CIGI

CHATHAM
HOUSE
The Royal Institute of
International Affairs

Research Volume Four

Global Commission on Internet Governance

Designing Digital Freedom

A Human Rights Agenda for Internet Governance

Research Volume Four

Global Commission on Internet Governance

Designing Digital Freedom

A Human Rights Agenda for Internet Governance

CIGI

CHATHAM HOUSE
The Royal Institute of
International Affairs

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

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

This work was carried out with the aid of a grant from the International Development Research Centre (IDRC), Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

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 conducted and supported independent research on Internet-related dimensions of global public policy, culminating in an official commission report — *One Internet*, published in June 2016 — that articulated concrete policy recommendations for the future of Internet governance. These recommendations 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 focuses 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

PREFACE

When I and my colleagues at the Centre for International Governance Innovation and Chatham House envisioned and launched the Global Commission on Internet Governance (GCIG) in 2014, we were determined to approach the work ahead strictly on the strength of evidence-based research. To make this possible, we commissioned nearly 50 research papers, which are now published online. We believe that this body of work represents the largest set of research materials on Internet governance to be currently available from any one source. We also believe that these materials, while they were essential to the GCIG's discussions over these past months, will also be invaluable to policy development for many years to come.

The GCIG was fortunate to have Professor Laura DeNardis as its director of research, who, along with Eric Jardine and Samantha Bradshaw at CIGI, collaborated on identifying and commissioning authors, arranging for peer review and guiding the papers through the publication process.

Questions about the governance of the Internet will be with us long into the future. The papers now collected in these volumes aim to be forward looking and to have continuing relevance as the issues they examine evolve. Nothing would please me and my fellow Commissioners more than to receive comments and suggestions from other experts in the field whose own research has been stimulated by these volumes.

The chapters you are about to read were written for non-expert netizens as well as for subject experts. To all of you, the message I bring from all of us involved with the GCIG is simple — be engaged. If we fail to engage with these key governance questions, we risk a future for our Internet that is disturbingly distant from the one we want.

Carl Bildt

Chair, GCIG

November 2016

INTRODUCTION:
HUMAN RIGHTS TENSIONS IN INTERNET GOVERNANCE

Laura DeNardis

INTRODUCTION

Human Rights Tensions in Internet Governance

The digital mediation of the public sphere has shifted responsibility for the conditions of individual civil liberties to the institutions and power structures that control the flow of information online. The operational tasks necessary to keep the Internet functioning and the public policies enacted around this technical infrastructure, collectively referred to as global Internet governance, are now the spaces that determine many aspects of human rights. The rights challenges mediated by Internet control structures are both deep and wide. Because the public sphere has moved online, the conditions of freedom of expression are now determined online. As all of life's functions — from online banking to network-connected cars to day-to-day communication — become digitally mediated, questions about individual privacy become exponentially more complex than in the offline realm. Other kinds of digitally mediated human rights range from the right to innovate and participate in the digital economy to protection from cyber bullying and online harassment.

The mediation of these human rights is distributed over many stakeholders, including traditional governments, new global institutions of Internet governance that design and administer technical infrastructure and, in particular, the private sector actors that own and operate the networks and platforms over which information flows. Many of these controlling stakeholders face inherent conflicts. For example, governments may not be interested in strong protections for personal privacy or cyber security because of their interest in accessing information for law enforcement, intelligence gathering, counterterrorism and other paradigmatic government functions. Authoritarian governments have an interest in blocking, filtering and, generally, censoring speech. Private industry often lacks market incentives for basic privacy because their business models are predicated upon the collection, aggregation and sharing of data to create advertising-driven revenue. These challenges will only increase as the Internet of Things and cyber physical systems continue to expand into the everyday objects of industry, home life and civic infrastructures.

Despite the worldwide description of cyberspace as "a free and open Internet," the global record of human rights online has not been commendable. Recent years have brought to light the mass surveillance practices of many governments. Other government interventions block Internet access for citizens. Censorship practices have become efficient and effective. Harassment of female bloggers has remained a constant problem. Cyber security is now a precursor for basic human rights when an outage or a hack of a car or an industrial control system creates human security and safety issues. Another complexity is that digital infrastructures, systems and institutions mediating human rights cross borders in ways that create jurisdictional complexity and contradictions. For example, private companies face a varied landscape of regulatory restrictions as to where data can be placed, as well as increasing conditions of intermediary liability for the content that users place on their systems. Acknowledging the challenges of human rights online is a necessary precursor to solving problems.

This research volume has assembled scholars, advocates and policy makers to elucidate and address intersections between Internet governance and human rights. Often, Internet governance discussions do not account for the special rights context of children in online environments. The first two chapters of this volume examine unique human rights considerations at the intersection of Internet governance and young people. As Sonia Livingstone, John Carr and Jasmina Byrne address in the first chapter, *One in Three: Internet Governance and Children's Rights* (2015), institutions of Internet governance have an opportunity to more specifically and effectively address children's rights rather than to suggest one-size-fits-all rights regimes. In the second chapter, *Education 3.0 and Internet Governance: A New Global Alliance for Children and Young People's Sustainable Digital Development* (2016), Divina Frau-Meigs and Lee Hibbard stress that global debates over Internet governance need to include discussions about how the future of education is moving from using information technology as a support tool (Education 2.0) to regarding information technology literacy as a basic competency (Education 3.0).

Some nations and regions have addressed Internet human rights issues through localized approaches. One example is Brazil's development of an Internet Bill of Rights, Marco Civil da Internet. Carolina Rossini, Francisco Brito Cruz and Danilo Doneda examine the nuances and merits of this effort in chapter 3, *The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet* (2015). In the European Union, a Court of Justice privacy ruling determined that citizens had a "right to be forgotten," essentially requesting that search engines de-index particular websites that compromised individual privacy. Researchers Kieron O'Hara, Nigel Shadbolt and Wendy Hall provide an analysis of this ruling in the fourth chapter, *A Pragmatic Approach to the Right to Be Forgotten* (2016).

Many Internet governance-related human rights decisions involve navigating competing values. Protecting one person's privacy, for example, may involve censoring another person's speech. Intelligence gathering for counterterrorism can come into conflict with basic privacy. What norms and ethics frameworks can serve as guideposts for questions about how the Internet is designed and administered? David Omand addresses the question of digital intelligence, in the aftermath of government surveillance disclosures by former National Security Agency contractor Edward Snowden, and how its collection and sharing fit within basic democratic principles of privacy in chapter 5, *Understanding Digital Intelligence and the Norms That Might Govern It* (2015). Rolf H. Weber, in the sixth chapter, *Ethics in the Internet Environment* (2016), addresses the topic of Internet governance and human rights through the lens of ethical standards for protecting privacy.

Many of the human rights issues embedded in Internet infrastructure and platforms are mediated by private industry, such as social media companies and other information intermediaries. The last two chapters in this volume address the private ordering of human rights online. Emily Taylor's chapter, *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality* (2016), helps explain private tensions between self-regulation and state rights violations and makes suggestions for solutions that comply with the rule of law but protect basic human rights. Finally, in *Corporate Accountability for a Free and Open Internet*, Rebecca MacKinnon, Nathalie Maréchal and Priya Kumar (2016) address the role of private Internet intermediaries in mediating human rights, focusing in particular on the role of systems of rankings and ratings — such as the Ranking Digital Rights Corporate Accountability Index — that can hold companies accountable and uphold global standards of human rights across borders.

Internet governance and cyber security are now the control points determining human rights. The purpose of this research volume is to explore direct connections between mechanisms of Internet governance and human rights, and to suggest design and administration interventions necessary to enhance individual rights such as privacy, autonomy, free speech and the right to innovate.

WORKS CITED

Frau-Meigs, Divina and Lee Hibbard. 2016. *Education 3.0 and Internet Governance: A New Global Alliance for Children and Young People's Sustainable Digital Development*. GCIG Paper Series No. 27. Waterloo, ON: CIGI.

Livingstone, Sonia, John Carr and Jasmina Byrne. 2015. *One in Three: Internet Governance and Children's Rights*. GCIG Paper Series No. 22. Waterloo, ON: CIGI.

MacKinnon, Rebecca, Nathalie Maréchal and Priya Kumar. 2016. *Corporate Accountability for a Free and Open Internet*. GCIG Paper Series No. 45. Waterloo, ON: CIGI.

O'Hara, Kieron, Nigel Shadbolt and Wendy Hall. 2016. *A Pragmatic Approach to the Right to Be Forgotten*. GCIG Paper No. 26. Waterloo, ON: CIGI.

Omand, David. 2015. *Understanding Digital Intelligence and the Norms That Might Govern It*. GCIG Paper Series No. 8. Waterloo, ON: CIGI.

Rossini, Carolina, Francisco Brito Cruz and Danilo Doneda. 2015. *The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet*. GCIG Paper Series No. 19. Waterloo, ON: CIGI.

Taylor, Emily. 2016. *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality*. GCIG Paper Series No. 24. Waterloo, ON: CIGI.

Weber, Rolf H. 2016. *Ethics in the Internet Environment*. GCIG Paper Series No. 39. Waterloo, ON: CIGI.

