CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 19 — SEPTEMBER 2015

The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet

Carolina Rossini, Francisco Brito Cruz and Danilo Doneda

THE STRENGTHS AND WEAKNESSES OF THE BRAZILIAN INTERNET BILL OF RIGHTS: EXAMINING A HUMAN RIGHTS FRAMEWORK FOR THE INTERNET

Carolina Rossini, Francisco Brito Cruz and Danilo Doneda

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and the Royal Institute of International Affairs.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHORS

Carolina Rossini is a Brazilian lawyer with over 15 years of experience in Internet and intellectual property law and policy. She is an Access to Knowledge and a digital rights advocate, with a focus on Internet governance, reform of copyright law, trade, open access and open education. In 2008, she founded the OER-Brazil project (www.rea.net.br), which aims for policy and practice changes to foster open educational resources in Brazil. She currently serves as vice president for international policy at Public Knowledge, a digital and consumer rights advocacy group based in Washington, DC. Alongside her work at Public Knowledge, she is a Global Partners Digital international associate and an X-Lab fellow for New America Foundation. Her degrees include an L.L.M. in intellectual property from Boston University, an M.B.A. from Instituto de Empresas-Spain, an M.A. in international economic negotiations from the State University of Campinas/State University of São Paulo and a J.D. from University of São Paulo.

Francisco Brito Cruz is co-director of the InternetLab and the project lead of "InternetLab Reports," which aims to monitor Internet policy law making in Brazil. Francisco holds a master's degree in jurisprudence and philosophy of law from the University of São Paulo (USP), where he also earned his bachelor of laws degree. He won the "Brazil's Internet Framework Bill & Development Award" (Google/FGV-SP, 2012) and was a teaching assistant at Fundação Getúlio Vargas (FGV) Law School (2012-2013). In 2013, Francisco was a visiting researcher at the Center for the Study of Law and Society from the University of California at Berkeley. Between 2012 and 2014, he acted as the coordinator of the Internet, Law & Society Nucleus at the USP Law School.

Danilo Doneda is a Brazilian lawyer and law professor with a Ph.D. in civil law from State University of Rio de Janeiro and an L.L.B. from the Federal University of Paraná. Currently, he serves as an adviser to the Consumer Office of the Ministry of Justice (Senacon), a coordinator of the Centre for Internet, Law, and Society of the Instituto Brasiliense de Direito Público (Cedis/IDP) and member of the Working Group on Consumer Law and Information Society of the Consumer Office of the Ministry of Justice (Senacon). In the past, he served as General Coordinator at the Department of Consumer Protection and Defense in the Ministry of Justice (Brazil), as well as professor at the State University of Rio de Janeiro, Pontifical University of Rio de Janeiro, UniBrasil and FGV. He was former visiting researcher at the Italian Data Protection Authority (Rome, Italy), University of Camerino (Camerino, Italy) and at the Max Planck Institute for Comparative and International Private Law (Hamburg, Germany). He has authored books and several papers and articles about civil law, privacy and data protection.

ACRONYMS

Anatel	National Telecommunications Agency
APC	Association of Progressive Communications
CDC	Consumer Defense Code
CETIC.Br	Center of Studies on Information and Communication Technologies
CGI.Br	Brazilian Internet Steering Committee
CTS-FGV	Center for Technology and Society at Fundação Getúlio Vargas
FoE	freedom of expression
IAP	Internet application provider
ICCPR	International Covenant on Civil and Political Rights
ICP	Internet connection provider
ICT	information and communication technology
ISP	Internet service provider
LAN	local area network
MCI	Marco Civil da Internet
SAL/MJ	Office of Legislative Affairs of the Ministry of Justice
STJ	Brazilian Superior Court of Justice
UDHR	Universal Declaration of Human Rights
UNESCO	UN Educational, Scientific and Cultural Organization

EXECUTIVE SUMMARY

The Marco Civil da Internet (MCI) — also known variously as the Brazilian Internet Bill of Rights, Brazilian Civil Rights Framework for the Internet or the Internet constitution[1] — was approved in Brazil in April 2014 after more than seven years[2] of intense national and international debate and a series of postponed votes in the Brazilian Congress. It established rights of Internet users, state obligations to foster Internet use, and duties and liabilities of companies — both Internet connection providers (ICPs) and Internet application providers (IAPs). It thus challenges actors that purport to be digital and borderless to abide by a deeply national geographic law. The legislation was celebrated, from the user's perspective, as one of the most innovative and protective Internet regulations in the world.[3] Some commentators called it "a far-reaching internet rights law" (Trinkunas and Wallace 2015, 2).

Human rights, including freedoms of expression, association and privacy, sit at the law's core and are embedded across various layers of digital networks — social, content, application and physical (Zittrain 2008) — under the MCI's framework of "Internet use." But until recently, no systematic methodology existed to evaluate this kind of legislation on its strengths and weaknesses as a human rights framework. As the MCI will form the basis for other laws and judicial interpretation — in Brazil and elsewhere, including human rights laws — developing and standardizing a process to evaluate its human rights dimensions becomes essential.

This paper takes the methodologies first developed by former United Nations Special Rapporteur on Freedom of Expression Frank La Rue (later converted to metrics by the Association for Progressive Communication) and applies them to the MCI as a first step toward evaluating its treatment of human rights online. It contains five major sections: the first explains the methodology used to examine the MCI as a human rights framework for the Internet; the second summarizes the process that led to the MCI bill, revealing the political and legal conditions that led to the final text; the third is a discussion of some sensitive Internet policy subjects affected by the law — privacy, freedom of expression (FoE), network neutrality, Internet intermediary liability and, finally, the role of government especially concerning access to Internet; the fourth explores the next steps of Brazilian Internet policy debates, focusing on reinforcing the strengths and addressing the weaknesses of the MCI; and the fifth is a table of the MCI's human rights topics through the lens of our methodology. The conclusions round out the paper.

SECTION I: SETTING A HUMAN RIGHTS ANALYSIS METHODOLOGY

To analyze the MCI from the human rights promotion and enforcement perspective, and to understand the extent of the legal protections it creates, it is crucial to measure the scale and scope of those protections. A significant body of international work already exists that offers a prime starting point: Frank La Rue's concept that human rights protections online equate to those offline. La Rue's framework is used to make a first measurement of the strengths and weaknesses of the MCI.

1 See Question More (2014). For an English version of the bill, see www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf. This version was authored by Carolina Rossini and distributed by the Brazilian Internet Steering Committee (CGI.Br) to all participants of NETmundial in Brazil in April 2014.

2 The seven years is counted from the first article published that argued for the implementation of a civil regulatory framework. See http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm.

3 Some examples can be seen in Abramovay (2014) and at http://rt.com/news/154168-brazil-Internet-freedom-law-conference/.

La Rue argued in 2011 (UN 2011a) that human rights protections are the same for offline and online environments — and that digital networks' ability to provide ample space for individual free expression could lead to the strengthening of other human rights, including political, economic, and social and cultural rights. He argues that FoE is both a fundamental right and an enabler of other rights, such as the right to education, the right to take part in cultural life, and the right to enjoy the benefits of scientific progress and its applications, as well as civil and political rights, such as the rights of association and assembly.

In his 2011 report, La Rue considered a number of online conflicts as having human rights consequences (and, thus, effects on the protection of FoE), such as arbitrary blocking or filtering of content, unfair impositions on Internet intermediary liability models, and disconnection of users, including for copyright violation, privacy and Internet access issues (ibid.). In the final recommendations regarding the identified restrictions to FoE, La Rue makes an important remark: when a restriction is imposed as an exceptional measure on online content, it should pass a three-part cumulative test:

1. The restriction must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency).
2. The restriction must pursue one of the purposes set out in Article 19, paragraph 3, of the International Covenant on Civil and Political Rights (ICCPR), namely: to protect the rights or reputations of others; or to protect national security or public order, or public health or morals (principle of legitimacy).
3. The restriction must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

The 2011 "General Comment No. 34" (UN 2011b) on Article 19 of the ICCPR also informs the methodology. This document, written by the UN Human Rights Committee, updated the guidelines regarding the protection of the FoE (Article 19 of the Universal Declaration of Human Rights [UDHR]). The relevance and application of human rights protections to the Internet is addressed in paragraphs 12, 15, 39, 43 and 44 of the General Comment's text.[4]

The UN Human Rights Committee also recognized that the same rights people enjoy offline should be protected online and that the right of FoE, especially on the Internet, is an issue of increasing interest and importance (ibid.). The committee recognized the global and open nature of digital networks as a "driving force accelerating progress towards development." The document asks policy makers to consider the promotion and facilitation of access to the Internet, and to commit to the promotion, protection and enjoyment of human rights when regulating digital networks.

These references inspired the Association of Progressive Communications (APC) to "provide guidance in monitoring and reporting in internet related human rights violations, specifically those related to freedom of expression"[5] through a metrics framework. The La Rue framework allows stakeholders to assess policies and laws that would regulate the activities and actors on the Internet. Although this initiative is not new to the APC (they had already built a human rights and Internet charter in 2001-2002[6]), the La Rue framework represents a jump forward, contemplating platforms and services that emerged as dominant forces in recent years.

The APC's La Rue framework is used here to compare the MCI to human rights standards because it provides a clear set of measurable indicators. La Rue's framework defines indicators that comply with his report to the Human Rights Council and with General Comment No. 34 on Article 19 of the UDHR, issued by the Human Rights Committee and reflect the realities of the Internet and its various layers. This is important because the rapid pace of technological change means that many public policy makers struggle to keep up with the latest developments in the field.

As a result, Internet policy is a relatively specialized area dominated by technocrats, and the wider social dimension remains comparatively poorly understood. In the absence of global agreement, different countries are developing very different systems of national Internet regulation, without necessarily understanding the implications for a global interconnected network.[7] The APC's La Rue framework is, therefore, not just useful for this paper — it can provide a clear road map for governments seeking to develop a comprehensive, enforceable, human rights-centred policy framework. These indicators provide a structured approach to a comprehensive range of Internet policy issues from the technical to the social, facilitating

4 See www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

5 See www.apc.org/en/node/16359/.

6 This charter was mostly based on the idea that the Internet should be considered a global public space open, affordable and accessible to all. Access and freedom of expression on the Internet and other information and communication technologies (ICTs) can be a powerful tool for social mobilization and development, resistance to injustices, and expression of difference and creativity. Hence, the APC believes that the ability to share information and communicate freely using the Internet is vital to the realization of human rights as enshrined in the UDHR (1948), the International Covenant on Economic, Social and Cultural Rights (1976), the ICCPR (1976) and the Convention of the Elimination of All Forms of Discrimination against Women (1980).

7 This is the idea of Internet fragmentation that is at the core of the research efforts of the Global Commission on Internet Governance. See, for instance, Global Commission on Internet Governance (2014) and Jardine et al. (2014).

consistent international approaches and political interoperability.

The framework contains 29 indicators divided into seven broad categories (see Annex I for the complete framework), which consider:

- arbitrary blocking or filtering of content;
- criminalizing of legitimate expression;
- imposition of Internet intermediary liability;
- the implications of disconnecting users including on the grounds of intellectual property rights violations;
- cyber-attacks;
- privacy and data protection; and
- Internet access.

It is important to note that there are other indicators to measure the MCI's strengths and weaknesses, including a UN Educational, Scientific and Cultural Organization (UNESCO) project with 16 indicators (Puddephatt, Zausmer and Rossini 2014). The differing frameworks and methodologies make meta-analysis difficult, but there are harmonies in the main issues:

- the ability to provide ready access to the Internet, including energy supply, communication infrastructure and the costs of the Internet in its different forms (landline, cellular networks);
- the limitations set by the governments and intermediaries on access to and use of web content, on FoE on the Internet, on the free flow of information, and on the protection of user rights and privacy;
- the responsibility of corporations to provide secure tools to the users for the use of the Internet, for protecting user privacy and anonymity, and to resist government abuses of user rights and liberties; and
- the ways in which the Internet empowers people across society, the economy, and in politics.

Attempting to make cross comparisons therefore involved making a "best effort" to extract the core meaning or goal of the indicator and its common characteristics. The La Rue framework is satisfactory in regard to those four issues, but is even more relevant for the goal of this paper since it is built with human rights concerns at its core.

SECTION II: BUILDING THE MCI — TIMELINE AND CONTEXT

Elaboration Process and Human Rights: Collaborative Law Making to Ensure Human Rights Standards?

Internet policy in Brazil begins with early information technologies industry and importation regulations[8] and the Communications General Act (Law n. 9.472/1997). In 1995, the country established a "truly multi-stakeholder governance body" — the Internet Steering Committee — in order to coordinate the early developments of Brazilian Internet usage (Trinkunas and Wallace 2015, 2, 17–21). In the same year, the Ministry of Communications issued the National Telecommunications Agency's "Norma 4," a decree that defined Internet access as a value-added service, not a telecommunications service under a heavy state regulatory regime. For some commentators, this "effectively shielded Brazil's domestic internet from state dominance and spawned a vibrant private internet sector" (ibid., 18). During the 1990s, this increasingly private sector allowed the spread of the Internet by domestic and commercial users, bringing up questions about how to regulate it.

