANSPARENCY OF U.S. GOVERNMENT DATA REQUESTS

The United States should provide more publicly-accessible information on its requests for user data, whether via requests to U.S. or multinational companies, or abroad through mutual legal assistance treaties. Making more hard information available about the true scope of U.S. government data requests may help reduce the degree of political distrust that currently prevails.

SEEK CORPORATE TRANSPARENCY

The flip side to increased transparency by the U.S. government is greater provision of information by the corporate recipients of data requests. Transparency reports now voluntarily offered by companies such as Facebook, Verizon, Comcast, Google, Microsoft and Vodafone on the scope of government demands for users' data could provide a model for other companies. As companies seek greater transparency from governments, they should provide it as well, including information on their sales to repressive countries of Internet-related products and services.

ARTICULATE THE CONNECTION BETWEEN INTERNET FREEDOM AND ECONOMIC PROSPERITY

Online commerce requires a basic level of security and free flow of online information in order to operate properly. U.S. officials should weave the economic argument into all of their appeals for greater Internet freedom and should present evidence that Internet repression imposes an economic cost.

EMPLOY TRADE AGREEMENTS

The Trans-Pacific Partnership and the Transatlantic Trade and Investment Partnership represent two key opportunities to further the Internet freedom

agenda. Some of America's negotiating partners will seek to use privacy concerns to block access by U.S. technology companies to foreign markets. The United States should oppose such moves and insist on provisions guaranteeing the free flow of online information across borders.

USE PUBLIC DIPLOMACY

While perhaps the last thing American policymakers wish to do in the wake of the Snowden scandal is to contest Internet freedom before foreign publics, they might be surprised at receptiveness to the message, if not the messenger. A recent poll, for instance, revealed widespread opposition to online censorship in developing countries; majorities in nearly all of those surveyed said that it is important for people to access the Internet without government censorship.[50] U.S. officials and diplomatic personnel overseas should engage in public diplomacy to help bolster the constituency that understands the importance of a free Internet.

The International Telecommunication Union Plenipotentiary scheduled for fall 2014 in Busan, South Korea, represents an important moment in the fight for Internet freedom. At this meeting, the first ITU treaty-writing conference since the Snowden revelations became public, the world's democracies and autocracies will once again contest who – if anyone – should control the online space. China, Russia, Iran and others will call for "Internet sovereignty," claiming the right of governments to determine the content of Internet flows within their territories.[51] Democracies may be divided; it remains unclear whether countries such as Brazil and Germany will embrace the Internet governance status quo or will realign with states opposing American positions.

Now, then, is a crucial time for the United States to reenergize its approach to Internet freedom. As technology entrepreneur Marc Andreessen recently said, given the loss of trust in the United States following the Snowden disclosures, it remains an open question whether in five years the Internet will operate as it does today.[52] Such concerns may turn out to be overdrawn. But with the future of online freedom at stake in decisions made by governments, corporations and individuals today, it is vital for the United States, despite all of the complications and difficulties of the past year, once again to take the lead in defense of Internet freedom.

The author thanks Ambassador David Gross and Dr. Dafna Rand for their expert, insightful feedback on this policy brief, and remains solely responsible for its contents.

ENDNOTES

1. The term "Internet freedom" means many things to many people, including freedom of speech, net neutrality, and the physical provision of information technology. As used by the U.S. government and in this policy brief, Internet freedom refers to the notion that universal rights – including the rights to freedom of expression, assembly and association – extend to the digital sphere.

2. For usage statistics and estimates, "Doing the ICANN-can," *The Economist*, March 22, 2014; and Eric E. Schmidt and Jared Cohen, "The Future of Internet Freedom," *New York Times*, March 11, 2014.

3. Richard Fontaine, "Getting 'Internet Freedom' Straight," TechCrunch, January 15, 2012, http://techcrunch.com/2012/01/15/getting-internet-freedom-straight/.

4. For a full articulation of such a strategy, see Richard Fontaine and Will Rogers, "Internet Freedom: A Foreign Policy Imperative in the Digital Age," Center for a New American Security, June 2011, http://www.cnas.org/publications/reports/internet-freedom-a-foreign-policy-imperative-in-the-digital-age.