ABOUT THE AUTHOR

Laura DeNardis, CIGI senior fellow, is a scholar of Internet architecture and governance and professor in the School of Communication at American University in Washington, DC. The author of *The Global War for Internet Governance* (Yale University Press, 2014) and several other books, Laura has had her expertise featured in numerous publications. She serves as the director of research for the Global Commission on Internet Governance and is an affiliated fellow of the Yale Law School Information Society Project, where she previously served as executive director. Laura holds an A.B. in engineering science from Dartmouth College, a master's degree in engineering from Cornell University, a Ph.D. in science and technology studies from Virginia Tech, and was awarded a post-doctoral fellowship from Yale Law School.

CHAPTER ONE:

ONE IN THREE: INTERNET GOVERNANCE AND CHILDREN’S RIGHTS

Sonia Livingstone, John Carr and Jasmina Byrne

ACRONYMS

CIGI	Centre for International Governance Innovation
CRIN	Child Rights International Network
ECPAT	End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes
FOSI	Family Online Safety Institute
GSMA	GSM Association
ICTs	information and communication technologies
IGF	Internet Governance Forum
ITU	International Telecommunications Union
OECD	Organisation for Economic Co-operation and Development
Ofcom	Office of Communications
UDHR	Universal Declaration of Human Rights
UNCRC	UN Convention on the Rights of the Child
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children's Fund
WSIS	World Summit on the Information Society

INTRODUCTION

Rights that people have offline must also be protected online. We believe in: rough consensus and running code.

– David D. Clark (1992)

An estimated one in three of all Internet users in the world today is below the age of 18.[1]

Children below the age of 18 possess the full range of human rights enjoyed by adults but, as legal minors undergoing crucial processes of human development, they cannot be treated in the same way as adults. States parties and others have unique obligations to those under the age of 18. Accepting the premise of the international NETmundial initiative on Internet governance[2] means that the full range of children's rights under international law and within national jurisdictions must be respected online as well as offline.

Over a decade ago, the 2003 phase of the World Summit on the Information Society (WSIS 2003) process culminated in the adoption of the Geneva Declaration of Principles and Plan of Action, in which the position of children was expressly recognized:

> We are committed to realizing our common vision of the Information Society for ourselves and for future generations. We recognize that young people are the future workforce and leading creators and earliest adopters of ICTs [information and telecommunications technologies]. They must therefore be empowered as learners, developers, contributors, entrepreneurs and decision-makers. We must focus especially on young people who have not yet been able to benefit fully from the opportunities provided by ICTs. We are also committed to ensuring that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being.

Yet, over the past decade or so, the complex tapestry of organizations that now constitute Internet governance has barely recognized the distinctive rights and needs of children as a substantial group of Internet users.

For 2015, the Internet Governance Forum (IGF) chose as its theme "policy options for connecting the next billion." An estimated 300 million of that number will be children, and most of them will live in developing nations. This represents a significant responsibility for many key actors, and for global Internet governance. Drawing on the universal child rights framework enshrined in the United Nations Convention on the Rights of the Child (UNCRC) (UN 1989), it is recommended that recognition of and provision for the "one in three" Internet users who are aged under 18 years should be embedded in the principles and practices of every organization concerned with policies intended to shape the wider operation of the Internet.

Following a statement of the aims and approach, this chapter argues that Internet governance bodies give little consideration to children's rights, despite growing calls from international child rights organizations to address their rights in the digital age. Typically, when children are acknowledged it is in the context of child protection while their rights to provision and participation are overlooked. This chapter specifically argues against an age-generic (or "age-blind") approach to "users," because children have specific needs and rights that are not met by governance

[1] The authors' estimate is explained in the section "One in Three: Children are a Rising Proportion of All Internet Users."

[2] For the terms of reference of this influential multi-stakeholder initiative, see www.netmundial.org/terms-reference.

regimes designed for "everyone." Discussions about users in general embed assumptions about their being adults.

In addition to addressing issues of child protection in the online space, policy and governance should now ensure children's rights to access and use digital media and consider how the deployment of the Internet by wider society can enhance children's rights across the board. As Internet use rises in developing countries,[3] international Internet governance organizations face a key challenge in shaping, through multi-stakeholder processes, the emerging models of best practice that will underpin the development of positive norms recognized by states, parents and other relevant parties.

The chapter ends with six conclusions and recommendations about how to embed recognition of children's rights in the activities and policies of international Internet governance institutions.

AIMS AND OBJECTIVES

Across truly diverse domestic, cultural and geographic contexts, many children now use the Internet as part of their everyday lives. Indeed, in developed, and increasingly also in developing, countries, many children's activities are underpinned by Internet and mobile phone access in one way or another to the point where drawing the line between offline and online is becoming close to impossible, as explained in the section "Children's Rights Extend Online As Well As Offline."

When the Internet was first developed, it was a phenomenon of developed countries, driven by developments in the United States and in the English language. Policy makers tacitly assumed that users were adults. Although Internet users have diversified in recent decades, that assumption remains largely undisturbed, especially by legislators, regulators and Internet governance organizations.

This chapter was written 25 years after the launch of the World Wide Web and 25 years after the UN General Assembly adopted the UNCRC, yet there is still little recognition of children's rights by global Internet governance.

The public, policy makers and practitioners are optimistic about the potential of the Internet and other ICTs to improve children's access to learning, information, health, participation and play. However, there is also concern that Internet access increases the risks to children, resulting in calls for their protection. The pressing challenge is to understand:

- when and how the Internet contributes positively to children's well-being — providing opportunities to benefit in diverse ways that contribute to their well-being; and[4]
- when and how the Internet is problematic in children's lives — amplifying the risk of harms that may undermine their well-being and development.

While Internet governance processes have given some recognition to young people (defined by the UN as those aged between 15 and 25 years old),[5] they have accorded too little recognition of the rights of children (defined by the UN as those under 18 years old). Yet questions about when and how the Internet contributes to or undermines children's rights are not generally asked within Internet governance circles, for several reasons.

First, although the Internet's origins lie within the taxpayer-funded public (and military) sector, since the mid-to-late 1980s, the driving force behind its development has been the private sector, propelled by the creative anarchy of small start-ups that succeed by creating a market for new products and services or by disrupting old business models (Leiner et al. 2012).[6] Second, because of the highly technical nature of the Internet, historically the medium was poorly understood by the public bodies that might otherwise have been expected to engage more closely with the evolution of such an important social, economic and political phenomenon.[7] Third, the Internet's increasingly global, cross-jurisdictional nature added to the complexity of the public policy challenge, limiting the efficacy of how

[3] The language of "developed" and "developing" countries is used here, while fully acknowledging the criticisms of this language made by those who reject its binary vision and possible normative values. The alternatives — high/low income countries, or global North/South — suffer related difficulties. The chapter follows the language of the UN and International Telecommunication Union (ITU) reports, from which statistics on children in the population are drawn.

[4] The Organisation for Economic Co-operation and Development (OECD) (2011a, 18) defines well-being as "meeting various human needs, some of which are essential (e.g. being in good health), as well as the ability to pursue one's goals, to thrive and feel satisfied with their life." See also Rees and Main (2015).

[5] For example, see Nordic Youth Forum (2012); see also the program of the IGF in 2009, when child protection matters were recognised (for example, www.un.org/webcast/igf/ondemand.asp?mediaID=ws091115-redsea-am1). The Youth Coalition on Internet Governance (www.ycig.org/) represents those under 30 years old (but described itself — in its most recent blog post in 2012 — as "fairly dormant").

[6] Governments have regarded the arrival of the Internet as an important source of economic growth, bringing new forms of revenue and new jobs to their citizens. Legislators were loathe to regulate or legislate for fear of stifling innovation, and this, in turn, was welcomed by Internet-based businesses that wished to be free to experiment with different business models and international markets.

[7] In its early years in particular, the online realm was conceived as somehow unreal (or "virtual") or as just too difficult and too fast moving to manage. One result was low awareness of the vulnerabilities of several user groups, including children — except in relation to questions of access and the digital divide (and here, the focus on "households" tended to mask the specific needs of children).

states might act or intervene even if they wished to.[8] And fourth, some issues associated with children's use of the Internet pose complex technical and policy challenges, but our understanding of these is not improved by ignoring them or consigning them to a box marked "too difficult."

Even though it is commonly realized that many users are children, this history has impeded careful consideration of the proper limits that should be observed by individuals or companies working in relation to the Internet, making it difficult to enact or even discuss the particular provisions required to address children's rights in the digital age. The exception has been efforts to prevent material depicting child abuse; however, such efforts have, unfortunately, for a host of reasons beyond the scope of this chapter, occasioned such concern over censorship and threats to free speech that full recognition of the breadth of children's rights (see "Children's Rights — Legal and Normative Dimensions") has been precluded. Such circumstances have not been helped by the lack of reliable statistics on child Internet users globally.