The growth of Internet use affected the legislative agenda, which began to focus on users' rights, duties or behaviour during the late 1990s, when many bills proposed rules about Internet user behaviour. Most of them (see Brito Cruz 2015, 30–44) set criminal conduct — prohibiting the use of the World Wide Web for criminal purposes, fighting pedophilia and child pornography, filtering inappropriate content and combatting anonymity (Santarém 2010, 20–71).

With the expansion of the commercial Internet, cases started arriving to the judiciary, including tort and other civil and criminal cases. However, without any clear policy or law in place, the decisions were often contradictory throughout the country (Brito Cruz 2015, 20).

In the wake of this morality-centred legislative agenda, Bill n. 84/1.999 arrived. It combined a number of legislative initiatives and was shaped into a comprehensive cybercrime bill. Led by Senator Eduardo Azeredo, the legislation proposed to criminalize many common Internet user behaviours, with chilling effects on FoE. Two provisions exemplify the extremism proposed in 84/1.999: that Internet service providers (ISPs) should surveil users and notify the government about any suspicious activities, and that personal identification and authentication should be a mandatory part of Brazilian Internet access.

8 An example of this is the debate regarding the National Computer Production Policy (Política Nacional de Informática). See www.planalto.gov.br/ccivil_03/leis/L7232.htm.

Cyber activists, civil society organizations and academics strongly opposed 84/1.999. Its authoritarian spin earned it the nickname "AI-5 Digital" in reference to Brazilian military dictatorship practices.[9] At this time, the lawyer and scholar Ronaldo Lemos pleaded in a newspaper article that the first Brazilian Internet law should focus on users' rights (Lemos 2007) and not on cybercrimes. The article helped spur coordinated actions by civil society organizations, which gained public support after a public hearing that the House of Representatives convoked to discuss AI-5 Digital.

Afterwards, the Federal Administration (the Office of Legislative Affairs of the Ministry of Justice [SAL/MJ], the Ministry of Culture and the Office of Strategic Affairs, led by Harvard scholar Roberto Mangabeira Unger[10]) signalled its willingness to influence the Congressional debate, with the Ministry of Justice amplifying the opposition to 84/1.999. The demonstrations against AI-5 Digital succeeded when, in June 2009, then President Luis Inacio Lula da Silva criticized the project during the opening of the X International Free Software Forum (FETEC 2009). As a result, the bill that finally passed was far less invasive than the first draft.

The idea of collaboratively developing an Internet bill emerged from the groups that assembled to oppose AI-5 Digital. The goal was to pivot away from the institutionally driven conservative agenda toward a transparent and participatory one centred on human rights. The Office of Legislative Affairs developed plans for implementing precisely this agenda after the presidential support expressed in 2009 (Brito Cruz 2015, 50–53).

Between 2009 and 2011, the SAL/MJ, in partnership with the Center for Technology and Society at Fundação Getúlio Vargas (CTS-FGV), for which Ronaldo Lemos was coordinator (2003–2013), organized an online platform to collect people's comments and insights for a new bill that promised to establish a regulatory framework to the Internet — the bill that became the MCI. The initiative was a joint effort of different federal administration bodies and the CTS-FGV, a key player in the Azeredo debates and a strong backer of positive, human-centred Internet legislation. The CTS-FGV was then joined by a broader coalition of media reform, free software, consumer and Internet access activists, including organizations such as Intervozes, Instituto Brasileiro de Defesa do Consumidor, Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação and OER-Br, among others. These activities started organizing into a coalition in support of a human rights, consumer and pro-universal access coalition, which was later responsible for a series of public demonstrations around the country.

The push for an Internet "civic milestone" had a dual purpose — to devise a political strategy of reversing the legislative agenda, and to establish a pre-congressional process that could identify broader consensus for complex regulatory choices. In practice, this civil milestone is a human rights-friendly Internet policy agenda that anticipated much of La Rue's work.

The online public consultation occurred in two phases: a broad principle-based discussion of a reference text, and a focused debate on a draft bill provided by the SAL/MJ and the CTS-FGV after an analysis of the reference discussion. Both organizations were moderators during the process, with SAL/MJ making the final decisions regarding the platform and wording of the provided texts. The process meant the draft bill was being built collectively and documented in an online platform,[11] a process the former Secretary of Legislative Affairs Pedro Abramovay called the "collaborative construction of the bill," a stark contrast to the AI-5 Digital.

In accordance with the authors' count and with official Ministry of Justice sources,[12] the first phase of the online debate assembled 133 participants (118 citizens and 15 entities, including class associations and non-governmental organizations) engaged in debate, suggesting principles and commenting on general and specific topics. During the second phase, 245 participants addressed contributions to the draft presented by the SAL/MJ (150 citizens, 14 entities) inserting comments on the online platform designed by the Ministry of Justice or by email. The total number of comments reached 1,507. In addition, 34 Brazilian diplomatic representations sent reports to the Ministry of Justice, answering a request by the Ministry of Foreign Affairs.

An analysis (Brito Cruz 2015, 79) of the online debate platform summarized the findings:

- most of the comments were made by individuals (citizens), not entities;
- some citizens were extremely active, forming a key part of the participatory portion;
- companies, class associations and civil society organizations focused their participation in the last days of consultation;

9 "AI-5" is the acronym for Ato Institucional n. 5 (in English, Institutional Act n. 5), the law that suspended political rights in Brazil in 1968 and was the milestone for the most severe and violent phase of Brazilian military dictatorship (1964–1988).

10 The involvement of Unger and other government officials was noted by Brito Cruz (2015) through interviews with Ministry of Justice policy makers.

11 See http://culturadigital.br/marcocivil/.

12 See the official reports launched on the Cultura Digital platform at http://culturadigital.br/marcocivil?s=relat%C3%B3rio. Another count can be found in Lemos et al. (2015).

- the participation of companies in the digital platform was timid compared to non-governmental organizations and class associations. Companies preferred to send their contributions via separate email;
- the public consultation successfully integrated different business sectors interested on the Internet application market. Many important clusters were represented in the public consultation in at least one of its phases (clusters such as telecommunication companies, small and big Internet application providers, local area network [LAN] houses and ecommerce);
- the concentration of contributions at the first phase was significant on the following topics: 1.1.1 ("Intimacy, privacy and fundamental rights"), 1.1.3 ("Log retention"), 1.1.4 ("How to ensure privacy?"), 1.2.5 ("Anonymous access") and 3.2.2 ("Expansion of broadband networks and digital inclusion"); and
- the dispersion of comments in the second phase was higher, but the debate focused on Articles 14 (data retention provisions) and 20 (which addressed the intermediary liability model to be adopted by the law).

The SAL/MJ led consolidation and drafted a new version of the bill based on input from the online platform. The new consolidated text reproduced the same structure discussed through the public consultation and the bill's justification text included a summary of arguments presented by process participants, demonstrating the quality and seriousness of participant stakeholders.

The Congress Discussion: Lobbying and the "Snowden Effect"[13]

Brazilian President Dilma Rousseff sent the text to the National Congress in 2012, and the MCI bill was assigned to rapporteur Alessandro Molon, a House Representative of the Working Party for São Paulo, and a special commission.[14] Molon developed a legislative strategy based on two fronts: the organization of public hearings in key cities, inviting relevant stakeholders; and the availability of the preliminary versions of his report and bill for debate and commentary through e-Democracia[15] — a public consultation platform developed by the House of Representatives.

Sixty-two experts and representatives of stakeholders spoke at hearings held in six capitals. The thematic panels addressed both specific issues and existing controversies (network neutrality, intermediary liability model, data retention, user rights, content take-down and guidelines for access to the Internet policies) and discussed key points of the MCI. The hearings served to consolidate the positions, reflecting, but not resolving, the biggest disputes. In addition to the debate at the hearings and at e-Democracia, Molon and his staff received more than 54 contributions by email and other less-public means, mostly from companies, class representative entities, and coalitions of national and international advocacy organizations.

After this round of contributions and edits, the final consolidated bill, n. 2.126/2011, was submitted several times to the House of Representatives with no real progress toward an approval until June 2014. That month, news broke of the United States' mass Internet surveillance via former National Security Agency employee Edward Snowden, shaking the Brazilian political agenda (Seligman 2014).

The revelations uncovered operations against the federal government (ibid.). Journalist Glenn Greenwald, responsible for the Snowden scoop in the British newspaper *The Guardian*, joined reporter Sonia Bridi, of the TV program *Fantástico* (owned by the Rede Globo). Bridi and Greenwald began a series of reports every Sunday, revealing digital espionage targeting the Brazilian government and the country's largest public company, Petrobras.

President Rousseff responded with vehemence on the issue (Rossini 2013). After cancelling her October visit to Washington, DC, she addressed the United Nations General Assembly[16] on September 24, 2014 during the High-level Meeting on the Rule of Law[17] and in her speech declared: "Tampering in such a manner in the affairs of other countries is a breach of International Law and is an affront to the principles that must guide the relations among them, especially among friendly nations. A sovereign nation can never establish itself to the detriment of another sovereign nation" (Sterling 2013). Rousseff also said that her government "will do everything within its reach to defend the human rights of all Brazilians and to protect the fruits borne from the ingenuity of our workers and our companies" (ibid.). In a clear shot across the bow of supposedly "borderless" technology companies, Rouseff

13 This topic was strongly inspired by excerpts of the master's thesis of one of the co-authors (Brito Cruz 2015).

14 To be voted by the Brazilian Chamber of Representatives, a bill needs to be analyzed by all the commissions related to the issues that are being regulated. When the issues are many, the chamber's presidency can create a "special commission" to discuss that one bill. This regimental instrument prevented the MCI from being distributed to all the commissions with any thematic affinity, ensuring its quick processing.

15 See http://edemocracia.camara.gov.br/.

16 The General Assembly is the main deliberative, policy-making and representative organ of the United Nations and comprises all 193 members of the United Nations.

17 See www.unrol.org/article.aspx?article_id=168.

added it was "even worse when private companies are supporting this espionage" (ibid.). Brazilians[18] welcomed their president's decision to cancel her Washington trip and address US Internet surveillance in a global public forum (Souza and Gomide 2013).

In saying this, Rouseff was not simply speaking in the manufactured outrage so typical of politics. She was instead speaking from a very different experience fighting against the dictatorship in Brazil in her youth. In dictatorships, surveillance is an essential tool that protects the regime. This is what makes the right to privacy a pillar for FoE and freedom of opinion, and fundamental to democracy. Brazil's recent experience with dictatorship forms a key part of national identity and politics.

Rouseff then declared a "constitutional urgency" for PL 2.126/2011[19] (as authorized by the Brazilian Constitution Article 64, paragraphs 1-2). The executive order stated that if the MCI bill was not voted on "within forty-five legislative days," the rest of the legislative agenda would be stopped until the MCI was considered. Congress had been cornered, and had to provide an up or down vote on the MCI.

The Snowden leaks also energized Brazilian civil society organizations, which were already pushing for the MCI's approval. In early October 2013, various advocacy organizations launched a manifesto supporting the bill (see Marco Civil, já! 2013). Foreign organizations, such as Mozilla (Dixon-Thayer 2013), the Wikimedia Foundation and others, supported the Brazilian advocates.

Although the Snowden revelations were a key driver to move the MCI onto the congressional floor, its text as originally submitted did not contain provisions addressing digital surveillance. Before the revelations and Rouseff's support, the bill did not deal with data protection or provide any solution for jurisdictional conflict regarding the application of Brazilian laws brought by global and free-flow-based Internet architecture. These issues presented new challenges and introduced changes into the MCI, including data localization requirements in the bill as it moved to the floor — a provision later abandoned (Brito Cruz 2015, 112–15).

In addition to the complicating factor of the executive asking for data localization — a provision heavily criticized by both civil society and the business sector — the rapporteur for the MCI, House Representative Molon, had to deal with two topics responsible for significant opposition by some stakeholders (Papp 2014, 73-74). First, he had to build a compromise with the social and corporate lobbies, which asked for constant changes in the bill text, on topics such as net neutrality and copyright takedowns; second, the text needed to guarantee a series of user rights to counterbalance the shrunken AI-5 Digital and another cybercrime law, Bill n. 2.793/2011 — also known as the Carolina Dieckmann Act — related to the access and leak of personal intimate pictures. These bills were both approved into law in 2012.[20]

The battle during the final editions of the MCI focused on the takedown and intermediary liability system when copyright was at the centre of the dispute. It also required serious political sensitivity and compromise from Molon. While digital rights advocates defended the presence of text in the MCI, media and content producers companies (who are strong copyright holders in Brazil), such as Rede

18 See http://epoca.globo.com/tempo/noticia/2013/07/spies-bdigital-ageb.html.

19 Trinkunas and Wallace (2015, 26) explain that by "[u]sing her presidential powers, [Rouseff] made the passage of the legislation a matter of 'constitutional urgency,' which meant that the Brazilian Congress faced a 45-day deadline to vote on the legislation, or else it would halt all other legislative work until the bill either passed or failed. Even so, the Brazilian Congress delayed acting on the Marco Civil for six months until the eve of the NETmundial meeting."