5. U.S. Department of State, *State Summary of Global Internet Freedom Task Force* (December 20, 2006), http://iipdigital.ait.org.tw/st/english/article/2006/12/20061220173640xjsnommis0.7082331.html.

6. Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom," Newseum, Washington (January 21, 2010), http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

7. Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World," The George Washington University, Washington (February 15, 2011), http://www.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm.

8. Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," German Institute for International and Security Affairs, March 2014, 9.

9. Scott Busby, "Ten Things You Need to Know About U.S. Support for Internet Freedom," May 29, 2014, http://blogs.state.gov/stories/2014/05/29/ten-things-you-need-know-about-us-support-internet-freedom.

10. Ibid.

11. U.S. Department of Treasury, Office of Foreign Assets Control, "Interpretive Guidance and Statement of Licensing Policy on Internet Freedom in Iran," March 20, 2010, http://www.treasury.gov/resource-center/sanctions/Programs/Documents/internet_freedom.pdf.

12. Executive Order 13606, "Blocking the Property and Suspending Entry Into the United States of Certain Persons With Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology,

April 23, 2012, http://www.whitehouse.gov/the-press-office/2012/04/23/executive-order-blocking-property-and-suspending-entry-united-states-cer.

13. Somini Sengupta, "U.N. Affirms Internet Freedom as a Basic Right," New York Times Bits Blog, July 6, 2012, http://bits.blogs.nytimes.com/2012/07/06/so-the-united-nations-affirms-internet-freedom-as-a-basic-right-now-what/.

14. U.S.-Korea Free Trade Agreement, http://www.ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text.

15. Lawrence E. Strickling, "Moving Together Beyond Dubai," April 2, 2013, http://www.ntia.doc.gov/blog/2013/moving-together-beyond-dubai.

16. Stewart M. Patrick, "The Obama Administration Must Act Fast to Prevent the Internet's Fragmentation," *The Internationalist*, February 26, 2014, http://blogs.cfr.org/patrick/2014/02/26/the-obama-administration-must-act-fast-to-prevent-the-internets-fragmentation/.

17. Beyond its impact on the Internet freedom agenda, the Snowden revelations exacted a toll on other important U.S. objectives, including building public-private information-sharing partnerships and exercising the full extent of intelligence cooperation with foreign governments. This policy brief focuses on the impact on the effort to promote the free flow of information online.

18. Katherine Maher, "No, the U.S. Isn't 'Giving Up Control' of the Internet," Politico Magazine, March 19, 2014, http://www.politico.com/magazine/story/2014/03/control-of-the-internet-104830.html#.U9vdsl1dXBE.

19. U.N. News Centre, "General Assembly backs right to privacy in digital age," December 19, 2013, http://www.un.org/apps/news/story.asp?NewsID=46780#.U9vuXl1dXBE.

20. Office of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age," June 30, 2014, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

21. European Commission, "Commission to pursue role as honest broker in future global negotiations on Internet Governance," February 12, 2014, http://europa.eu/rapid/press-release_IP-14-142_en.htm.

22. Reporters Without Borders, "Enemies of the Internet 2014," March 12, 2014, http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf.

23. Ibid., 4.

24. Eileen Donahoe, "Dispatches: The Future of the Internet," April 24, 2014, http://www.hrw.org/news/2014/04/24/dispatches-future-internet.

25. Leo Kelion, "Future of the internet debated at NetMundial in Brazil," BBC News, April 23, 2014, http://www.bbc.com/news/technology-27108869.

26. Cynthia Wong, "Surveillance and the Corrosion on Internet Freedom," July 30, 2013, http://www.huffingtonpost.com/cynthia-m-wong/surveillance-and-the-corr_b_3673037.html.

27. Natalia Gulyaeva and Maria Sedykh, "Russia Enacts Data Localization Requirement; New Rules Restricting Online Content Come into Effect," Chronicle of Data Protection, July 18, 2014, http://www.hldataprotection.com/2014/07/articles/international-eu-privacy/russia-enacts-new-online-data-laws/.

28. Michael Pizzi, "US surveillance imperils global free expression, rights group says," Al Jazeera America, January 21, 2014, http://america.aljazeera.com/articles/2014/1/21/us-sets-dangerousprecedentwithnsasurveillancesayshrw.html.