This chapter seeks to transcend past difficulties and inform future global Internet governance deliberations in addressing children's rights. This matter is urgent because around one in three Internet users is under 18 years old, using the UN definition of a child.[9] While this chapter certainly does not advocate for identical policy approaches across infancy, childhood and adolescence, it argues that the legal status of children below the age of 18 should be distinctively recognized and addressed. This is because:

- they are legal minors and so cannot enter into contracts or licences, explicit or implicit (as often occurs on the Internet), nor are they easily able to seek redress or have redress sought against them;

- they often use online services not targeted toward them but rather to adults, or where site or service providers are unaware of or negligent of their status;[10]

- they have particular educational and informational needs that are not readily met through provision for the general population;

- they can be particularly vulnerable to sexual exploitation and abuse, which includes not only violent behaviour, but also any sexual activity with children below the age of sexual consent;

- they lack sufficient Internet (and other) literacies to fully grasp the demands and norms of the online environment (where buyer beware generally holds sway over seller beware); and

- they (and their parents) generally do not understand the data collected from them or otherwise held concerning them, whether directly or indirectly (as "big data"), nor is provision made specifically to inform them or to provide redress.

The Global Commission on Internet Governance, to which this chapter contributes, aims "to articulate and advance a strategic vision for the future Internet governance" (Centre for International Governance Innovation [CIGI] 2015). This chapter asks:

- What framework for children's rights can usefully underpin governance efforts to support children's rights in the digital age?

- What roles do or could international Internet governance bodies play in relation to children's rights?

- What efforts are needed to develop international policies and practice so as to ensure that children's rights are facilitated rather than undermined by the spread of the Internet?

The chapter draws on the working definition of Internet governance[11] developed by WSIS (2005), namely: "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet."

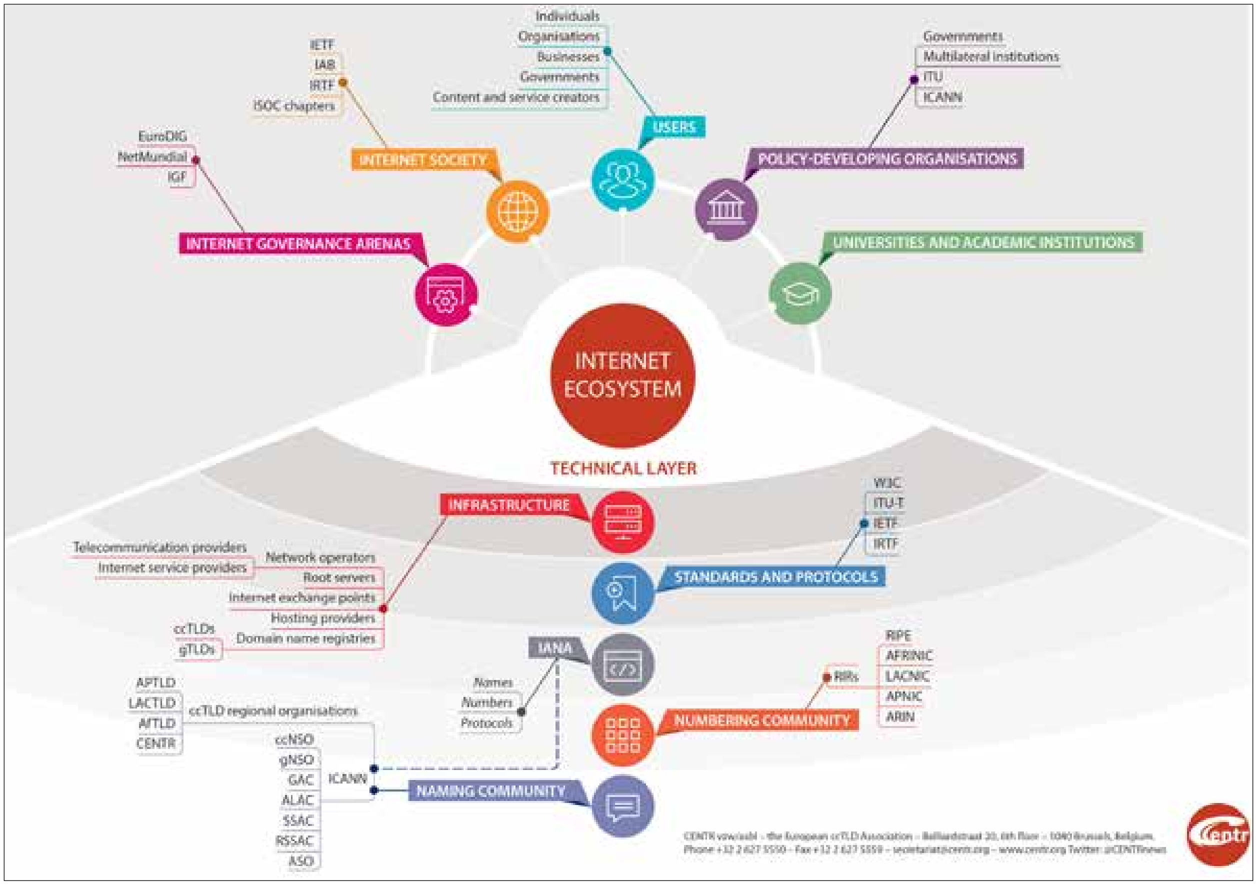
[8] From a public perspective, the prospect of state intervention, even for reasons of safeguarding or protection from abuse and exploitation, was often equally unwelcome, for reasons of political distrust and concern to protect free speech emanating especially from North America. This distrust grew as the Internet spread further across the globe, reaching states far from the Global North's political traditions. A problematic consequence is a general cloud of suspicion about the legitimate role of governments in relation to the Internet.

[9] This is qualified insofar as the laws in particular countries may specify a younger age. Article 1 of the UNCRC states: "The Convention defines a 'child' as a person below the age of 18, unless the laws of a particular country set the legal age for adulthood younger. The Committee on the Rights of the Child, the monitoring body for the Convention, has encouraged States to review the age of majority if it is set below 18 and to increase the level of protection for all children under 18" (United Nations Children's Fund [UNICEF] n.d.). Thus, law recognizes that those who have not reached the age of majority typically will lack either the knowledge or worldly experience to equip them to engage in a wide range of activities. It also makes provision for recognizing children's "evolving capacities."

[10] Consider, for example, the top 10 sites visited by six- to 14-year-olds in the United Kingdom in 2013: 63 percent visited Google, 40 percent YouTube, 34 percent the BBC, 27 percent Facebook, 21 percent Yahoo, 17 percent Disney, 17 percent Wikipedia, 16 percent Amazon, 16 percent MSN and 15 percent eBay. Adapted from COMSCORE data in the annex to Office of Communications (Ofcom) (2013).

[11] A classic definition of Internet governance is that it represents "the simplest, most direct, and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies" (Mueller 2010, 9). See also Brown and Marsden (2013), Kurbalija (2014) and Mansell (2012).

Figure 1: Internet Ecosystem



Source: Council of European National Top Level Domain Registries, reproduced with permission.

In considering the available analyses of Internet governance as they may apply to children (for example, Staksrud 2013), this chapter draws on the work of the Council of Europe, End Child Prostitution, Child Pornography & Trafficking of Children for Sexual Purpose (ECPAT), EU Kids Online, the ITU, the OECD and UNICEF, among others. These organizations lead regional and global debates and/or produce national and international reports. It also refers to international statements of children's rights in the digital age from UN treaty bodies and UN special representatives (UN Committee on the Rights of the Child, Council of Europe, the Special Rapporteur on Freedom of Expression, Special Representative of the Secretary General on Violence against Children, and others).

CHILDREN'S RIGHTS ARE LARGELY ABSENT FROM INTERNET GOVERNANCE

In the early days of the Internet, Internet governance was concentrated on the technical layer of the Internet ecosystem (see Figure 1; see also Nye 2014), the engineering required to ensure connectivity, irrespective of the content thereby communicated or the consequences for users or wider society. Today, the bodies in this technical layer still make decisions that affect both users' experiences and wider society. By contrast, the bodies shown in the centre of Figure 1 have few decision-making powers, yet it is these bodies (which operate substantially through multi-stakeholder dialogue) that constitute Internet governance.[12]

Although the 2003 phase of the WSIS recognized children's rights, by the 2005 Tunis Agenda (WSIS 2005), which gave birth to the IGF, this broad and positive vision of the Internet as a mechanism for empowering and enriching the lives of children was lost,[13] possibly because children's rights were never institutionalized within the framework

[12] Clearly, the ITU, governments and intergovernmental agencies are also part of the multi-stakeholder dialogue and these bodies also have decision-making powers, but in an important sense these are external to their role within the multi-stakeholder Internet governance frameworks where, at least nominally, everyone participates on an equal footing. Meanwhile, national governments also have powers regarding the operation of the Internet within their own jurisdictions.

[13] For a recent assessment, see ITU (2014a).

and mechanisms of what was to become known as Internet governance.[14]

Insofar as attention was given to children's rights within Internet governance, the focus tended to be on child abuse material or illegal contact by child sex offenders — these are important but far from the only issues that concern children.[15] Indeed, such a narrow lens positions children solely as vulnerable victims, neglecting their agency and rights to access, information, privacy and participation.[16] The problematic consequence is that highly protectionist or restrictive policies are advocated for children in ways that may undermine their freedom of expression or that trade children's particular needs off against adult freedoms online (La Rue 2014; Livingstone 2011; Siebert 2007).