20 On November 30, 2012, President Dilma signed the two acts popularly known as the AI-5 Digital and Carolina Dieckmann Act into federal laws n. 12,735/12 and n. 12,737/12, respectively. These laws amend and revise the Brazilian Penal Code, defining crimes committed in the digital environment and via access to information technology devices, and the counterfeiting of cards, criminalizing the behaviours with penalties of between one to five years' imprisonment and fines. The Carolina Dieckmann Act defines the counterfeiting of debit and credit cards as a criminal offence, submitting it to the same treatment imposed for the falsification of private documents. It also defines as criminal offences the violation of professional secrets, the invasion of any third-party information technology devices — including computers, notebooks, tablets, mobile phones, etc., whether connected to the Internet or otherwise — via the circumvention of security mechanisms with the aim of destroying, altering or obtaining data, or securing illegal benefits. These offences are punished with imprisonment of three months to one year and a fine. The same penalties apply to those who produce, supply, distribute, sell or deploy devices or software with the intention of permitting said illegal acts. The intentional interruption of information technology and telematic services is also defined by the act as a crime. However, since it is a crime only against public safety, this amendment will not enable attacks on private websites to be considered as a crime. The A15-Digital Act had two of its provisions vetoed. In its final text, the law established the creation and structuring of judicial police bodies specialized in combatting cybercrimes. Law accessible at www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12735.htm and www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm.

Globo,[21] were loudly against it. At the centre of the dispute was the need for a judicial order-based takedown system and the presence of copyright-related norms in the MCI, specifically in the former Article 15 of the bill. That battle was then won by the business sector[22] and an express exception was inserted in the intermediary liability article determining that copyright-based disputes were exempt from the MCI.[23] This was a loss for FoE online (Rossini 2012) and also for the assurance of due process in battles over what stays and what is taken down. Final resolution of this issue will come later, with a reform of the copyright law.

This complex, multi-front political negotiation was coordinated by Molon and his staff. In different parts of the text, he added new provisions, and publicized them as reports along the way, functioning as a "curator" of the compromises and "version control" actor, as agreements grew gradually and independently. This process was markedly different from the previous public elaboration process coordinated by the executive, in which positions were open to the public immediately after the insertion of contributions on the online platform used by that time.

Other factors also complicated the MCI in early 2014. The bill found itself in a crossfire between the federal administration and its own supporting coalition, led by Representative Eduardo Cunha. Cunha started a mini-rebellion against the executive, refusing to vote for bills supported by President Rousseff. The bill thus became hostage (or a bargaining chip) in a broader political negotiation that involved non-Internet policy issues.[24]

However, the executive and social pressure became so loud, and Molon had done such a good job of finding the compromises and the political alliances needed, that once 2.126/2011 got its moment on the floor, it was approved. And although there were compromises, the final approved text was mostly the product of the public, multi-stakeholder consultation process (Brito Cruz 2015, 116–19). Most — although perhaps not all — stakeholders saw it as a uniquely legitimate piece of law. It served as remarkable proof that a "collaborative" law-making process based on online and mostly transparent platforms — that in the MCI's case gathered thousands and thousands of comments in its different phases and through its different platforms — can affect the political environment and result in the creation of a significant new kind of law.

SECTION III: ANALYSIS — THEMATIC REMARKS ON SENSITIVE INTERNET POLICY ISSUES

FoE: Marco Civil's Flagship

The MCI expressly incorporated human rights at its core, including FoE and privacy. These rights echo the 1988 Brazilian Constitution items IV, V, VI, IX, X, XIII and XIV of Article 5 and also Article 220. These items clarify that a series of guarantees are an integral and formative part of this right, including freedom of thought and expression of thoughts, freedom of conscience and religious expression, FoE of intellectual, artistic, scientific communication and freedom of information. The MCI simply reaffirms that all those guarantees have legal force online and on Internet use in a broad sense.

FoE is a cornerstone of the MCI's framework (Thompson 2012) and serves as the foundation for Internet use in Brazil (Art. 2) and access in Brazil (Art. 8). The MCI reinforces that right in a series of other instances, first determining in Article 3º that the guarantee of freedom of speech and communication and expression of thought, in accordance to the Constitution,[25] is a core implementation and interpretation principle for Internet use and its regulations in Brazil.

Under Section III, Articles 18 and 19, the MCI creates an intermediary liability system, exempting the providers of Internet connections from civil damages resulting from third-party-generated content. It thus frees connection-providing ISPs from pressures to police data traffic as part of risk management practices. It then moves to set a clear liability system and takedown procedure applicable to

21 Globo is the number one media company in the country by several indicators. It controls many of the media markets in the country, from the major television stations to newspapers, and certainly has a level of control over the process given the economic capital it has at its disposal, its stake in the regulations and its ability to control debates about these subjects through its coverage, which is backed by its cultural and social capital as the number one source of news and entertainment in Brazil. Myriad newspapers and media companies throughout the country play similar roles, but Globo is by far the largest network of television stations, newspapers, magazines, radio stations and websites in Brazil, and the seventeenth-largest media firm in the world by revenue. Its television networks control three-quarters of the advertising revenues and more than 50 percent of market share, its newspaper has the number two circulation and its online portal is the second-most visited media site in Brazil. See ZenithOptimedia (2013). For Internet figures see www.alexa.com/topsites/countries/BR.

22 See http://blogs.estadao.com.br/link/marco-civil-recua-para-conseguir-consenso/.

23 This understanding is reinforced by Article 31 that establishes: "Until the entry into force of specific law provided for in §2º of art. 19, the liability of the [IAP] for damages arising from content generated by third parties, in case of copyright or related rights infringement, shall continue to be governed by applicable copyright legislation in force, at the time of entry into force of this Law."

24 See Papp (2014, 113–17).

25 Brazil's Constitution guarantees Brazilians broad access to information from different and multiple sources within a democratic environment where freedom of speech and the press is ensured.

application service providers (UNESCO 2012), determining that they can only be liable if, after a specific court order, no steps are taken to ban the unlawful content.

With this framework in place, the MCI protects and promotes a democratic culture where both individual liberty and collective self-governance are possible, enabling each individual's ability to participate in the production and distribution of culture (Balkin 2004). Exceptions are made for copyright and "revenge porn," wherein a court order is not required and the user's notification alone is enough to make the intermediary liable should the intermediary refuse to make the content unavailable in a short time (Brito Cruz 2015, 103).

FoE and Intermediary Liability

Liability for ICPs, such as carriers, is completely excluded by Article 18, while Article 19 establishes that application service providers will only be held liable for civil damages resulting from content generated by third parties, should they refuse to follow a court order requesting specific removal of the content. This "safe harbour" measure for intermediaries via the official establishment of a judicial notice-and-takedown framework (Spinola 2014) has clarified previously murky legal questions concerning intermediary liability, and should also prevent pre-emptive censorship by parties uncertain about their legal obligations.

From mid-2014 to early 2015, the Brazilian Superior Court of Justice (STJ) consolidated a number of precedents, ruling that, while ISPs are not responsible for pre-screening content, they are liable for complying with court-issued notice-and-takedown requests within 24 hours.[26] Failure to fulfill this requirement can result in fines and damages.[27] Accordingly, in a June 2014 case, the STJ ordered Google to compensate an Orkut user for moral damages, since the company did not immediately comply with an order to remove content.[28] Similar decisions confirmed the notice-and-takedown procedure, which was likewise strengthened by the 2014 passage of MCI legislation.[29] The Supreme Justice Tribunal ruled in March 2015 that news providers are liable for not preventively controlling offensive posts by its users.[30] Clarifying their decision, the judges held that, unlike technology companies classified as application service providers (such as Google and Microsoft), news portals have a duty to ensure that their media is not used to disseminate defilements on honour, privacy and intimacy of others, since their primary activity is providing precise information to a vast public. The judges considered this an objective case of liability, saying that news sites were providing a defective service (Art. 14, §1 of the Consumer Defense Code [CDC] and Art. 927 of the Civil Code — risk-based liability).[31] In this case, the judges applied the Consumer Defense Code and not the MCI or the logic on which other judgments had been based.

However, it is crucial to understand that all these cases were judged before needing to apply the MCI, since they started before it passed into law. An interesting case is now going to the Supreme Justice Tribunal, where the nature of content platforms may be discussed and liability might be resolved on the basis of the editors' behaviour; so if a news portal actively edits and deletes comments, there might be a higher propensity to liability, compared to a case where there is no editing by the news portal owner (Antonialli, Brito Cruz and Valente 2015).

Intermediaries exercise a bigger or a smaller police power — interfering more or less on FoE and other human rights — based on the liability risk they might face under a certain jurisdiction. The MCI makes clear when an intermediary is responsible or not, and if there is a risk, the steps that need to be taken to avoid that liability. The intermediary liability system makes the MCI consistent with international human rights norms, specifically the right to FoE and its corollary rights to seek and receive information. However, the March 2015 decision poses a challenge for FoE online that is not solved by the MCI, which deals with ICPs and IAPs, not content providers (such as online newspapers). It remains to be seen if this will be addressed by the law under development as of June 2015.

Privacy: Between Data Protection and Data Retention

The MCI treats privacy and data protection as fundamental rights, applying the constitutional provision of Article 5º, items X and XII to Internet use in Brazil. Art 3º of the MCI mentions privacy (Art. 3º, II) and data protection (Art. 3º, III) separately, setting clear differences in their scope. This approach was inspired by the European Union's Charter

26 STJ, Appeals to the Superior Court No. 1501187 / RJ (December 16, 2014), 1337990 / SP (August 21 2014); Interlocutory Appeals No. 484995 / RJ, 1349961 / MG (September 16, 2014), 305681 / RJ (September 4, 2009).

27 STJ, Appeal to the Superior Court No. 1337990 / SP (August 21, 2014). See also STJ, Interlocutory Appeals No. 1349961 / MG (September 16, 2014), 305681 / RJ (September 4, 2014).

28 STJ, Appeal to the Superior Court No. 1337990 / SP (August 21,2014), available at ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201102765398&dt_publicacao=30/09/2014.

29 STJ, Interlocutory Appeal No. 225.088–RS, September 9, 2013, available at ww2.stj.jus.br/revistaeletronica/ita.asp?registro=201201857568&dt_publicacao=09/09/2013.

30 See http://blogs.estadao.com.br/deu-nos-autos/o-futuro-dos-comentarios-de-internet/.

31 See www.procon.sp.gov.br/texto.asp?id=745.

of Fundamental Rights,[32] in which they are also mentioned in different articles (Arts. 7º and 8º).

The initial drafts of the MCI did not deal with privacy protection and data retention at length. However, this changed after the Snowden revelations, when government representatives, as a reaction, pushed for specific data protection and privacy implementation rules. The version that passed into law in April 2014 contains lengthy privacy and data treatment related provisions as a result, although Brazil continues to publicly consult on a specific data protection law as of June 2015.

The privacy provisions in the MCI can be classified in three main groups: principles and users' rights; specifications for log retention; and access to personal data. The MCI does not specifically define personal data — a task being done by the data protection bill — but covers a set of user-related data protected or regulated under the statute. Article 5º of the MCI specifies a series of definitions, notably connection records and logs as the set of information pertaining to the date and time of the beginning and end of a connection to the Internet, the duration thereof, and the Internet Protocol address used by the terminal to send and receive data packages.

Article 3º sets protection of privacy and protection of personal data, while Article 7º specifies the actions protected and regulated. For general privacy, Article 7º clarifies privacy protections guaranteed for Internet use, including: the inviolability of intimacy and private life, that the right for protection and compensation for material or moral damages resulting from their breach is safeguarded (Art 7º, I); the inviolability and secrecy of the flow of users' communications through the Internet, except by court order, as provided by law (Art. 7º, II); and the inviolability and secrecy of users' stored private communications, except upon a court order (Art. 7º, III).

For data retention, Art. 7º, VII decrees that access to the Internet is essential to the exercise of citizenship, and guarantees as a core user right the non-disclosure to third parties of users' personal data, including connection records and records of access to Internet applications, unless with express, free and informed consent. Art. 7º, VIII, IX and X[33] lay out guarantees and protections when any form of data collection is performed in a connection or application service provision.

Both articles clarify that these cases are "pursuant to law," setting the stage for further regulation and enforcement mechanisms in those cases where the MCI is not explicit. This indicates that a new statute — specifically, a decree issued by the presidency — will be responsible for regulating aspects of privacy, data protection and usage.

Article 7, VI — read in conjunction with VIII — mandates that providers make privacy policies, or any terms of use applicable to personal data, clear and understandable. This is particularly important given the fact that consumer law often applies to personal data used on the Internet.[34]

Finally, in Article 8º, the MCI voids contractual clauses in breach of the guarantee to the right to privacy and FoE in communications, as a condition for the full exercise of the right to access to the Internet. It names two cases, including clauses on the inviolability and secrecy of private communications over the Internet (Art. 8, I) and, in adhesion contracts, clauses that do not provide an alternative to the contracting party to adopt the Brazilian forum for resolution of disputes arising from services rendered in Brazil (Art. 8, II).