29. President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," December 12, 2013, 215, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

30. David Ignatius, "After Snowden, a diminished Internet?" *The Washington Post*, February 5, 2014.

31. Gordon M. Goldstein, "The End of the Internet?" *The Atlantic*, July 2014.

32. The U.S.-EU Safe Harbor agreement governs the transfer of private data for commercial purposes and requires American companies to adhere to data-protection principles. See Natasha Lomas, "Post-Snowden, European Commission Sets Out Actions Needed to Restore Trust in E.U.-U.S. Data Flows," TechCrunch, November 27, 2013, http://techcrunch.com/2013/11/27/not-so-safe/.

33. Secretary of State John Kerry, Remarks to the Freedom Online Coalition Conference via teleconference, April 28, 2014, http://www.state.gov/secretary/remarks/2014/04/225290.htm.

34. Author conversation with State Department official, July 17, 2014.

35. United Nations Human Rights Council Resolution, "The promotion, protection and enjoyment of human rights on the Internet," June 20, 2014, www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc.

36. Kerry, Remarks to the Freedom Online Coalition Conference.

37. Scott Busby, State Department on Internet Freedom at RightsCon, March 4, 2014, http://www.humanrights.gov/2014/03/04/state-department-on-internet-freedom-at-rightscon/.

38. Erin Mershon and Jessica Meyers, "Internet administration to shift from U.S. to global stage," Politico, March 14, 2014.

39. Ignatius, "After Snowden."

40. Presidential Policy Directive/PPD-28, "Signals Intelligence Activities," January 17, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

41. Jonathan Masters, "What Is Internet Governance?" Council on Foreign Relations, April 23, 2014, http://www.cfr.org/internet-policy/internet-governance/p32843.

42. Freedom House, *Freedom on the Net 2013: A Global Assessment of Internet and Digital Media*, October 3, 2013, 1-2, 9, http://www.freedomhouse.org/report/freedom-net/freedom-net-2013#.U_ZoT6N4F8E.

43. Joe Parkinson, Sam Schechner and Emre Peker, "Turkey's Erdogan: One of the World's Most Determined Internet Censors," *The Wall Street Journal*, May 2, 2014.

44. Reporters Without Borders, "Russia: control from the top down," March 11, 2014, http://12mars.rsf.org/2014-en/2014/03/11/russia-repression-from-the-top-down/.

45. Gary King, Jennifer Pan, and Margaret E. Roberts, "A Randomized Experimental Study of Censorship in China," paper prepared for the annual meetings of the American Political Science Association, August 28, 2013, 1.

46. Reporters Without Borders, "Enemies of the Internet," 4-5.

47. Schmidt and Cohen, "The Future of Internet Freedom."

48. Kerry, "Remarks to the Freedom Online Coalition Conference."

49. On this point, see the President's Review Group on Intelligence and Communications Technologies, 214.

50. Pew Research Global Attitudes Project, "Emerging and Developing Nations Want Freedom on the Internet," March 19, 2014, http://www.pewglobal.org/2014/03/19/emerging-and-developing-nations-want-freedom-on-the-internet/.

51. Paul Mozur and Yang Jie, "China Argues for 'Internet Sovereignty.' Is It a Good Idea?" *The Wall Street Journal*, June 23, 2014, http://blogs.wsj.com/chinarealtime/2014/06/23/chinas-lays-out-argument-for-internet-sovereignty-convinced/.

52. Anne L. Kim, "Marc Andreessen on Surveillance, Online Education and Bitcoin," TechnoCrat blog, May 20, 2014, http://blogs.rollcall.com/technocrat/marc-andreessen-on-nsa-surveillance-online-education-and-bitcoin/?dcz=.

About the Center for a New American Security

Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policy-makers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. The views expressed in this report are those of the authors and do not represent the official policy or position of the Department of Defense or the U.S. government.

Center for a New American Security
1152 15th St., NW
Suite 950
Washington, DC 20005

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org
www.cnas.org

Contacts
Neal Urwitz
Director of External Relations
nurwitz@cnas.org, 202.457.9409

JaRel Clay
Communications Associate
jclay@cnas.org, 202.457.9410

Photo used wtih permisiion of Alain-Christian.