Most international guidelines, special reports and recommendations that deal with human rights, child rights and the Internet emphasize the importance of striking a balance between opportunities and risks, freedom of expression and the right to privacy, children's right to special protection measures as well as online and offline dimensions of children's experiences. They urge that enabling these benefits while also minimizing the Internet-facilitated abuse of children requires a coordinated international-level action and global policy framework. Former UN Special Rapporteur on Freedom of Expression, Frank La Rue, for example, in his final statement in 2014, criticized overly protectionist policies that focus exclusively on risks and neglect the potential of the Internet to empower and benefit children, since the Internet is "an important vehicle for children to exercise their right to freedom of expression and can serve as a tool to help children claim their other rights, including the right to education, freedom of association and full participation in social, cultural and political life. It is also essential for the evolution of an open and democratic society, which requires the engagement of all citizens, including children" (La Rue 2014, 16).

In recent years, various UN agencies and related bodies concerned with children's well-being have addressed the importance of the Internet in relation to children's rights. Notably, in September 2014, the UN Committee on the Rights of the Child devoted a special Day of General Discussion to children's rights and the digital media in order to "develop rights-based strategies to maximize the online opportunities for children while protecting them from risks and possible harm without restricting any benefits."[17]

Their recommendations reinforce the imperative to re-examine each article of the UNCRC in the digital age. Not only did the committee recommend that national laws and policies dealing with children need to incorporate ICT-specific provisions while ICT-related legislation needs to assess the impact on children, but also that children's equal and safe access to the Internet should be part of the post-2015 development agenda.

Some regional bodies have also paved the way for global innovation in programs and standard setting that recognize the challenge of a free and open Internet that is also a safe space for children. For example, the Council of Europe's guide, "Human Rights for Internet Users," and the guide's "Explanatory Memorandum," calls for measures that allow content created by children online that compromises their dignity, security or privacy to be removed or deleted at the child's request, subject to the technical means to implement them.[18] It further proposes legal remedies and complaint procedures for children whose right to participation has been violated. Related developments and innovations have been instituted by the European Commission's Safer Internet (now Better Internet for Kids) program, including its cross-national networks of hotlines for reporting illegal child sex abuse images, helplines for children, Internet safety centres for positive provision of educational and parenting resources, and networks of researchers and children's charities to support provision, protection and participation in relation to Internet matters.[19]

[14] This remains a telling feature of the current landscape, especially since children's organizations are not always able to participate actively and advocate on children's behalf in these unfolding governance processes and dialogues, due to lack of sufficient awareness, expertise or resources to enable their inclusion in key decision-making and legislative/regulatory processes.

[15] As, for example, the *Finding Common Ground* report written to underpin this series (CIGI 2014), and the mapping of international internet public policy issues by the Intersessional Panel of the Commission on Science and Technology for Development (2014). Notably, in the NETmundial "Multistakeholder Statement" (2014) — regarded by many as a milestone summation of current thinking on Internet governance — the words "child," "children," "youth" and "young" do not appear anywhere.

[16] This blind spot is replicated in academic texts such as Mueller (2010), DeNardis (2014), Castells (2001) and Decherney and Pickard (2015).

[17] See www.ohchr.org/EN/HRBodies/CRC/Pages/Discussion2014.aspx. The resulting report is at www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf.

[18] https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2014)6&Language=lanEnglish&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864; https://wcd.coe.int/ViewDoc.jsp?id=1929453; See also Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet. Adopted by the Committee of Ministers on February 20, 2008. See https://wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Language=lanEnglish&Ver=0001&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 and the Explanatory Memorandum available at www.coe.int/web/internet-users-rights/children-and-young-people-explanatory-memo.

[19] See http://ec.europa.eu/digital-agenda/en/creating-better-internet-kids for the program, http://ec.europa.eu/digital-agenda/en/news/study-better-internet-kids-policies-member-states for an evaluation of evidence-based policy in Europe, and http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0064&qid=1440601174526&from=EN for an evaluation of the Safer Internet Programme.

Several international governmental and civil society organizations have their own specific principles of Internet governance, but as yet there is no agreed set of common principles that would guide all multi-stakeholder engagements. Nevertheless, the core values enshrined in documents by organizations such as the Council of Europe, the United Nations Educational, Scientific and Cultural Organization (UNESCO), the OECD and the NETmundial initiative[20] converge around the following principles: human rights and shared values (freedom of expression, freedom of association, privacy, accessibility, freedom of information), openness, universality, protection from illegal activity, cultural and linguistic diversity, and innovation and creativity, as well as a multi-stakeholder cooperation process that is open, transparent, inclusive and accountable.

This chapter argues that child rights are consistent with all of these principles and processes. Implementation of child rights in the digital age requires not only adherence to human rights and values, but also empowerment and participation of child users that fosters their creativity, innovation and societal engagement. It is argued below that children's rights are everybody's responsibility — from parents to states to the private sector — so what better place to start the dialogue on how these rights can be translated into the digital world than through Internet governance processes.

Beyond the principles at stake, our concern extends to organizational practice. For instance, the IGF is based on multi-stakeholder dialogue and consensus building. Yet discussions at the IGF commonly refer to Internet users (or society or "the population") as if everyone is an adult. Systematic attention to children's needs and rights has been lacking, and the views of children have not been well represented in key deliberative forums, although there has been sporadic attention to those of young people.[21] Generally, the IGF's activities are determined by its Multi-stakeholder Advisory Group, which lacks specific expertise in relation to children. Yet, as the next section argues, children represent a substantial and growing proportion of Internet users.

ONE IN THREE: CHILDREN ARE A RISING PROPORTION OF ALL INTERNET USERS

Globally, children comprise approximately one in three of the total population. In more developed countries, children under the age of 18 comprise approximately one-fifth of the population; in less developed countries, however, children constitute a substantially greater percentage of the total population — between one-third and one-half of the population (Table 1).[22]

Table 1: Global Population Figure Estimates by Age, 2015 (in thousands)

Age	Global	More Developed	Less Developed (including least developed)	Least Developed
0–4	642,161	69,065	573,096	126,597
5–10	726,250	79,943	646,307	135,023
11–17	834,777	98,909	735,869	136,511
Total children 0–17	2,203,188	247,916	1,955,272	398,131
Total population	7,324,782	1,259,588	6,065,192	940,125
% of total	**30.07**	**19.68**	**32.23**	**42.35**

Data source: UN Department of Economic and Social Affairs, Population Division.

Note: Data represent 2015 population estimates at medium variant.

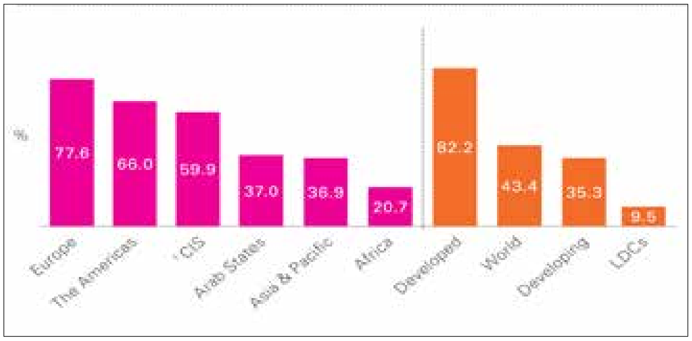
In terms of Internet use, ITU figures show that the Global North is reaching market saturation at 82.2 percent of all individuals, compared to just 35.3 percent of those in developing countries (see Figure 2). Therefore, most future growth in the online population will be concentrated in

[20] See, for example, NETmundial initiative principles at www.netmundial.org/principles, UNESCO (2015) and Declaration by the Committee of Ministers on Internet governance principles available at https://wcd.coe.int/ViewDoc.jsp?id=1835773.

[21] Only in 2009 were children discussed in a plenary session. The Youth IGF was created in 2009, and supported by the UK children's charity Childnet to participate in meetings, but it is unclear whether this has resulted in any change in Internet governance practice. See also Nordic Youth Forum (2012).

[22] Note that data is not collected and categorized consistently from developing countries. Instead, two common classification systems are used: that of most, less and least developed countries (classifications used, for example, by various UN agencies such as the UN Department of Economic and Social Affairs, UNESCO, UNICEF), and that of low-, middle- and high-income countries (as used by the World Bank). There is not necessarily alignment of countries within and between these classification systems, and indeed, some countries categorized as high income may fall within what is referred to as the "Global South." An attempt to use regional blocks — Sub-Saharan Africa, the Middle East and North Africa, the Association of Southeast Asian Nations and so on — presents the same challenges. Data used here are presented using the categories commonly used by those producing the most accurate and recent population and socio-economic data.

Figure 2: Percentage of Individuals Using the Internet



Source: ITU World Telecommunication/ICT Indicators database, reproduced with permission.