The MCI sets its jurisdiction regarding data privacy and retention in Article 11, and goes beyond Brazilian territory to also establish that its rules apply whenever a service is offered to Brazilian citizens. The MCI, in this sense, adopted the "targeting theory" for asserting its legal jurisdiction.[35] That was the compromise reached in exchange for not requiring data "localization" (requiring servers containing data on Brazilian citizens to be placed in Brazil).[36] Thus, a company is bound by Brazilian law when its marketing or services are directed to Brazilians.

Mandatory data retention and privacy regulation obligations begin with the collection and storage of user data by connection providers and Internet applications. The MCI does not specifically define personal data in Article 5º, but it is understood that protected personal data may refer to information such as time, duration, location, Internet Protocol address, connection data, browsing data and more. These data — commonly referred to as metadata — indicate not only usage of telecommunications and Internet connection services, but often enable individual

32 See http://ec.europa.eu/justice/fundamental-rights/charter/.

33 See www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf.

34 Decree 7.962 of 2012 establishes as mandatory the easy and meaningful communication of any relevant characteristic or restriction of the service to the consumer.

35 See www.britcham.com.br/download/040614_3.pdf. This theory is also adopted in Europe, see www.hldataprotection.com/2012/11/articles/international-eu-privacy/recent-ecj-decision-embraces-targeting-theory-of-jurisdiction/.

36 That now historic article provided: "The Executive branch, through Decree, may force connection providers and Internet applications providers provided for in art. 11, who exercise their activities in an organized, professional and economic way, to install or use structures for storage, management and dissemination of data in the country, considering the size of the providers, its sales in Brazil and breadth of the service offering to the Brazilian public." Projeto de Lei n. 2126 de 2011 [Draft Law No. 2126 of 2011], translated by Carolina Rossini (November 14, 2013). For possible fragmentation effects of such provision see Chander and Le (2014).

identification of users, since they reveal intimate aspects of usage. ICPs are obliged to keep connection data for at least one year (Art. 13), while IAPs are obliged to keep application access and use data for at least six months (Art. 15). The police or public prosecutor office can — preventively — request that providers keep data logs for a longer period in case of specific investigations (Art. 13 §2 and Art. 15 §2).

Mandatory data retention of user data and metadata is an obligation of both ICP services and IAP services, regardless of whether a user is part of an ongoing investigation or not. Additionally, connection providers are prohibited to track and collect data of user's access to Internet applications as a proportional measure to user's privacy (Art. 14). Internet application services will perform that collection, as explained later on.

This bulk collection has been highly criticized in Brazil and elsewhere, and has inspired questions of its legality under the Brazilian Constitution. According to its critics, there remains little to no empirical evidence from public authorities about the difficulty of pursuing investigations in the absence of such broad collection data. In any case, the MCI makes it clear that the data stored must be used only in accordance to the law, while the logs stored must only be disclosed upon judicial order.

However, Article 10 §3 establishes a major exception: in certain situations, personal data can be requested by an administrative authority — the police and public prosecutor for instance — without a judicial warrant. Not all personal data is subject to this kind of request, only "personal qualification, affiliation, and address." This is a clear application to a provision from Law 12.683 of 2012, regarding money laundering and its investigations. As the provision is an exception, its interpretation must take into account the limits to the requisition of personal data set in Law n. 12.683 of 2012, which narrow the access to data that is only vital for specific ongoing investigations. Thus, even if this provision is a fundamental exception in the MCI, it is neither a general nor a multi-purpose exception.

Companies must also permit practice-compliance inspections. The MCI does not specify who is the authorized inspector, instead anticipating a decree to address the issue. Article 12 lists sanctions for non-compliance with data retention provisions (and other obligations created by the MCI) from warning, corrective measures and fines, suspension, and prohibition of activities involving data retention. Foreign companies are subject to the sanctions, which can also be imposed on their Brazilian subsidiaries.

Measures of data retention by application service providers are specified further in Articles 15, 16 and 17. Under Article 15, only for-profit legal entities are bound to the provisions, and a judicial order is the only way to request access and disclosure of logs to authorities. Article 17 exempts application providers from liability for third-party damages if data are not retained beyond the obligations set in Articles 15 and 16.

The principles of proportionality (measuring importance of the data requested and its importance to the investigation) and specification (regarding the limitations of the time period the data requested refers to) form important constraints on potential data abuse. Under Article 23 of the MCI, when issuing an order, a judge must take any necessary precaution to assure the privacy of the individuals affected by the disclosure of the data. This provision also includes the possibility to decree secrecy of justice, including to the requests for record retention.

An Enabler Element: Net Neutrality

Of all the provisions of the MCI, network neutrality exposed most clearly some innate tensions between the private sector and the public interest community. The text that passed into law has adopted both a broad net neutrality framework and a narrower framework. According to this broader framework, which says that the preservation and guarantee of network neutrality is a core principle for the discipline of Internet use in Brazil, net neutrality contributes to the enjoyment of a wide range of fundamental rights, such as preserving the open, general-purpose Internet architecture, fostering decentralized innovation, and promoting the Internet's potential to expand people's capabilities on social, cultural and political domains and its ability to protect autonomy and FoE. This broad framework then works as a fundamental cornerstone to a narrower framework in Article 9, where discrimination, antitrust and market concentration play a leading role for norms interpretation and enforcement (Van Schewick 2012).

The net neutrality mandate sits inside Article 9, where ISPs — the party that is responsible for the transmission, switching or routing — are obliged to treat all data equally, without discrimination by content, origin, destiny, content, platform or application. Although it does not solve all net neutrality questions, it remains one of the great civil society victories of the MCI process.

The net neutrality rule resembles many regulations in force across South America, including in Colombia, Chile and Peru,[37] in recognizing a general non-discrimination obligation and strict technical exceptions. However, the MCI leaves for future regulation a complete meaning for technical exceptions:

- §1º The discrimination or degradation of traffic shall be regulated in accordance with the private attributions granted to the President by means of Item IV of art. 84 of the Federal Constitution aimed at the

37 See www.thisisnetneutrality.org/beta/#map_wrap.

> full application of this Law, upon consultation with the Internet Steering Committee and the National Telecommunications Agency, and can only result from:
>
> — I. technical requirements essential to the adequate provision of services and applications; and
>
> — II. prioritization of emergency services.

Article 9 also determines how ISPs must act when practising exceptions to the general net neutrality rule. For instance, when discriminating or degrading traffic as a consequence of the exceptions allowed, ISPs must refrain from harming users, act with proportionality, transparency and isonomy, deploy mitigation measures and provide an advance notice to users of the exceptional practices. It also requires that services offered in periods and conditions when exceptions are in place must be offered in a non-discriminatory and pro-competitive manner. Finally, the rule bans filtering and monitoring of online communications, preventing ISPs from applying deep packet inspection[38] or similar methods.

Under Article 24, when public authorities — including the federal government, states, federal district and municipalities — are the actor promoting optimization of network infrastructures and implementation of storage, the management and dissemination of data centres in the country, the technical quality, innovation and the dissemination of Internet applications, they have to do no harm to openness, neutrality and participation. However, the meaning of openness, neutrality and the participatory nature of the Internet remained disputed during the public consultations. The entry of Internet.org in Brazil has illustrated the murkiness of these issues.

The Role of Public Authorities in Fostering the Discipline of Internet Use in Brazil

Another advancement of the MCI was the reconfirmation that access to the Internet is a right for all citizens. The law further clarifies the role of the public sector in fostering Internet development in Brazil based on the principles set by Article 4. Thus, in addition to diversity of policies, norms and regulations in Brazil specifically focused on infrastructure development and access provision — including the telecommunications law, the Brazilian Broadband plan and a set of regulations and incentives to the development of mobile Internet in Brazil[39] — the MCI determines guidance principles for the following government acts:

- muti-stakeholderism, based on a democratic, transparent and cooperative participation (Art. 24, I);
- expansion of Internet use in Brazil, supported by CGI.Br (Art. 24, II);
- interoperability for e-government, to allow for better flow of information and celerity of procedure (Art. 24, III);
- interoperability of public and private networks and services (Art. 24, IV);
- preference for open and free technologies and standards (Art. 24, V), reconfirming the national preference for free software;
- access to public information (Art 24., VI);
- optimization and management of networks and storage innovation and stimulus for implementation[40] of data centres in Brazil (Art. 24, V);
- education for Internet use (Art. 24, VIII);
- promotion of culture and citizenship (art. 24, IX); and
- inclusive provision of public services through the Internet (Art. 24, X).

Articles 26 and 27 go further, guiding the government to foster Internet culture and education based on secure Internet use, as well as digital inclusion, innovation and access to digital public services for all, including those in remote areas. Article 25 sets accessibility guarantees.

What Remains Missing?

Implementation of the MCI

Although the MCI is law in Brazil, some of its provisions lack granular regulation, which can reduce

38 See https://en.wikipedia.org/wiki/Deep_packet_inspection.

39 Brazil, which was first connected to the Internet in 1990, has enacted a handful of initiatives in recent years to expand and enhance broadband and mobile phone usage. With programs ranging from tax incentives for suppliers of ICT, to the installation of LAN houses (public and private Internet access points) throughout the country, to policies fostering Internet use in public schools, to the introduction of 4G services in April 2013, Brazil is making concerted efforts to facilitate continued investment in infrastructure and to increase the number of citizens with Internet access. However, the Center of Studies on Information and Communication Technologies (CETIC.Br) found that almost 60 percent of Brazilian residences lack Internet access due to various obstacles, such as high prices, limited availability of services, and persistent social inequalities. See Freedom House (2012–2014 editions) at https://freedomhouse.org/report/freedom-net/2013/brazil#.VYdjlBNViko, and CETIC.Br at http://cetic.br/pesquisa/domicilios/.

40 In this regard, a regulation by the Treasury (Receita Federal) establishing a higher tax for data centres hired by Brazilian companies in foreign lands. See http://computerworld.com.br/negocios/2014/10/22/governo-crava-50-de-imposto-em-servicos-de-dc-prestados-do-exterior.

its scope or enforcement until those are further clarified. Implementation of the MCI has proven to be as complex as the negotiation of the original texts.

After the MCI passed into law, the first task was to craft a regulatory decree, to be created and signed directly by the presidency, in consultations with bodies such as the National Telecommunications Agency (Anatel) and CGI.Br. Article 24, as discussed above, also determined that any upcoming regulation should pass through a multi-stakeholder filter. Later in 2014, inspired by the original bill creation process, the Ministry of Justice provided a platform to support the discussions of a text for the decree. The online debate was designed around four main topics: net neutrality, privacy, data retention and a general "catch-all" category." Anatel and CGI.Br also developed public consultations that fed into the Ministry of Justice consultation.

The network neutrality discussion gathered the most participation and controversy.[41] The allowance of zero rating under the MCI has proven to be one of the most difficult disputes, and the announcement of a possible partnership between Facebook and the Brazilian government to launch Internet.org in Brazil only fed the stakeholder debates.[42]

As of April 30, 2015, 1,772 inputs had been sent by stakeholders to be curated and consolidated by the Ministry of Justice.[43] A comprehensive mapping of arguments and recommendations was done by the Brazilian research centre, InternetLab, which indicates over 20 important regulatory issues that need to be addressed.[44] The Ministry of Justice is currently drafting the decree based on this online debate, which is expected to be published in 2015.

The Role of the Judiciary Branch

Following approval of a law, judges play a key role in defining standards of interpretation for the law's provisions. However, Brazil follows a civil law tradition, and thus court decisions, while providing some clarification and lines of interpretation, are not binding in regard to future cases as they would be under a case law tradition. An interpretation would only bind if used in the Brazilian Supreme Federal Court (on constitutional issues) or the Superior Court of Justice (when regarding the uniform application of federal law provisions). These courts resolve different court decisions when results are in contradiction.

Since the expansion of the commercial Internet in Brazil in the 1990s, a series of Internet-related cases have reached Brazilian courts. Before the MCI approval, the scene featured some radically different decisions resulting from Judiciary branch struggles to create rules about topics such as intermediary liability and data retention, two of the most disputed issues in Brazil. The decision that blocked YouTube[45] stands as one such radical case, one apparently contrary to the MCI. In the case, the São Paulo Court of Appeals blocked local access to YouTube by ordering ISPs to suspend the connections between final users and YouTube's servers. The decision emerged from civil litigation in which a model was trying to block paparazzo footage of her and her boyfriend allegedly having sex on a European beach.

The variety of decisions across the country demonstrate a scattered and heterogeneous legal landscape (Brito Cruz 2015 20)[46] before the MCI. Its approval clarified and unified the parameters to guide the judiciary work moving forward when deciding Internet-related cases. But it still faces a challenge of being applied by judges who had completely different understandings about similar cases before the law. Two other very different decisions are worth mentioning due to their notoriety and because they exemplify this space before an enforceable MCI.

The first decision was to block the Secret app in August 2014. Secret was a mobile application that allowed users to share anonymous posts with followers. It was a huge success in Brazil just after the approval of the MCI. For months, the app was largely used among teenagers, raising bullying and child pornography questions. The Espirito Santo State Prosecution Office filed a lawsuit to block the app (Etherington 2014), arguing that it was illegal since the Brazilian Constitution forbids anonymity on expression. The prosecution office succeeded in granting an injunction to ban the app from the iTunes Store and Google Play in Brazil. The Electronic Frontier Foundation commented that "this high-profile case points to a potential danger

41 For more information about the public consultation process and a description of the most commented topics, see the InternetLab series of reports about the issue at www.internetlab.org.br/en/blog/internetlab-reports/. The network neutrality regulation was, by far, the most controversial topic according to this debate mapping initiative.

42 For more information about the Internet.org initiative recent moves, see www.internetlab.org.br/en/opinion/internet-org-platform-raises-new-questions-on-the-debate-about-zero-rating-and-the-digital-divide/.

43 For a more accurate participation profile, see www.internetlab.org.br/en/internetlab-reports/internetlab-reports-public-consultations-no-13/.

44 See www.internetlab.org.br/wp-content/uploads/2015/08/Report-ILABReportsMCI2.pdf.

45 Injunction order concealed during the judgement of the case N. 583.00.2006.204563-4, São Paulo Court of Appeals, by Judge Enio Zuliani.

46 Some sectors of the judiciary tried to consolidate or uniformize the case law, such as Justice Nancy Andrighi of the Superior Court of Justice (REsp 1.306.066, REsp 1.175.675, REsp 1.192.208, REsp 1.316.921 e REsp 1.323.754). Andrighi suffered opposition in her position from some state courts such as São Paulo and Minas Gerais (TJ-SP: Apelação Cível n. 431.247-4/0-00, da 8ª Câmara de Direito Privado, em 22/03/2007. TJ-MG: Apelação Cível n. 1.0439.08.085208-0/001, da 13ª Câmara Cível, em 16/03/2009).

of broadening the scope of the constitution's prohibition and applying it to prevent the use of privacy enhancing technologies, which would also bring undesirable repercussions to the rights of reading and browsing anonymously" (Pinho and Rodriguez 2015). The Secret decision might also prevent challenges to business innovation in Brazil, sitting as a guidance principle for the actions of the government and public authorities (Art. 24, VII).

The second decision involved a child pornography investigation in Piauí state. The presiding judge sent an order to the messaging service WhatsApp, which now is part of Facebook, to disclose information relevant to a police investigation. After receiving no answer, the judge, referring to Article 11 of the MCI, ordered the service suspended nationwide. This attempt to enforce Brazilian jurisdiction backfired, and millions of users spent days worrying that one of the country's leading messaging services would be completely blocked. The decision was reversed after a few days of national uproar, but it suggests possible (and unforeseen) chilling effects of MCI enforcement.

There was a real sense that the decision contradicted the MCI's spirit and guiding principles set for Internet use and development in Brazil; however, the judge applied the MCI in compliance with Civil Procedure Code rules to impose the obligation to ISPs to suspend the connection of users with WhatsApp servers. Then a review by the STJ, while agreeing that the blockage of WhatsApp (based on the sanctions of Art. 12 for the disobedience of Art. 11 of the same statute) was not unlawful, declared it actually disproportionate and thus reversed it. This hints at the power of a La Rue-style three-step analysis that includes concepts such as proportionality.

Such decisions show the MCI it is not the only Internet legislation, but actually part of a broader framework of laws and policies in force or under debate in Brazil. Thus, although the MCI advances the normative and interpretative tools available for the judiciary, this new framework does not automatically mean that interpretations will be uniform, nor that a principles- and human rights-oriented vision and actions will be applied by judges from Oiapoque to Chui.[47] The judiciary bears the burden of taking the advanced framework of rights and principles approved by Congress and consolidating human rights-centred legal understandings and decision-making rubrics.

The Data Protection Bill[48]

On January 28, 2015, the Brazilian Ministry of Justice issued the preliminary draft bill for the Protection of Personal Data (Anteprojeto de Lei para a Proteção de Dados Pessoais) on a website created for public debate.[49] In 2010, a previous version of the bill was also submitted to a public debate on Internet. The new draft is a result of the comments gathered on the first debate and the historical developments on the subject following the passing of the MCI.

The draft bill applies to individuals and companies that process personal data via automated means, provided that either the processing occurs in Brazil, or personal data was collected in Brazil. The draft bill would impose data protection obligations and requirements on businesses processing personal data in Brazil, including:

- a requirement to obtain free, express, specific and informed consent to process personal data, with limited exceptions. For example, consent is not required if the personal data is processed to either comply with a legal obligation, or implement pre-contractual procedures or obligations related to an agreement in which the data subject is a party;
- a prohibition on processing sensitive personal data, except in limited circumstances. For example, sensitive personal data may be processed with the specific consent of the data subject after the data subject has been informed of the risks associated with processing the sensitive personal data. Sensitive personal data includes, among other information, racial and ethnic origins, religious, philosophical or moral beliefs, political opinions, health and sexual orientation information, and genetic data;
- an obligation to immediately report data breaches to the relevant authority;
- a requirement to allow data subjects access to their personal data and correct it if it is incomplete, inaccurate or out-of-date, with limited exceptions;
- a restriction from transferring personal data to countries that do not provide similar levels of data protection; and
- an obligation to adopt information security measures that are proportional to the personal data processed and protect the information from unauthorized access, destruction, loss, alteration, communication or dissemination.

47 An expression used to refer to the most remote areas in Brazil between the extreme north and extreme south of the country.

48 For more details of the public consultations of the data protection bill and the trends and compromises emerging, see www.internetlab.org.br/en/tag/data-protection, which provides periodic updates of the process.

49 See http://dadospessoais.mj.gov.br/.

The draft contains penalties for violations, including fines and the suspension or prohibition of processing personal data for up to 10 years. Participation in the discussion is open to the public and comments on the draft bill may be submitted on the website.

Several controversial aspects of the bill were highlighted by comments submitted during the public consultation, such as the definition of anonymous data and their relationship to the law. This issue came out after some commentators argued that a data protection bill should not apply to anonymous data, with others arguing that de-anonymization attacks are known to be effective and thus even "anonymous" data must be also covered.[50]

Another popular issue in the public consultations was the nature of the user's consent. User consent in the draft data protection bill was proposed as a strong concept — it should be free, explicit and informed. Some commentators argued that this is more idealistic than realistic, and that on some occasions a person's will would be better recognized by indicators such as the context of a given situation in which someone is disclosing its own data. The Ministry of Justice is working to consolidate and curate the stakeholders' input provided by July 5, 2015, promising progress and, it is hoped, clarity on the topic.

Copyright Law Reform

In December 2007, the Brazilian Ministry of Culture under Gilberto Gil's leadership started the National Copyright Law Forum, a series of seminars across the country with the participation of lawyers, researchers, artists and industry representatives, with the goal of gathering information and paving the way for a copyright reform process. Based on these events, a series of testimonies to Congress and other closed and open meetings with different stakeholders, the Ministry of Justice prepared a draft copyright reform bill, which was submitted to public consultation in 2010.

The consultation took place in an online platform,[51] similar to that used for the MCI consultation on Internet regulation. More than 8,000 contributions were submitted. The end result was considerably superior to the current law, featuring greater attention to public interest issues, an expanded list of copyright exceptions,[52] permission to circumvent digital rights management/technical protective measures in certain conditions, checks on the collective management of copyright (a serious problem in Brazil), and an explicit recognition that copyright may be limited by consumer protection law, antitrust law and human rights.

After a series of political setbacks, Bill 3133/2012[53] went through a new round of modifications, and, in 2014, a new text was finalized by the office of the president's chief of staff and was ready to be sent to Congress.[54] However, this bill — the text of which was leaked later that year — is not yet officially public. In early 2015, the new minister of culture, Juca Ferreira, reaffirmed his commitment to the reform.[55]

Copyright reform is a crucial step in clarifying issues such as exceptions and limitations to copyright in an online environment, what society will accept regarding copyright enforcement and the consequences of copyright infringement. The reform will address the intermediary liability issue in the copyright infringement context — an issue the MCI abandoned before its approval; however, its path to becoming law remains a long one.[56]

50 This debate is available on the discussion around the Art. 5º, IV of the Brazilian Data Protection Draft Bill available at http://dadospessoais.mj.gov.br.

51 See www2.cultura.gov.br/consultadireitoautoral/.

52 See http://infojustice.org/archives/26900.

53 See www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=534039.

54 See www.creativecommons.org.br/blog/copyright-week-en/.

55 See www.teletime.com.br/12/01/2015/juca-assume-com-promessa-de-reforma-na-legislacao-de-direito-autoral-e-de-incentivos/tt/401348/news.aspx.

56 "A concerning last-minute change has chipped away at the Bill's safe harbor provisions regarding copyright infringement. Article 15 of MCI originally provided that ISPs are not responsible for infringing content by Third Parties unless they disobey a specific judicial order to take down said content. However, following a visit by the Minister of Culture to the legislator serving as rapporteur of MCI, the rapporteur introduced a new paragraph into Article 15, saying that the article would not apply in cases of 'copyright and neighborhood rights'" (Rossini 2012).

SECTION V: APPLYING FRANK LA RUE'S HUMAN RIGHTS FRAMEWORK — SUCCESSES AND SHORTCOMINGS OF THE MCI

This section applies the Frank La Rue framework as structured by the APC (see Annex I) to the MCI text. Author comments are included to provide context to some in-focus issues.

La Rue Framework Standard	Is it addressed by the MCI? How?
National constitution or laws protect Internet-based freedom of expression (FoE).	Both the Brazilian Constitution and the MCI guarantee FoE. FoE appears in MCI in: Art. 2º; Art. 3º, I; Art. 8º; Art. 18; Art. 19 §2.
Comment: Refer to Section III, "FoE: Marco Civil's Flagship" and "FoE and Intermediary Liability" for an in-depth analysis.	
State participates in multi-stakeholder initiatives to protect human rights online.	The MCI consolidates the practice as a policy-making guideline for Internet development in Brazil. Art. 24, I sets that the government shall establish mechanisms of governance that are multi-stakeholder, transparent, cooperative and democratic, with the participation of the government, the business sector, civil society and the academia.
Comment: The Brazilian Internet Steering Committee has practised multi-stakeholderism for almost 20 years. Originally created in 1995, it is a multi-stakeholder organization composed of representatives of government ministries and agencies, businesses, civil society and the scientific community. There are 21 members in all, 12 from the private sector and 9 from government.[57] Brazil has been experimenting with multi-stakeholderism in a series of policy-making processes, with the "open-to-participation-by-any" platform e-Democracia[58] as infrastructure. A series of laws have been debated with the public through this platform. Multi-stakeholderism was also consecrated in the final principles coming out of the NETmundial meeting in April 2014 in Brazil.[59] However, further research is needed to map and understand the success of the Brazilian model in each and all of the instances where multi-stakeholderism has been applied. The authors suggest that some crucial factors be used, including measures of: inclusiveness, transparency, accountability, legitimacy and effectiveness (Gasser, Budish and Myers 2015).	
There are no generic bans on content.	The MCI does not have any generic ban provision regarding content.
Comment: The MCI has deep foundations in protecting FoE. There is no generic provision to ban content in the Brazilian legislation or Constitution. Brazil does, however, ban certain forms of speech if they are related to hate crimes. So, despite a constitutional principle of FoE and its reaffirmation within the MCI, Brazilian lawmakers and law enforcement have drawn the line[60] when it comes to agitating racial, religious or ethnic tensions.[61] Brazil also criminalizes acts of prejudice (and related speech) against its senior citizens.[62]	
Sites are not prohibited solely because of political or government criticism.	The MCI does not bring bans on sites because of political or government criticism. However, *offendees* possibly can use the mechanism in Art. 19 to take down critical content, if the criticism is considered a crime of honour, such as defamation or libel (Art. 138, 139 and 140 of Penal Code).
Comment: The MCI foresees the need for a court order in any action for content takedown. As Brazil is a champion of personality rights-related takedowns, based on the Google Transparency Report,[63] the hope is that judges will provide a court order in fewer cases, since the MCI mandate may block persecution for government criticism. Constitutional safeguards do protect government criticism in Brazil, although Brazilian Electoral Law regulates and restricts speech during the electoral period,[64] with the goal of ensuring trustable information to citizens about candidates. In 2013, Freedom House reported that while "there is no evidence of the Brazilian government employing technical methods to filter or otherwise limit access to online content…it does frequently issue content removal requests to Google, Twitter, and other social media companies. Such requests increased in 2012 ahead of Brazil's municipal elections, with approximately 235 court orders and 3 executive requests requesting Google to remove content that violated the electoral law."[65]	

57 See /www.cgi.br/publicacao/internet-governance-in-brazil-a-multistakeholder-approach/.

58 See http://blog.openingparliament.org/post/60749859717/case-study-5-brazils-e-democracia-project. Besides allowing multi-stakeholdersim participation, the e-Democracia platform is also part of Brazil's open government efforts. See http://blog.openingparliament.org/post/66000066598/legislative-openness-working-group-launched-at-ogp.