Note: LDCs refers to "least developed countries."

the Global South, where the population outnumbers that in the Global North by a ratio of more than five to one.[23]

The tipping point has already passed: two-thirds of the world's nearly three billion Internet users live in the Global South (ITU 2014b), where the proportion of children in the population is far higher than in the Global North; therefore, a sizeable and rising portion of the projected growth in Internet users will include children. Reliable data on the proportion of children included among the individuals in Figure 2 cross-nationally is not available.[24] However, the UN Population Division reports that children under 18 comprise one-third of the world's population, with almost 10 times as many children living in developing compared to developed countries.

ITU data on Internet usage among 15- to 24-year-olds by country reveals that in developing countries, young people online outnumber the overall online population by a factor of two or three (ITU 2013). For this reason, too, it seems fair to assume that depending on the age of first Internet use,[25] they will comprise a growing proportion of the Internet-using population as more of the developing world gains Internet access.

In sum, it is not currently possible to calculate the proportion of Internet users that are children with precision. The estimate that they comprise one in three of all users is based on the following:

- Under-18s comprise one-third of the world's population. Not all of them are Internet users, of course, but the indications are that children go online at a similar rate (or, to be precise, at a lower rate for small children and a higher rate for adolescents), averaged across the age span, as adults.

- Across those developed and developing countries in which ITU data are available, the average percentage of 0- to 15-year-olds online is similar to the percentage of 25- to 74-year-olds online. While infants are unlikely to be Internet users, in developed countries even preschool children are now accessing the Internet. Further, young people aged 15 to 24 are between two and three times more likely to be online than older people, and this ratio is also higher in developing countries.

- Thus, as the Internet spreads, evidence suggests that children under 18 are as likely to be online as adults over 18. While children comprise only a fifth of the population in developed countries (and so, in the beginning of the Internet, were closer to one-fifth of all Internet users), present and future growth in the online population is primarily occurring in developing countries, where children comprise between one-third and one-half of the population.[26]

In developed countries, most children live with one or both of their parents and attend school, so there has been a perhaps understandable, historically based tendency to regard parents and educators as responsible for guaranteeing children's needs and rights across the board. This assumption is being contested; first, because of the growing complexity of technology and the speed of change; and second, because in developing countries

[23] See UN Department of Economic and Social Affairs, Population Division at http://esa.un.org/unpd/wpp/Demographic-Profiles/index.shtm.

[24] However, according to the ITU World Telecommunication/ICT Indicators database, data on Internet users younger than 15 have been collected from household surveys (for example, the ICT Household Survey in Brazil) and made available in some 28 countries. While in some countries the percentage of 0- to 15-year-olds online is less than the percentage of 25- to 74-year-olds, in others it is higher. Averaging across those 28 countries, a similar percentage of 0- to 15-year-olds and 24- to 74-year-olds are online. As already stated, the percentages of 15- to 24-year-olds online are substantially higher than that for 25- to 74-year-olds in all countries. For this reason, the authors are confident in their estimate that children comprise one in three Internet users; in countries where adults are online, children are generally online in equal measure, averaged across countries. Nonetheless, it is clearly problematic that, according to the ITU's estimates, fewer than half of those countries where data on Internet use by age is available include information on Internet use by children under 15 years old. In relation to children's rights, not only is it vital to know how many children use the Internet, but such data should be disaggregated by gender, among other factors, to identify instances of inequality or discrimination.

[25] In the United Kingdom, 11 percent of three- to four-year-olds are already Internet users (Ofcom 2013).

[26] This is in part because life expectancy is lower so that "childhood" occupies a larger proportion of the life span in such countries, where those under 18 are likely to bear considerable responsibilities, yet this does not bring them commensurate rights.

many children lack parents with the time or resources to support their needs.[27]

The emphasis is shifting toward a more holistic approach that recognizes the roles of all the different actors in the Internet value chain. However, in relation to children growing up in many developing countries, it is unlikely that the existing social, law enforcement and educational infrastructures are effectively aligned. It is within these varied contexts that children's access to and use of the Internet needs to be understood. To put it another way, since it cannot be safely assumed that child Internet users have the benefit of informed parents or adequate schooling, the way in which Internet governance organizations address the needs of Internet users worldwide must encompass those of child users.

Indeed, emerging evidence from research in developing countries suggests considerably higher estimates of risk of harm and considerably lower levels of provision and participation for children in relation to ICTs than in developed countries (Livingstone and Bulger 2013; 2014). Indeed, "going online" may take a different form and meaning in different countries, and care is required in assuming that conditions in developing countries will replicate what is known in developed countries.

For example, access and use are often "mobile first" and/or community-based (for example, via cybercafés or various workarounds to gain access) rather than home- or school-based, and connectivity and even electricity may be unstable. Socio-economic, ethnic and gender inequalities in use, along with harmful or exploitative consequences of use, are more acute and there is evidence that girls' rights are particularly infringed, as are those of minority or disadvantaged children (Barbosa 2014; Beger and Sinha 2012; Gasser et al. 2010; GSM Association (GSMA) 2013; Samuels et al. 2013; UNICEF 2014). Further, in many countries, what constitutes "the Internet" is highly commercial, with little local, public or own-language provision. Regulation may be largely lacking or highly punitive, with relatively few child-focused mediators of empowerment or protection. Many children's Internet experiences concern content and services heavily tailored for adult consumers, with easy access to largely unregulated and potentially harmful content, contact and conduct, and insufficient support from parents or teachers to guide their safe and empowered Internet use.

CHILDREN'S RIGHTS — LEGAL AND NORMATIVE DIMENSIONS

What do we mean by children's rights? Children's rights are set out in the UNCRC and other international and regional human rights instruments including the Universal Declaration on Human Rights (UDHR), the UN Covenant on Civil and Political Rights, European Convention for the Protection of Fundamental Rights and Freedoms, and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.[28]

The UNCRC is the most comprehensive human rights document regarding children, and is almost universally ratified by states parties, with the notable exception of the United States.[29] It guarantees all children equal civic, political, cultural, economic and social rights, including the right to access information and the right to education, and specifically emphasizes that some rights commonly thought of in relation to adults (for example, participation and assembly) also apply to children. In addition to those rights, including in human rights frameworks, the UNCRC recognizes children's unique needs, capacities and vulnerabilities. Thus, it states that children have the right to development and play; it specifies in detail their rights to protection from all forms of violence, abuse and exploitation, and it emphasizes their right to be brought up in a protective and caring family environment.

Part 1 of the UNCRC (articles 1–41) concerns substantive rights, while Part 2 (articles 42–54) concerns their implementation. While they should be understood as part of a holistic framework, the substantive rights are commonly divided into three "Ps":

- Rights to **provision** concern the resources necessary for children's survival and their development to their full potential.
- Rights to **protection** concern the wide array of threats to children's dignity, survival and development.
- Rights to **participation** enable children to engage with processes that affect their development and enable them to play an active part in society.

Children's rights are universal, applying equally to all children in all social, economic and cultural contexts. They are also indivisible and interrelated, with a focus on the child as a whole. Thus, there is, in principle, no hierarchy of human rights, and decisions with regard to any one right must be made in light of all the other rights

[27] See Lippman and Wilcox (2014). In Eastern and Southern Africa, for example, 27 percent of children of lower secondary school age do not attend school, in South Asia 26 percent of children of the same age do not attend school, while in Western and Central Africa, this proportion rises to 40 percent of children. See UNICEF data at http://data.unicef.org/education/secondary. Further, in many developing and less/least developed countries, schools are characterized by overcrowding and by ailing or no infrastructure, and they are often poorly managed and under-resourced.

[28] Available at Council of Europe (2007) and http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=&CL=ENG.

[29] South Sudan was the latest country to ratify the convention in May 2015.

in the convention. Child rights advocates generally agree that the UNCRC's "greatest contribution has been in transforming the public perception of children. Whereas children previously tended to be seen as passive objects of charity, the Convention identified them as independent holders of rights. States parties are no longer just given the option to pursue policies and practices that are beneficial to children — they are required to do so as a legal obligation" (UNICEF 2014, 40).[30]

As a normative and analytic framework with which to ensure that important dimensions of children's lives are properly addressed by policy actors, and to gain a holistic perspective on the manifold factors that affect their well-being, the UNCRC remains a remarkably resonant, even inspiring document — and a vigorous call to global action. It recognizes children as rights-holders, with full human rights and not a partial version thereof.

The convention consists of 54 articles. There are also three optional protocols, the most relevant one to this topic being the optional protocol on the sale of children, child prostitution and child pornography. Of the UNCRC's 41 articles that deal with substantive matters, around half have immediate and obvious relevance to the Internet and the digitally networked age more broadly, as set out in Box 1.

Although formulated before mass adoption of the Internet, the UNCRC applies as much in the digital age as before. It is the yardstick by which any and every action taken by states or private sector actors can be judged. Its guiding principles include: the best interests of the child (this being an overarching principle that should guide all decisions related to the child), non-discrimination, survival and development, and participation (of children in matters that affect them). The application of these principles in the context of cyberspace may require the evolution of different approaches or ways of thinking, but the values set out in the UNCRC retain their immediacy and are of undiminished importance.