59 See www.netmundial.org/principles.

60 See changes introduced in the late 1990s in the Brazilian Penal Code at www.planalto.gov.br/ccivil_03/leis/l9459.htm.

61 See, for instance, www.csmonitor.com/World/Americas/2012/1204/Watch-your-tongue-Prejudiced-comments-illegal-in-Brazil.

62 In Brazil it is a crime to "despise, humiliate, belittle or discriminate any elderly person, for whatever reason." See Artigo 96, Lei 10.741/2003. www.planalto.gov.br/ccivil_03/leis/2003/L10.741.htm.

63 See www.google.com/transparencyreport/removals/government/BR/.

64 Campaigning is confined to a three-month period, and there are restrictions on how and where political advertising can appear. The law also specifically protects political candidates from content that would "offend their dignity or decorum." See www.cjr.org/cloud_control/brazilian_takedown_requests.php?page=all.

65 See https://freedomhouse.org/report/freedom-net/2013/brazil#.VYhqFRNViko.

La Rue Framework Standard	Is it addressed by the MCI? How?
State blocks or filters websites based on lawful criteria.	Art. 19 determines that IAPs "make unavailable the content that was identified as being unlawful, unless otherwise provided by law." IAPs shall act based upon a court order, also mandated in that article.
Comment: Refer to Section III, "FoE: Marco Civil's Flagship" and "FoE and Intermediary Liability" for further details on FoE and intermediary liability.	
State provides lists of blocked and filtered websites.	This is a shortcoming of the MCI. It does not create any statutory obligations to the state to release lists of blocked websites or Internet applications.
Comment: Despite the non-existence of a government mandate in the MCI for listing blocked sites, citizens can use the mechanisms of the Brazilian Access to Information Act to request the information. State and federal court decisions are also available via the courts' websites, if secrecy is not imposed. Brazil has also launched a series of related transparency commitments as part of its open government efforts.[66]	
Blocked or filtered websites have explanation on why they are blocked or filtered.	Refer to Arts. 19 and 20 of the MCI.
Comment: Most court decisions are available to the public via the courts' websites. Additionally, Art. 20 mandates the IAP to notify the user responsible for the content, when the IAP has that user's contact information, and inform the user about the execution of the court order with information that allows the user to legally contest and submit a defence. The user can request the for-profit IAPs to replace the content made unavailable with a note "available to the public with the explanation for the take down" or with the text of the court order that gave grounds to the unavailability of the content.	
Content blocking occurs only when ordered by competent judicial authority or independent body.	This is a partial success. While a court order is a general mandate as noted, Article 19, § 4º [67] sets exceptions, increasing the risk of intermediary liability for copyright issues (which continues without a specific intermediary liability model and awaits the copyright reform) and also for those cases of "revenge porn" as per Art. 21, in which a court order is not necessary and the content must be taken down immediately upon any form of notice.
Comment: Refer to Section III, "FoE: Marco Civil's Flagship" and "FoE and Intermediary Liability," and Section IV, "Copyright Law Reform" for further details on FoE and intermediary liability.	
Blocking or filtering of online content is connected with offline national law enforcement strategies focused on those responsible for production and distribution of content, including child pornography.	The MCI deals with intermediary liability from Arts. 18–21. Other laws, including the Brazilian Penal Code and the Child and Adolescent Statute, determine what is a crime.
Comment: The Child and Adolescent Statute punishes the "presentation, production, sale, supply, disclosure, or publication, by any means of communication, including the Internet, of photographs or images of pornography or sex scenes involving a child or an adolescent is punished with up to six years in prison and a fine" (Art. 241). Under the scope of this article, law enforcement agencies (federal and state prosecutors and police) and other government bodies produce strategies against the crime.[68] The 2013 National Plan to Combat Sexual Violence against Children and Adolescents (CONANDA 2013) dedicates special attention to those responsible for production and distribution of content. The plan coordinates institutional tactics within different spheres of the public service. The Office of the Public Prosecutors has signed memorandums of understanding with ISPs since the early 2000s, laying out a series of best practices to combat and police these crimes.	
Defamation is not a criminal offence.	The Brazilian Criminal Code establishes that defamation is a minor criminal offence. The MCI's intermediary liability framework created a notice and takedown system to deal with cases of defamation, slander and libel.
Comment: Over the years, civil society organizations have protested abuses of defamation, with Freedom House and the international non-profit organization Article 19 tracking its use in Brazil and beyond. Specifically, Article 19 commented: "The 'honour crimes' of slander and libel, and contempt are used in Brazil as a political instrument of intimidation, and go against the standards set by the Inter-American Commission on Human Rights, which has repeatedly stated that the best solution for defamation and contempt is civil, not criminal remedies." The organization Article 19 has noted that "the penalties provided for in cases of defamation and contempt in Brazil — three months to two years' imprisonment plus a fine — are disproportionate and incompatible with the recommendations of international human rights bodies" (Article 19 2013).	

66 See www.opengovpartnership.org/country/brazil.

67 "In order to ensure freedom of expression and prevent censorship, the provider of internet applications can only be subject to civil liability for damages resulting from content generated by third parties if, after an specific court order, it does not take any steps to, within the framework of their service and within the time stated in the order, make unavailable the content that was identified as being unlawful, unless otherwise provided by law."

68 One example is the Intersetorial Commission to Combat Sexual Violence against Children and Adolescents, led by the Human Rights Office of the Presidency.

La Rue Framework Standard	Is it addressed by the MCI? How?
Journalists and bloggers are protected against abuse or intimidation.	The MCI does not specifically address this issue.
Journalists and bloggers are not regularly prosecuted, jailed or fined for libel.	The MCI does not specifically address this issue.
Journalists, bloggers and Internet users do not engage in self-censorship.	The MCI does not specifically address this issue.
Comment: The MCI does not specifically address these issues, but does provide for FoE as a core principle of the use of the Internet in Brazil, as noted in Section III of the paper. The MCI also secures due process regarding certain kinds of content takedown. Brazil has a specific law to regulate and protect the press, but the legal context cannot be considered sufficient to protect these actors. Freedom House reports have pointed to many cases of abuse, intimidation, persecution and possible eventual self-censorship by journalists and bloggers in Brazil. Due to the cases identified, Brazil was considered "partially free" in the 2014 Freedom of the Press report (Freedom House 2014). Notwithstanding the killings of five journalists in 2013, Brazil is no longer ranked by Reporters Without Borders among the world's five deadliest countries for media personnel (Reporters Without Borders 2013).	
National security or counterterrorism laws restrict expression only where the expression is intended to incite imminent violence, it is likely to incite such violence and there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.	The MCI does not address national security issues.
Comment: Brazil is regulating these state activities through a national strategy on cyber security. Based on a recent publication by Igarape Institute, although organized crime is a major threat to Brazilian cyberspace, resources are focused instead on military solutions better suited to the exceptional case of warfare (Diniz, Muggah and Glenny 2014). For now, due process should be observed by both criminal and civil courts. A multi-stakeholder debate was called for to further develop national security and counterterrorism in a cyber context. In this debate, civil society agents have suggested the inclusion of the Necessary and Proportionate principles (Electronic Frontier Foundation and Article 19 2014).	
State does not delegate censorship to private entities.	The MCI establishes, in Art. 19, a procedure where content removal (in general) is dependable on a judicial court order and, thus, a certain grade of state accountability.
Comment: FoE is a core principle of the MCI. For a takedown of content, the MCI established a notice and takedown procedure similar to the US Digital Millennium Copyright Act. Due to the youth of the MCI and the few cases as yet adjudicated, it is hard to foresee all the consequences of this process. However, one concern is the lack of specific regulation regarding takedown notices for copyright infringement, an issue that was to be later decided within the copyright reform. Also, Brazil has not yet adopted any regulation regarding the "Right to be Forgotten" (or more precisely, de-listed). A bill with only two articles (PL 7881/2014)[69] was proposed by one of the MCI's core opposition — House Representative Eduardo Cunha — but has not yet gathered enough support to be a candidate for approval. The bill has received strong opposition by the civil society organizations that fought for the MCI's approval.	
Internet intermediaries are not liable for refusing to take action that infringes on human rights.	Intermediaries are only liable when they refuse to take action provoked by a court order, that need to be lawful and specific (Arts. 18 and 19).
Comment: The liability, however, stands when the case hits one of the exceptions included by MCI: copyright and revenge porn cases.	
State's requests to Internet intermediaries to prevent access to content or to disclose private information are strictly limited to purposes such as the administration of criminal justice; and by order of a court or independent body.	This is a success. Art.19 holds that content removal court orders should be specific and clear, and Arts. 13, 14, 15 and 16 establish that the orders regarding the disclosure of private information should keep the same standard. In both cases, there is a need for court orders. These are the general rules that law enforcement authorities or private entities need to be in compliance with.
Comment: Art. 10 §3 establishes an exception in the MCI: some personal data can be requested directly by an administrative authority — the police and public prosecutor, for instance — without a judicial warrant. Not all personal data is subject to this kind of request, only "personal qualification, affiliation and address." The implications of the exception are unclear, because it is an issue for further regulation (the MCI regulatory decree, which is still expected to be published in 2015). Only then will it be possible to be sure which administrative authority and in which situation this exception is valid. This kind of data is considered less valuable by persecutory authorities since it is produced directly by the user, without any technical or external authentication (and it is possible to lie while filling out Internet "personal info" forms).	

69 See www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=621575.

La Rue Framework Standard	Is it addressed by the MCI? How?
There are effective remedies for individuals affected by private corporations' actions, including the possibility of appeal through the procedures provided by the intermediary and competent judicial authority.	The remedies for individuals affected by private corporations' actions can be found in different normative bodies inside Brazilian jurisdiction. The MCI's Art. 11 establishes that the national legislation must be mandatorily respected when, in "any operation of collection, storage, retention and treating of personal data or communications data" by ISPs and IAPs "where, at least, one of these acts takes place in the national territory."
Comment: The MCI establishes punctual and complementary remedies that need to be placed side-by-side with at least four legislative bodies: the CDC (and the Consumer Defense National System); the Brazilian Constitution; the Civil Code; and the Civil Procedure Code. The CDC recognizes that, in consumer relations, the individual is in a weaker position when compared to the company that provides products and services to this individual, thus the CDC provides for a series of rights to that individual and obligations for that company, to equalize the relationship balance. One example is that every actor in the supply chain is liable for consumer rights violation. Thus, the Consumer Defense National System can provide additional protection in this field of enforcing the CDC provisions. The Brazilian Constitution protects the right to petition and the access to justice, as well as set a number of individual rights that cannot be damaged by private corporation actions, such as the right to privacy, intimacy and FoE. The Civil Code and the Civil Procedure Code provide the legal taxonomy of possible actions to be filed against corporations for reparation or granting an injunction against any violation of rights.	
State discloses details of content removal requests and accessibility of websites.	The MCI does not specifically address this issue.
Comment: Since 2012, Brazil has not had a Law of Access to Information[70] and, as part of its commitments to the Open Government Partnership, it has set a series of commitments regarding transparency of the judiciary and of the public defense (Ministerio Publico). The state does not publish those numbers in a pro-active manner, but could be provoked to do so through a request for information.	
Internet access is maintained at all times, including during political unrest.	The MCI does not specifically address this issue.
Comment: Brazil has a series of commitments, detailed in a series of public policies and state regulations, to guarantee universal access to Internet in Brazil.	
Disconnecting users is not used as a penalty, including under intellectual property law.	The MCI does not specifically address this issue.
Comment: It is fair to say that user disconnection is not a liability enforcement mechanism. Brazil has not implemented any mechanism similar to three-strike laws. Users may be disconnected just for not fulfilling their contractual obligations with providers (not paying their Internet or mobile bills, for instance). The idea was discussed in 2009 with Bill n. 5.361/2009, but the representative who presented it gave up supporting the proposed measure.	
State does not carry out cyber attacks.	The MCI does not specifically address this issue.
Comment: It is unclear whether the Brazilian government engages in cyber attacks, but Brazil is not in explicit or weaponized conflict with any nation. A series of measuring maps place Brazil as the geographic origin of a great diversity and amount of cyber attacks[71]; however, it is unclear if any of these is performed directly or indirectly (work-for-hire) by the Brazilian government.	
State takes appropriate and effective measures to investigate actions by third parties, holds responsible persons to account and adopts measures to prevent recurrence.	The MCI does not specifically address this issue.
Comment: This is a complex issue that demands an evaluation of the whole Brazilian justice system. We should not expect one law to deal or solve issues of justice impunity. The MCI does set a series of due process-related mechanisms, but here the role and behaviour of the judiciary and other authorities, such as the police, are the ones at the centre. The organization Article19.org in Brazil has commented: "The impact of impunity has a far reaching chilling effect on FoE across the world. Attacks against all types of journalists, human rights defenders and media workers are rarely investigated, let alone punished, and this results in self-censorship, stopping journalists criticising governments, or investigating issues such as corruption and human rights violations. As well as dealing with murder, many of the cases we come across detail constant levels of harassment, threats, office break-ins and arbitrary arrests, which also have a chilling effect. The problem isn't just the pitiful rate of successful convictions for such crimes, but also a lack of thorough and effective investigations."[72]	

70 The law regulates the right of access to public information already guaranteed by the Constitution since 1988. It provides good procedures for processing information requests and covers obligations concerning proactive disclosure and the duty to provide data in an open and non-proprietary format. This piece of legislation also provides sanctions for those who deny access to information not protected by law and outlines exceptions that generally comply with international standards of freedom of information (Article 19 2012).