The UNCRC conceives of the child as an individual rights-holder and as a member of a family and community, with parents or guardians (article 18) having primary responsibility for their upbringing. However, the level of parental guidance will be dependent on the child's "evolving capacities" (article 5): "The Convention recognises that children in different environments and cultures who are faced with diverse life experiences will acquire competencies at different ages, and their acquisition of competencies will vary according to circumstances. It also allows for the fact that children's capacities can differ according to the nature of the rights to be exercised. Children, therefore, require varying degrees of protection, participation and opportunity for autonomous decision-making in different contexts and across different areas of decision-making" (Lansdown 2005, ix).

States have obligations to ensure appropriate legal and administrative measures that enable the realization of the rights of the child. Additionally, when children lack adequate parenting or guardianship, the UNCRC requires the state to provide special assistance and protection to the child. Insofar as the state devolves some responsibility for Internet governance to international bodies, this includes responsibility for child users. In the absence of this, assuming parents are available and competent in all matters regarding their children's Internet use is unrealistic, especially given the Internet's complex, cross-border nature.

Ratification of human rights treaties such as the UNCRC makes states legally bound by the provisions of such treaties. Following ratification, governments should put in place legislative and other measures that are in accordance with the treaty obligations. However, to ensure compliance with a convention as comprehensive as the UNCRC, national laws need to be reviewed and amended and their enforcement ensured, which is a complex and lengthy process. The UN Committee on the Rights of the Child, comprised of independent experts, provides recommendations to the states parties on the implementation of the UNCRC based on examination of national reports and dialogues with the states.

[30] This report adds that, "when the Convention on the Rights of the Child was adopted in 1989, less than a handful of independent human rights institutions for children existed in the world. Today, there are more than 200 operating in more than 70 countries, including ombudspersons, child commissioners, mediators, and child rights or human rights commissions" (UNICEF, 2014, 44). Also noteworthy is that "under article 4 of the Convention, States Parties are obligated to invest in children to the maximum extent of their available resources. As a result, increasing numbers of countries are designing budgets with children specifically in mind" (ibid., 46).

Box 1: Selected Articles of the UNCRC of Particular Relevance to the Digital Age

Provision:

- To the resources necessary for life, survival and development. (Article 6)
- To preserve his or her name, identity, nationality and family relations. (Article 8)
- Which recognizes "the important function performed by the mass media" and so encourages provision of diverse information and material of social and cultural benefit to the child (including minorities) to promote children's well-being. (Article 17a-d)
- Of an education to facilitate the development of their full potential. (Article 28)
- Of an education that will facilitate "the development of the child's personality, talents and mental and physical abilities to their fullest potential" and prepare them "for responsible life in a free society." (Article 29)
- For rest, play, recreation and leisure as appropriate to their age, including the provision necessary to "promote the right of the child to participate fully in cultural and artistic life." (Article 31)
- Of "all appropriate measures to promote physical and psychological recovery and social reintegration of a child victim of any form of neglect, exploitation, or abuse…[so as to foster] the health, self-respect and dignity of the child." (Article 39)
- "A child belonging to such a [ethnic, religious or linguistic] minority or who is indigenous shall not be denied the right, in community with other members of his or her group, to enjoy his or her own culture," religion and language. (Article 30)

Protection against:

- Any kind of discrimination. (Article 2)
- "Arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation." (Article 16)
- "Information and material injurious to the child's well-being." (Article 17e)
- "All forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse." (Article 19)[31]
- All forms of sexual exploitation and sexual abuse, including "(a) The inducement or coercion of a child to engage in any unlawful sexual activity; (b) The exploitative use of children in prostitution or other unlawful sexual practices; (c) The exploitative use of children in pornographic performances and materials." (Article 34)
- "The sale of or traffic in children for any purpose or in any form." (Article 35)
- "All other forms of exploitation prejudicial to any aspects of the child's welfare." (Article 36)
- "Torture or other cruel, inhuman or degrading treatment or punishment." (Article 37)

Participation rights:

- The right of children to be consulted in all matters affecting them. (Article 12)[32]
- Freedom of expression. (Article 13)[33]
- Freedom of thought. (Article 14)
- Freedom of association and peaceful assembly. (Article 15)
- Access to information. (Article 17)
- The right to participate freely in cultural life and the arts. (Article 31)

[31] The second part of this article is particularly pertinent for Internet governance institutions: "Such protective measures should, as appropriate, include effective procedures for the establishment of social programmes to provide necessary support for the child and for those who have the care of the child, as well as for other forms of prevention and for identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment described heretofore, and, as appropriate, for judicial involvement" (UN 1989).

[32] This is a qualified right, contingent on a judgment of the child's maturity: "States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child" (ibid.).

[33] Note that this right is not qualified according to the child's maturity, although, as for adult freedom of expression, it is qualified in order to respect the rights or reputations of others, national security, public order or public health or morals.

In relation to children, this responsibility has been articulated most notably in the form of a General Comment (no. 16 on state obligations regarding the impact of the business sector on children's rights) on the UNCRC by the Committee on the Rights of the Child (2013).[34] These business principles have been explicitly elaborated to take into account children's situations and their vulnerabilities, as well as developing specific tools for assessing the impact and monitoring of compliance.[35] Since children's rights now transcend the physical realm, being also applicable online, there is an evident need for a degree of harmonization with instruments that deal with the Internet more broadly.[36]

International Internet governance organizations have a unique opportunity to foster the multi-stakeholder dialogues that will help shape this harmonization, as examined in the next section. Without such intervention, it is likely that states will take a range of national-level actions that may threaten the global nature of the Internet and lead to widening disparities in the level of benefits that children might derive from cyberspace.

CHILDREN'S RIGHTS EXTEND ONLINE AS WELL AS OFFLINE

Not only are children going online in ever-greater numbers, but they increasingly rely on the Internet for a range of basic needs and rights — for education, information, communication, play, family relations, and so on.[37] Amanda Third et al.'s (2014) multinational consultation with children living in 16 countries concluded that children now regard access to digital media as a fundamental right and, further, they recognize that digital media are fast becoming the means through which they exercise their rights to information, education and participation.[38]

Thus, it is timely to translate the UNCRC into a clear set of standards and guidelines and a program of action that addresses children's rights in the digital age. These rights are broad-ranging and include positive ("'freedom to"') and negative ("'freedom from") obligations on states to protect human rights. The Internet is increasingly associated with many of the major physical, sexual and psychological harms from which the UNCRC holds that children should be protected. At the same time, it has been argued that the Internet: "has become the main technology through which children with access, skills and agency exercise the information and communication rights protected under the Convention" (Gasser 2014, 118).

Recent international evidence reviews have documented the relevance of the Internet to both the risks of harm that face children and the opportunities to benefit children.[39] The evidence base is growing more robust and, although much of the available research has been conducted in developed countries,[40] there is also a growing body of recent research in developing countries.[41]

As this evidence shows, use of the Internet on a mass scale by individuals and institutions is reconfiguring the routes or pathways by and through which children engage with their worlds. Given limitations of space, six illustrations of how children's rights are exercised through and impacted by the Internet are offered (see Table 2).

[34] The purpose of the General Comment is "to provide States with guidance on how they should: a. Ensure that the activities and operations of business enterprises do not adversely impact on children's rights; b. Create an enabling and supportive environment for business enterprises to respect children's rights, including across any business relationships linked to their operations, products or services and across their global operations; and c. Ensure access to effective remedy for children whose rights have been infringed by a business enterprise acting as a private party or as a State agent" (Committee on the Rights of the Child 2013, 4).

[35] See UNICEF, UN Global Compact and Save the Children (2013) and UNICEF and Danish Institute for Human Rights (2013).

[36] In the European Union, for example, a series of mechanisms have evolved to monitor or report on the activities of Internet-based businesses in terms of their impact on children's usage of their services. Following a call from then European Commission Vice President Neelie Kroes in December 2011, the CEOs of 28 major Internet businesses established the CEO Coalition (www.webwise.ie/news/ceo-coalition-responds-to-commissioner-neelie-kroes-2). This, in turn, was followed by a response from a group of industry players that established the ICT Coalition (www.ictcoalition.eu/), which established a self-reporting mechanism to demonstrate compliance with declared online child safety objectives. By contrast, it is very difficult to ascertain comparable, broad-ranging monitoring and reporting processes in the developing world where, arguably, because many aspects of the online social and educational infrastructure will be comparatively immature, the need is far greater.

[37] See, for example, Barbosa (2014), Child Rights International Network (CRIN) (2014), Internet Safety Technical Task Force (2008) , Livingstone and Bulger (2014), Livingstone, Haddon and Görzig (2012), Madden et al. (2013), Rideout, Foehr and Roberts (2010).

[38] A recent pan-European consultation with children reached a similar conclusion — see http://paneuyouth.eu/.

[39] For recent international reports, see UNICEF Innocenti Research Centre (2012), ITU (2013) and Family Online Safety Institute (FOSI) (2011).

[40] See, for example, Ainsaar and Loof (2012), Livingstone et al. (2011); Livingstone, Haddon and Görzig 2012), Livingstone and Bulger (2014), O'Neill, Staksrud and McLaughlin (2013), Jones, Mitchell and Finkelhor (2012), Rideout, Foehr and Roberts (2010), Wartella et al. (2013), OECD (2011b; 2012), Internet Safety Technical Task Force (2008) and Madden et al. (2013).

[41] See, for example, Popovac and Leoschut (2012), Davidson and Martellozzo (2010), Barbosa (2014), Soldatova et al. (2014), Livingstone and Bulger (2013), Gasser, Maclay and Palfrey (2010), GSMA (2013) and van der Gaag (2010).

Table 2: Indicative Domains in Which Children's Rights Are Reconfigured by Internet Use

Risks	Opportunities
Grooming,[42] sexual abuse and sexual exploitation including child pornography The Internet has greatly expanded the volume of child abuse images in circulation, arguably transforming the "market" for such images. Even fairly well-resourced specialist law enforcement units (e.g., the UK's Child Exploitation and Online Protection Centre) acknowledge that they cannot cope with the scale of image-related offences through traditional policing methods (i.e., detection, arrest and prosecution). Technical tools may help and are now being developed. As regards grooming offences, the scale of offending and its cross-national nature is already posing unprecedented challenges to the capacity of law enforcement agencies in the developed as well as developing world.[43]	**Education and learning** ICTs can transform children's learning opportunities and experiences and their access to knowledge and resources. The ability to access relevant information and quality content can therefore have a significant positive impact on the realization of the rights of the child, especially the right to education (Frau-Meigs and Torrent 2009; UNICEF 2014). Access and affordability are connected and children in remote, poor or rural areas are less likely to benefit from the opportunities that the Internet offers. This is particularly pronounced in developing countries (or small language communities), where the uptake is growing rapidly, but still lags behind high income countries.
Bullying and harassment Wherever the Internet is used, it is quickly recognized that Internet users — including children — pose a risk of harm to other users. When children are conceived only as victims, such problems can go unnoticed, as can the vulnerabilities of the "perpetrators." Research shows that many children are resilient to hostility, humiliation or exploitation by their peers, but some are vulnerable, resulting in mental distress, self-harm or even suicide. It also explains how these risks undermine children's rights regarding identity, reputation, privacy and play as well as safety. Yet, as part of their development, children need to explore relationships and identity issues in their own ways. Such complexities demand subtle interventions from parents, teachers, industry providers and child welfare services (Bauman, Cross and Walker 2013; Rutgers 2014; Sabella, Patchin and Hinduja 2013).	**Information and digital literacy** Increasingly, children are turning to the Internet for access to knowledge and information of diverse kinds. Some information is vital to their well-being (e.g., sexual, health or safety-related), and much is beneficial in other important ways. In addition, children are increasingly creators of online content that could include texts, images, animations, blogs, applications and videos. For this they need opportunities to learn to create, code and share content. Limitations of media and information literacy, as well as limitations on information access, mean that children may lack opportunities to develop their critical, evaluative and digital literacy skills, or that they may rely on problematic or misleading information (Albury 2013; CRIN 2014; Gasser et al. 2012; Horton 2013; Wartella et al. 2015).
Advertising and marketing In the physical world, regulations and practices have developed over many years which have limited the extent to which a range of products and services can either be advertised to or purchased by children. These have yet to be satisfactorily translated into a reality in the online space. A host of emerging practices, from online marketing, "advergames," in-app purchases, digital and viral marketing strategies, and the growing prospects of mining "big data" (the key asset behind many Internet services), all pose risks to children in terms of commercial and peer pressures, their privacy, exposure to inappropriate products and messages, and the digital literacy and competencies of children and, importantly, also the competence (or even awareness) of their parents to protect them (Bakan 2011; Brown 2009; Nairn and Hang 2012; Wilcox et al. 2004).	**Participation, voice and agency** Internet and social media provide opportunities for civic engagement and self-expression among children (Collin et al. 2011). As platforms for participation in social and civic life, these can transcend traditional barriers linked to gender, ability/disability or locale. In societies where certain groups are excluded from the decision-making processes of their communities and societies, ICTs can offer an opportunity to connect with peers, engage in political processes, and underpin the agency that will allow them to make informed decisions and choices in matters that affect them (Raftree and Bachan 2013). Children engage in issues concerning them in many ways — through social networking, digital storytelling, blogging, citizen journalism and online groups or networks.[44]

[42] Grooming refers to the "solicitation of children for sexual purposes" (Council of Europe 2007).

[43] See, for example, ECPAT (2015), Martellozzo (2011), Webster et al. (2012) and Whittle et al. (2013).

[44] See, for example, UNICEF's u-report at www.ureport.ug/.

As these examples reveal, the risks and opportunities of Internet use are impacting both positively and negatively on children's well-being and, therefore, on their rights. How this occurs, as the evidence further documents, depends on the child, their life circumstances and the wider context, and these factors interact with the specific features of the Internet — transnational, networked, interactive, ubiquitous, persistent, mobile, heavily commercial and so forth.

Age is of crucial importance in mediating the risks and opportunities of Internet use. It is pertinent that the UNCRC insists that children's rights are addressed "according to the evolving capacity of the child" (UN 1989). Yet the Internet is largely age-blind, rarely treating children according to their age or capacity, most often not treating them as children at all. In this sense, including children in governance designed for everyone fails to address their particular rights and needs.

Further vulnerabilities also matter. Just as it is inappropriate to assume all Internet users are adults, it is equally inappropriate to assume all child users are media-savvy, socially supported and psychologically resilient. Many are, to be sure, but a significant proportion is not, with age and maturity making a huge difference in this regard: research shows that those who are vulnerable (for all kinds of reasons and in all kinds of ways) are both least likely to gain the benefits of Internet use and most likely to encounter the risk of harm.[45]

Also of importance is socio-economic status, given considerable differences among children within and across countries worldwide. For many children, limitations in access preclude them from gaining the benefits of Internet use, generating new digital inequalities and forms of exclusion. On the other hand, gaining access to mobile or online technologies in the absence of adult support or regulatory infrastructure, as is the case for many children living in conditions of poverty or deprivation, can mean that the Internet poses greater risks to their safety than it affords opportunities. In the digital age, such problems can only be overcome:

- if children have sufficient and affordable access to the Internet (along with the digital literacy required to use it well) so as to fully realize their rights;
- if children are sufficiently supported and safe offline so that provision of Internet access does not place them at greater risk; and
- if children have opportunities for meaningful participation in and through digital platforms and services, including in relation to their governance.

For Internet governance organizations, along with child rights organizations, companies and states, it is imperative that the conditions under which child users actually live are recognized when designing and distributing online technologies, networks and services. It is particularly pertinent that "the Internet" available to children varies considerably across geopolitical contexts and may not be the same as that experienced by adults (for financial, linguistic, cognitive or social capacities reasons). Indeed, since children's rights are now exercised through the Internet, and since Internet governance organizations themselves influence the nature of the Internet, such organizations should surely concern themselves with children's rights, to the benefit of all.

RESPONSIBILITY FOR ENSURING CHILDREN'S RIGHTS: WHO ARE THE STAKEHOLDERS?

Joseph Nye Jr. (2014, 7) argues that Internet governance consists of multiple actors who are complexly interlinked in an ecosystem or "regime complex": "While there is no single regime for the governance of cyberspace, there is a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages."

In terms of responsibility for children, the UNCRC (and common sense) accords parents the primary responsibility (article 18 and 3), but states are required to support parents both by managing the wider environment of risks and opportunities in which they bring up their children and by intervening when necessary (for example, when parents are absent or unable) (article 4). As the environment in which children grow up becomes digitally mediated, parents and the state face particular and new challenges:

- Regarding parents, there is an abundance of evidence that they often lack the awareness, competence, will, time and resources, or the understanding, to protect and empower their children online — and this applies even more in the Global South than the North (Barbosa 2014; ITU 2013; Livingstone and Byrne 2015).
- Regarding states, the transnational and rapidly evolving nature of Internet services and providers limits their power to underpin children's rights online (consider the challenges of law enforcement) within their jurisdictions.

[45] As pan-European research from EU Kids Online shows, the relation between risk and harm is contingent — and important — but not inevitable (Livingstone et al. 2012). For the complexities of adolescent vulnerability, see also boyd (2014), Internet Safety Technical Task Force (2008), Lenhart (2015) and Whittle et al. (2013).

- Hence, some responsibility for children's rights in the digital age falls to companies and other intermediaries. This has been taken forward proactively — via a range of best practice solutions, checklists and practical guidance — in the recently produced UNICEF and ITU *Guidelines for Industry*.[46]

In principle, the multi-stakeholder approach required to ensure children's rights is familiar to those concerned with Internet governance. But for Internet governance organizations, the idea of including parents and children as crucial constituencies in multi-stakeholder governance is less familiar,[47] even though article 12 of the UNCRC states that children have the right to participate and express their views "in all matters that concern them."[48] There are, however, some signs of change.