71 For denial of service attacks, for instance, see www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16608&view=map.

72 See www.article19.org/resources.php/resource/37751/en/international-day-to-end-impunity:-brazil-must-adopt-measures-to-end-impunity.

La Rue Framework Standard	Is it addressed by the MCI? How?
There are adequate data and privacy protection laws and these apply to the Internet.	Partially. The MCI law passed several data protection provisions, which constitute first steps in order to protect Internet user's privacy. The core of these protections are Arts. 7, IX, X, XI and XIII, Arts. 10 and 11, which establish basic data protection notions, such as the need of user's consent. However, the law did not create an enforcement framework. See Section III, "Privacy: Between Data Protection and Data Retention" of this article for details.
Comment: The MCI it is not a "privacy protection" specific law, but a framework of general rights and principles for Internet users and uses. See Section III, "Privacy: Between Data Protection and Data Retention" of this paper for details. Also see Section IV for a discussion of the Brazilian Data Protection Bill.	
The right to anonymity is protected.	No. There is no protection to anonymity in the MCI.
Comment: The Brazilian Constitution prohibits anonymity in any form of expression (Art. 5º, IV). This provision limits the scope of the MCI's FoE protection, and it could only be changed through constitutional reform. No constitutional reform is in the current political agenda of Brazil.	
State does not regularly track the online activities of human rights defenders, activists and opposition members.	The tracking of online activities of activists or human rights defenders it is not supported by the MCI's provisions.
Comment: This kind of surveillance activity, however, is conducted by some Brazilian law enforcement agencies, in particular after the emergence of massive street demonstrations in 2013. Police authorities from Rio de Janeiro and São Paulo opened inquiries to investigate protest leaders, searching computers and social media profiles to incriminate and implicate citizens in the planning of violent acts during the 2014 World Cup.[73] It was in preparing for, and during, this event that the Brazilian intelligence agencies and other law enforcement agencies acquired social media mapping software (Muggah 2013). Another controversial initiative is the Humaniza Redes, which is a federal administration program that targets human rights violations online. The program includes the production of social media mapping analysis, which raised concerns from activists (Guimarães 2015).	
Encryption technologies are legally permitted.	There is no explicit reference of encryption technologies in either the MCI or any other Brazilian piece of legislation. This means that such technologies are legally permitted in Brazil, since they are not expressly forbidden by any law.
Comment: A report by the new Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression to Human Rights Council, David Kaye, addressed encryption techniques and anonymity and their impacts on FoE. Kaye reported that "[s]ome Governments seek to protect or promote encryption to ensure the privacy of communications. For instance, the [MCI], adopted in 2014, guarantees the inviolability and secrecy of user communications online, permitting exceptions only by court order" (A/HRC/29/32).[74] This perception was formed by a direct analysis of Brazilian government and civil society contributions for his report, which indicates at least a safe regulatory environment for encryption technologies in the country.	
State does not adopt real name registration policies (identity disclosure laws).	The Brazilian government agencies adopt, in general, a real name registration policy in the public service, which was not changed by the MCI.
Comment: Brazil does not allow anonymity for expression and has a unified national identification system. There are bills in the Brazilian Congress foreseeing the obligation of user identity registration to access Internet in LAN houses, cybercafés and other public spaces, such as libraries. Since the late 2000s, a series of states, such as São Paulo and Amazonas, have passed specific laws with the mandate of user identity registry for this kind of connectivity-related business. These efforts are justified by proponents of bills such as these as a piece in the fight against cybercrime.	
Limitations on privacy rights are exceptional (such as for administration of justice or crime prevention) and there are safeguards to prevent abuse.	The MCI sets general norms on access to user data by courts and other authorities such as the office of the public prosecutor.
Comment: See Section III, "Privacy: Between Data Protection and Data Retention" for further details on privacy.	
State has a national plan of action for Internet access.	The MCI establishes universal Internet access as a state goal in Art. 24, II, VII and VIII, and Art. 26.
Comment: Brazil has a complex and intricate framework to foster universal access, from setting infrastructure to providing computer and laptop subsidies for schools and teachers. The main national strategy is the National Plan for Broadband Access. The plan has received criticism over the years,[75] but one of President Rousseff's mandates targets to increase Internet penetration to 98 percent by 2018,[76] under the not yet launched Broadband for All Program.[77]	

73 See http://globalvoicesonline.org/2014/07/22/brazil-preemptively-arrests-activists-before-world-cup-final/.

74 See www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Pages/ListReports.aspx.

75 See www.cartacapital.com.br/blogs/intervozes/o-fracasso-do-plano-nacional-de-banda-larga-3770.html.

76 See www.tecmundo.com.br/internet/78156-dilma-quer-banda-larga-velocidade-25-mbps.htm.

77 See www.zdnet.com/article/brazilian-president-makes-internet-for-all-pledge/.

La Rue Framework Standard	Is it addressed by the MCI? How?
Concrete and effective policy is developed with the public and private sector to make the Internet available, accessible and affordable to all.	The MCI sets a mandate for multi-stakeholder participation in its Art. 24. Brazil has a series of goals regarding affordability.
Comment: For a complete study on access and affordability see Rossini (2014).	
Development programs and assistance policies facilitate universal Internet access.	See above: "State has a national plan of action for Internet access."
Comment: For a complete study on access and affordability see Rossini (2014).	
State supports production of local multicultural and multilingual content.	The MCI states that the discipline of the Internet use in Brazil is based upon the principle of plurality and the diversity (Art. 2, III) and that the state must seek users' accessibility for all different Internet users (Art. 25). Art. 27 determines that initiatives that aim to foster the Internet use and the digital culture must seek to reduce inequality gaps, and promote national and local production and distribution of online content.
Comment: Brazil's government has conducted other assessment strategies to support multicultural and multilingual content. For instance, both the Ministry of Culture[78] and the Office for Strategic Affairs have developed initiatives in this direction.[79]	
State supports initiatives for meaningful access by marginalized groups.	The MCI's Art. 25 sets that the applications developed by the public sector must seek "accessibility to all interested users," including the ones with physical and motor disabilities, "perceptual, sensorial, intellectual, mental, social and cultural characteristics, respected confidentiality and legal and administrative constraints." Art. 27 establishes that public initiatives that promote digital culture shall seek to reduce inequality gaps, especially regarding the access and use of information and communication technologies.
Comment: For a complete study on access and affordability see Rossini (2014).	
Digital literacy programs exist, and are easily accessible, including primary school education and training to use the Internet safely and securely.	The MCI Art. 27 foresees digital inclusion and literacy.
Comment: Digital literacy efforts and concerns are not new to Brazil. Brazil's digital literacy rate is around 46 percent, but recent initiatives mean Brazil is now connecting its citizens to the Web at a faster rate than most other countries in the region (Bilbao-Osorio, Dutta and Lanvin 2013. The use of ICTs is now part of the formal curricula in public schools and also on teachers' professional training. UNESCO supports a series of programs on media and information literacy in Brazil.[80]	

78 The Ministry of Culture supported a book about digital culture with interviews and articles from its most pre-eminent bureaucrats, intellectuals and organic scholars. The book is organized around the spirit of the Ministry during the mandate of Gilberto Gil (2003–2008) and Juca Ferreira (2008–2010, 2015), and brings a number of examples of policies that aimed the production of multicultural and multilingual digital content. The book is available at www.cultura.gov.br/documents/10877/0/cultura-digital-br+(2).pdf/9d6734d4-d2d9-4249-8bf5-d158d019ba6d.

79 See www.sae.gov.br/wp-content/uploads/Publica%C3%A7%C3%A3o-Midias-Digitais.pdf.

80 See www.unesco.org/new/pt/brasilia/communication-and-information/access-to-knowledge/media-and-information-literacy/.

SECTION VI: CONCLUSION

The MCI received significant international attention as a new type of legislation predicated on ensuring individuals' rights as they pertain to the Internet. It was a necessary legal and political step to set the framework of Internet use in Brazil. The MCI has advanced the debate of human rights online by reaffirming that access and use of the Internet are necessarily shaped by FoE and privacy, setting supporting mechanisms such as net neutrality, intermediary liability system, and fostering education and Internet inclusion and accessibility to guarantee those. It also points a way toward solving vexing issues through radical public involvement.

However, the MCI cannot be seen in isolation. The Internet policy system in Brazil needs to be understood as a complex system of laws and policies, their upcoming regulations, and their interpretations and enforcement by judges and other authorities. Some positive effects of the MCI need time to emerge, and its chilling effects still need to be documented for later improvement. But Brazil has set an important precedent, consolidating the idea — in a national law — that human rights are applicable online, as they are offline.

By constructing and administering ICT infrastructure and use through a revolutionary democratic model, the MCI contains both technical and political elements to foster an inclusive information society in Brazil. The MCI process, with its rights and guidance for future norm setting, supports a strong democratic system. This is what makes these new Brazilian regulations and institutions revolutionary, pioneering an example of how to legislate in our new digital reality.

Acknowledgements

The authors want to recognize and thank the contributions of Pedro Henrique Soares Ramos, Marilia Monteiro and Cristiana Gonzales. Finally, the authors thank Natalia Langenegger for support with footnotes and John Wilbanks for his peer review and editorial review.

WORKS CITED

Abromovay, P. 2014. "Brazil's Statute of Virtual Liberty." Project Syndicate. www.project-syndicate.org/commentary/pedro-abramovay-highlights-the-global-significance-of-the-country-s-new-internet--bill-of-rights#x00R3PBQ5Dli6DaY.99.

Antonialli, D., F. Brito Cruz and M. Valente. 2015. "O futuro dos comentários de Internet." Link, May 20. http://blogs.estadao.com.br/deu-nos-autos/o-futuro-dos-comentarios-de-internet/.

Article 19. 2013. "ARTICLE 19 Criticises Brazil's Criminalisation of Expression at Inter-American Commission." October 30. www.article19.org/resources.php/resource/37325/en/article-19-criticises-brazil%E2%80%99s-criminalisation-of-expression-at-inter-american-commission.

Balkin, Jack M. 2004. "Digital Speech and Democratic 2013. The Global Information Technology Report 2013: Growth and Jobs in a Hyperconnected World." World Economic Forum.

Bilbao-Osorio, Beñat, Soumitra Dutta and Bruno Lanvin, eds. 2013. *The Global Information Technology Report 2013: Growth and Jobs in a Hyperconnected World*. World Economic Forum.

Brito Cruz, Francisco. 2015. "Law, Democracy and Digital Culture: The 'Marco Civil da Internet' Lawmaking Process." Master's thesis, University of São Paulo.

Chander, Anupam and Uyen P. Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." UC Davis Legal Studies Research Paper No. 378. http://ssrn.com/abstract=2407858 or http://dx.doi.org/10.2139/ssrn.2407858.

CONANDA. 2013. "Participação Social." www.sdh.gov.br/sobre/participacao-social/conselho-nacional-dos-direitos-da-crianca-e-do-adolescente-conanda.

Diniz, G., R. Muggah and M. Glenny. 2014. "Deconstructing Cyber Security in Brazil: Threats and Responses." Strategic paper. Igarape Institute. http://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf

Dixon-Thayer, D. 2013. "Brazil's Groundbreaking Internet Civil Rights Bill Needs Support!" *The Mozilla Blog*, April 16, https://blog.mozilla.org/blog/2013/04/16/marco-civil/.

Electronic Frontier Foundation and Article 19. 2014. "Necessary & Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance." www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf.

Etherington, D. 2014. "Brazil Court Issues Injunction Against Secret and Calls for App to Be Remotely Wiped." TechCrunch. http://techcrunch.com/2014/08/20/brazil-court-issues-injunction-against-secret-and-calls-for-app-to-be-remotely-wiped/.

FETEC. 2009. "Lula Lula defende expansão da rede digital e critica projeto que censura a internet." www.fetecpr.org.br/lula-defende-expansao-da-rede-digital-e-critica-projeto-que-censura-a-internet/.

Freedom House. 2014. "Freedom on the Net 2014." https://freedomhouse.org/report/freedom-net/2014/brazil.

Gasser, Urs, Ryan Budish and Sarah Myers West. 2015. "Multistakeholder as Governance Groups: Observations from Case Studies." Berkman Center Research Publication No. 2015-1. http://ssrn.com/abstract=2549270.

Global Commission on Internet Governance. 2014. "Outcome of the first meeting of the Global Commission on Internet Governance." May 29. www.ourinternet.org/press/outcome-of-the-first-meeting-of-the-global-commission-on-internet-governance/.

Guimarães, J. 2015. "O desafio do Humaniza Redes." http://justificando.com/2015/05/05/o-desafio-do-humaniza-redes.

Jardine, E., S. Bradshaw, P. Fehlinger and N. Seidler. 2014. "The IGF 2014 Fragmentation Track." *Reimagining the Internet* (blog), August 25. www.cigionline.org/blogs/reimagining-internet/igf-2014-fragmentation-track.

Lemos, R. 2007. "Internet brasileira precisa de marco regulatório civil." May 22. http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm.

Lemos, R., F. Steibel, C. A. Souza and J. Nolasco. 2015. "A Bill of Rights for the Brazilian Internet ("Marco Civil") – A Multistakeholder Policymaking Case." https://publixphere.net/i/noc/page/IG_Case_Study_A_Bill_of_Rights_for_the_Brazilian_Internet.

Marco Civil, já!. 2013. "Manifesto". October 06. http://marcocivil.org.br/manifesto-mc/

Muggah, R. 2013. "Brazil's Wired Protests." ETH, August 23. http://isnblog.ethz.ch/social-media/brazils-wired-protests.

Oppermann, Daniel. 2014. "Internet Governance and Cybersecurity Cybersecurity in Brazil. In *Multilateral Security Governance, Conference of Forte de Copacabana*, edited by Felix Dane, 167–181. Rio de Janeiro: KAS. http://ssrn.com/abstract=2587178.

Papp, A. C. 2014. "Em nome da Internet: os bastidores da construção coletiva do Marco Civil." http://issuu.com/annacarolinapapp/docs/em_nome_da_internet.

Pinho, L. and K. Rodriguez. 2015. "Marco Civil Da Internet: The Devil in the Detail." EFF, February 25. www.eff.org/pt-br/node/84822.

Puddephatt, A., R. Zausmer and C. Rossini. 2014. "Defining Indicators of Internet Development — UNESCO Background Paper." March 1. www.gp-digital.org/publication/defining-indicators-of-internet-development-unesco-background-paper-draft/.

Question More. 2014. "Brazil Passes 'Internet Constitution' Ahead of Global Conference on Web Future." April 23. http://rt.com/news/154168-brazil-internet-freedom-law-conference/.

Reporters Without Borders. 2013. "2013 World Press Freedom Index: Dashed Hopes After Spring." Reporters Without Borders, December 19. https://en.rsf.org/press-freedom-index-2013,1054.html.

Rossini, C. 2012. "New Version of Marco Civil Threatens Freedom of Expression in Brazil." EFF, November 9. www.eff.org/deeplinks/2012/11/brazilian-internet-bill-threatens-freedom-expression.

———. 2013. "Internet and Statecraft: Brazil and the Future of Internet Governance." Global Voices Advocacy, October 14. https://advocacy.globalvoicesonline.org/2013/10/15/internet-and-statecraft-brazil-and-the-future-of-internet-governance/.

———. 2014. "Case Study: Affordable Internet Access in Brazil." A4AI Alliance for Affordable Internet, Washington, DC. August. https://a4ai.org/wp-content/uploads/2014/08/A4AI-Case-Study-Brazil-FINAL_US.pdf.

Santarém, Paulo Rená da Silva. 2010. "O direito achado na rede: a emergência do acesso à Internet como direito fundamental no Brasil." Master's dissertation, University of Brasília.

Seligman, F. 2014. "Por trás da disputa política, a força das Teles." March 19. http://apublica.org/2014/03/por-tras-da-disputa-politica-forca-das-teles/.

Souza, L. and R. Gomide. 2013. "Spies of the Digital Age." Epoca, July 27. http://epoca.globo.com/tempo/noticia/2013/07/spies-bdigital-ageb.html.

Spinola, D. 2014. "Brazil Leads Efforts in Internet Governance with its Recently Enacted 'Marco Civil da Internet.' What's In It for Intermediary Liability?" The Center for Internet and Society, Stanford. April 30. http://cyberlaw.stanford.edu/blog/2014/04/brazil-leads-efforts-internet-governance-its-recently-enacted-marco-civil-da-internet.

Sterling, B. 2013. "Pres. Dilma Rousseff at the UN General Assembly." *Wired*, September 24. www.wired.com/2013/09/pres-dilma-rousseff-at-the-un-general-assembly/.

Thompson, Marcelo. 2012. "Marco Civil ou Demarcação de Direitos? Democracia, Razoabilidade e as Fendas na Internet do Brasil." Revista de Direito Administrativo 261. http://ssrn.com/abstract=2101322.

Trinkunas, H. and I. Wallace. 2015. "Converging on the Future of Global Internet Governance." Foreign Policy at Brookings. July. www.brookings.edu/~/media/research/files/reports/2015/07/internet-governance-brazil-us/usbrazil-global-internet-governance-web-final.pdf.

UN. 2011a. "Promotion and Protection of the Right to Freedom of Opinion and Expression." Note by the Secretary-General. August 10. www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf.

———. 2011b. "General Comment No. 34." September 12. www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

UNESCO. 2012. "Fostering freedom online: The role of internet intermediaries." http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

Van Schewick, B. 2012. "Network Neutrality and Quality of Service What a Non-Discrimination Rule Should Look Like." http://cyberlaw.stanford.edu/downloads/20120611-NetworkNeutrality.pdf.

ZenithOptimedia. 2013. "Google Takes Top Position in Global Media Owner Rankings." Press release. May 28. www.zenithoptimedia.com/wp-content/uploads/2015/01/Top-30-Global-Media-Owners-2013-press-release.pdf.

Zittrain, J. 2008. *The Future of Internet*. Alexandria, MN: Caravan Books.

ANNEX: FRANK LA RUE FRAMEWORK AS STRUCTURED BY THE APC

Principle

1. National laws or constitution protect Internet-based FoE.

Arbitrary blocking or filtering

2. There are no generic bans on content.
3. Sites are not prohibited solely because of political or government criticism.
4. State blocks or filters websites based on lawful criteria.
5. State provides lists of blocked and filtered websites.
6. Blocked or filtered websites have explanation on why they are blocked or filtered.
7. Content blocking occurs only when ordered by competent judicial authority or independent body.
8. Where blocked or filtered content is child pornography, blocking or filtering online.

Criminalizing legitimate expression

9. Defamation is not a criminal offence.
10. Journalists and bloggers are properly protected.
11. National security or counterterrorism laws restrict expression only where:
    a. the expression is intended to incite imminent violence;
    b. it is likely to incite such violence; and
    c. there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

Imposition of Internet intermediary liability

12. State does not delegate censorship to private entities.
13. State requests to Internet intermediaries to prevent access to content, or to disclose private information are:
    a. strictly limited to certain purposes such as for the administration of criminal justice; and
    b. by order of a court or independent body.
14. Private corporations:
    a. act with due diligence to avoid infringing individuals' rights;
    b. only implement restrictions to these rights after judicial intervention;
    c. are transparent to the user involved about measures taken and where applicable to the wider public; provide, if possible, forewarning to users before the implementation of restrictive measures; and
    d. minimize the impact of restrictions strictly to the content involved.
15. There are effective remedies for individuals affected by private corporations' actions, including the possibility of appeal through the procedures provided by the intermediary and competent judicial authority.
16. Private corporations disclose details of content removal requests from States and accessibility of websites.

Disconnecting users from the Internet

17. Internet access is maintained at all times, including during political unrest.
18. Disconnecting users is not used as a penalty, including under intellectual property law.

Cyber attacks

19. State does not carry out cyber attacks.
20. State takes appropriate and effective measures to investigate actions by third parties, hold responsible persons to account and adopts measures to prevent recurrence.

Protection of the right to privacy and data protection

21. There is adequate data and privacy protection laws and these apply to the Internet.
22. The right to anonymity is protected.
23. State does not adopt real name registration policies.
24. Limitations on privacy rights are exceptional (such as for administration of justice or crime prevention) and there are safeguards to prevent abuse.

Access

25. State has a national plan of action for Internet access.
26. Concrete and effective policy developed with public and private sector to make the Internet available, accessible, and affordable to all.
27. State supports initiatives for meaningful access to diverse content, including for disabled people.
28. Access to law and access to legal information.
29. There are digital literacy programs.

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

Global Commission on Internet Governance

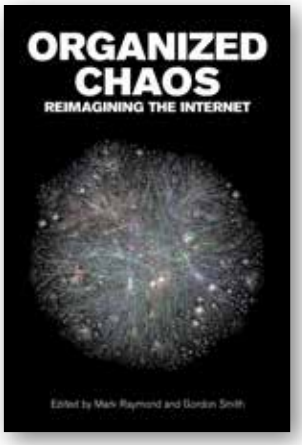
The Global Commission on Internet Governance (GCIG) was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem. Launched by two independent global think tanks, the Centre for International Governance Innovation and Chatham House, the GCIG will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

Toward a Social Compact for Digital Privacy and Security

Statement by the Global Commission on Internet Governance

On the occasion of the April 2015 Global Conference on Cyberspace meeting in The Hague, the Global Commission on Internet Governance calls on the global community to build a new social compact between citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the Internet technical community, with the goal of restoring trust and enhancing confidence in the Internet. It is now essential that governments, collaborating with all other stakeholders, take steps to build confidence that the right to privacy of all people is respected on the Internet. This statement provides the Commission's view of the issues at stake and describes in greater detail the core elements that are essential to achieving a social compact for digital privacy and security.

Available for free download at www.cigionline.org/publications



Organized Chaos

CDN$25

Edited by Mark Raymond and Gordon Smith

"Anonymous." Cybercrime. Hacktivist. Cyber security. Now part of the lexicon of our daily language, these words were unknown a decade ago. The evolution and expansion of the Internet has transformed communication, business and politics, and the Internet has become a powerful influence on everyday life globally. But the Internet is a medium that is not controlled by one centralized system, and the debate over who will govern the Internet has commanded attention from a wide range of actors, including states, policy makers and those beyond the traditional tech industries.

Organized Chaos: Reimagining the Internet examines the contemporary international politics of Internet governance problems, exploring issues such as cybercrime, activities of the global hacktivist network Anonymous and "swing states," and highlighting central trends that will play a role in shaping a universal policy to govern the Internet. In this book, some of the world's foremost Internet governance scholars consider the critical problems facing efforts to update and refine Internet governance at an international level and the appropriate framework for doing so. This volume provides the basis for developing a high-level strategic vision required to successfully navigate a multi-faceted, shifting and uncertain governance environment.

Available for purchase at www.cigionline.org/bookstore

GLOBAL COMMISSION ON INTERNET GOVERNANCE PAPER SERIES

The Regime Complex for Managing Global Cyber Activities
GCIG Paper Series No. 1
Joseph S. Nye, Jr.

Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate
GCIG Paper Series No. 2
Tim Maurer and Robert Morgus

Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community
GCIG Paper Series No. 3
Aaron Shull, Paul Twomey and Christopher S. Yoo

Legal Interoperability as a Tool for Combatting Fragmentation
GCIG Paper Series No. 4
Rolf H. Weber

Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem
GCIG Paper Series No. 5
Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

The Impact of the Dark Web on Internet Governance and Cyber Security
GCIG Paper Series No. 6
Tobby Simon and Michael Chertoff

On the Nature of the Internet
GCIG Paper Series No. 7
Leslie Daigle

Understanding Digital Intelligence and the Norms That Might Govern It
GCIG Paper Series No. 8
David Omand

ICANN: Bridging the Trust Gap
GCIG Paper Series No. 9
Emily Taylor

A Primer on Globally Harmonizing Internet Jurisdiction and Regulations
GCIG Paper Series No. 10
Michael Chertoff and Paul Rosenzweig

Connected Choices: How the Internet is Challenging Sovereign Decisions
GCIG Paper Series No. 11
Melissa E. Hathaway

Solving the International Internet Policy Coordination Problem
GCIG Paper Series No. 12
Nick Ashton-Hart

Net Neutrality: Reflections on the Current Debate
GCIG Paper Series No. 13
Pablo Bello and Juan Jung

Addressing the Impact of Data Location Regulation in Financial Services
GCIG Paper Series No. 14
James M. Kaplan and Kayvaun Rowshankish

Cyber Security and Cyber Resilience in East Africa
GCIG Paper Series No. 15
Iginio Gagliardone and Nanjira Sambuli

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime
GCIG Paper Series No. 16
Eric Jardine

The Emergence of Contention in Global Internet Governance
GCIG Paper Series No. 17
Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond

Landmark EU and US Net Neutrality Decisions: How Might Pending Decisions Impact Internet Fragmentation?
GCIG Paper Series No. 18
Ben Scott, Stefan Heumann and Jan-Peter Kleinhans

Available for free download at www.cigionline.org/publications

CIGI
Centre for International Governance Innovation
www.cigionline.org

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

EXECUTIVE

President	Rohinton P. Medhora
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Vice President of Finance	Mark Menard
Chief of Staff and General Counsel	Aaron Shull

PUBLICATIONS

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Graphic Designer	Melodie Wakefield
Graphic Designer	Sara Moore

COMMUNICATIONS

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

CIGI
67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs
10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org