For example, there are signs of greater understanding between Internet governance experts and children's welfare and rights advocates regarding the imperative of dealing with the apparent explosion in availability of images of child sexual abuse on the Internet.[49] Although widely reviled and — in nearly all countries — illegal, the sheer scale and technical complexity of this problem has generated a new form of multi-stakeholder action involving national and international law enforcement agencies, child rights organizations and private sector firms (network operators, content intermediaries and Internet protocol registries). Some of these responses have occasioned concern among advocates of freedom of expression lest censorious governments take this opportunity to control other kinds of Internet content.

In other areas, adult and child rights can still be seen to conflict, as sometimes do children's own rights to simultaneously participate and to be protected (Livingstone 2011). For example, how should one weigh children's privacy rights against the ability of parents and/or companies to monitor children's online activities sufficiently closely as to protect them from the risk of harm (Bartholet 2011; Shmueli and Blecher-Prigat 2011)? Identity-politics and sexual matters are particularly contentious, with little agreement over which online experiences should fall under expression or information rights and which should trigger efforts to protect the child (CRIN 2014; Gillespie 2013; La Rue 2014). Provision that allows for case-by-case consideration according to the specific context is, in such circumstances, particularly desirable to meet the needs of particular individuals.

Some commentators have regarded institutional or governmental efforts to protect children from sexual or violent offences as offering a cover for politically or theologically motivated censorship or surveillance. In this sense, children's rights are positioned as an impediment to adult rights: "Child protection arguments are part of a new pattern in which children are increasingly used to justify restrictions not only on their access to information, but also on the rights of adults. In many cases, the restrictions are rooted in a genuine, well-meaning desire to protect children from harmful information, while in others they have been used to defend discrimination and censorship" (La Rue 2014, 13).

Historically, there was some justice to these concerns. But the solution cannot be to neglect or reject the case for children's protection or, indeed, the full panoply of their rights on- and offline. Ensuring that systems of child protection online are not exploited for other purposes, legitimately or nefariously, must become a key plank of international Internet governance. Moreover, such complexities lead us to focus less on the specific outcomes required of Internet governance bodies in addressing children's rights, but rather on the necessity for developing child-sensitive processes of consultation, deliberation, evidence and engagement.[50]

Nonetheless, once the case has been accepted that age-specific considerations should apply to processes of Internet governance, we suggest that Internet governance

[46] For Guidelines for Industry on Child Online Protection developed by UNICEF and the ITU, see www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_E.PDF (Rutgers 2014).

[47] In *Finding Common Ground* (CIGI 2014), the Internet governance ecosystem is analyzed in terms of five categories of actor: the private sector, including network operators and content intermediaries, Internet protocol and domain name registries, and the international coordination of state-firm relations; the public sector, including the role of the state in developing national legislation for privacy, data protection, intellectual property, cybercrime, cyberespionage and censorship, as well as regional trade agreements; the United Nations, including the UN Human Rights Council and UN development bodies (UNDP, United Nations Conference on Trade and Development, UN CSTD and UNESCO), UN Group of Governmental Experts, the IGF, the ITU and the UN Guiding Principles on Business and Human Rights and the UN Global Compact; the OECD; and individuals as actors in Internet governance — as participants in the networked public sphere, using the Internet and social media for civic protest and issue-specific campaigning, and to hold governments and corporations to account.

[48] For good practice examples, see Nordic Youth Forum (2012) and Third et al. (2014). As the former UN Special Rapporteur on Freedom of Expression observed, not consulting children is problematic both for children in the here-and-now (given their right to be consulted), but it can also be argued that if children are not respected as rights-holders early on, they may not become the responsible adult citizens on which an open and democratic Internet relies (La Rue 2014). Children's views are a key mechanism by which the particular problems they face online can be discovered. Only then can we gain a clear vision of how their rights are being infringed or going unsupported. See Frau-Meigs and Hibbard for more on this point (2015, forthcoming).

[49] For example, the Dynamic Coalition on Child Online Safety, led by ECPAT International, has been part of the IGF since 2009 and has succeeded at raising the issue of child online exploitation in many Internet governance fora. See www.intgovforum.org/cms/dynamic-coalitions-49674/79-child-online-safety#introduction.

[50] See Lansdown (2011), plus the online tool kit at www.savethechildren.org.uk/resources/online-library/toolkit-monitoring-and-evaluating-childrens-participation.

organizations could productively draw on the experience of child rights organizations and independent child rights bodies and institutions (for example, ombudspersons) — including experts in child protection, child participation, gender and other inequalities, child helplines, education, and so forth. For example, Save the Children UK and UNICEF have collaborated on a resource guide to enable children's voices to be heard by a range of organizations and governance processes. Those organizations supporting participation of children in governance processes have an obligation to prepare children, protect them from harm and ensure their inclusion and non-discrimination (Gibbons 2015, 11).

Social media platforms also offer opportunities for children's engagement, provided that ethical standards and procedures are followed. For example, UNICEF hosts "Voices of Youth," a platform on which a community of youth bloggers and commentators from all over the world offer their insights on a range of topics affecting them. One of the key topics of this platform is digital citizenship.[51]

CONCLUSIONS

This chapter has examined the available evidence regarding children's rights to provision, protection and participation in the digital age in order to understand the challenges for international Internet governance institutions. Now that children under 18 years old — who have greater needs and fewer resources for either protection or empowerment compared with adults — constitute an estimated one-third of all Internet users, addressing their rights is a priority. Note that throughout this chapter we have focused on children rather than young people in general, and we urge the importance of considering children in relation to Internet governance because of their distinctive needs — as legal minors, not necessarily supported by caring and informed adults, often in the vanguard of online experimentation, and with generic human rights and particular rights regarding their best interests and development to their full potential.

This chapter has argued that children's rights to, in and through digital media are increasingly interlinked, and it is becoming impossible to distinguish these from their rights "offline." Understanding children's rights in the digital age, together with providing access and balancing protection and participation rights, poses pressing challenges for Internet governance. While the task of underpinning children's rights hardly came into being with the advent of the Internet, the Internet makes pre-existing phenomena newly visible (for example, the existence of sexual activities, both voluntary and coercive, among teenagers) while also providing a new set of tools for monitoring and intervention. It also alters the terrain on which much of children's lives are lived and, therefore, through which their rights are to be achieved.

There is, for historical and ideological reasons, already a link between Internet governance and human rights frameworks. As Carl Bildt (2013), chair of the Global Commission on Internet Governance, says:

> Last year we managed — as a broad coalition of countries — to get the UN Human Rights Council [UNHRC] to adopt the landmark resolution 20/8. Basically, it states that the protection of the freedom of speech and the freedom of information that the UN Universal Declaration of Human Rights [UDHR] seeks to protect in the offline world should apply equally in the online world. That is truly important. For all.

Regarding children's rights, greater steps are needed, because children's human rights necessitate special provision (special protection measures, best interest of the child, evolving capacity, participation, and so on), and there are good reasons to be concerned about whether children's rights will be met even where children and adults' rights are the same. This is because infringements of harm generally have a disproportionate impact on the vulnerable, and thus an approach that is age-generic (arguably, age-blind, by analogy gender-blind or disability-blind approaches) is unlikely to suffice.

In short, while enabling innovation is a central priority for Internet governance, any innovation must recognize that one in three users (or more or less) is likely to be a child — both an independent rights-holder and a legal minor possibly lacking adequate parental or state protection. Internet governance principles, discourses and practices must, therefore, be reshaped to accommodate this knowledge. At present, recognition of children's rights online is impeded by the fact that existing legal approaches to governance (or consumer protection) assume that users are adult, and by the technological difficulty faced by many Internet services of knowing in practice whether a user is an adult or a child.

[51] See www.voicesofyouth.org/en/page-1.

The chapter ends with six conclusions and recommendations:

- It is vital that Internet governance organizations recognize that around one in three Internet users is aged under 18, and so assumptions about users (for example users' awareness, understanding, abilities, needs or rights) should **acknowledge and address the fact that an estimated one in three Internet users are children**. We have argued that an age-generic approach on the part of Internet governance and service providers tends to blind them to the specific needs of children, and to normalize an overly adult-centric approach to Internet governance.

- In the context of the CIGI GCIG Paper Series, **it is particularly important that recognition of children's rights is embedded in the activities, policies and structures of Internet governance** processes. It is encouraging that some children's rights are occasionally acknowledged and addressed by Internet governance, in particular those focused on safety and protection. However, **children's rights encompass protection, provision and participation rights**, not only protection rights. The full array of rights is set out in the UNCRC framework, and these apply equally online as offline. Also important are strategies for addressing conflicts among these rights, with particular **care required to ensure that children's rights to provision and participation are not unduly sacrificed in the effort to protect them**.

- While states bear the primary responsibility to ensure the realization of children's rights through the creation of legislative and policy frameworks, there are **other crucial actors involved, including international governance organizations, educators, welfare professionals and the private sector**. This chapter has observed that rights frameworks now encompass the activities and responsibilities of business as well as states, for everyone and specifically for children, and has enjoined the Internet industry and Internet governance to embrace this development also.

- This chapter has also argued that, in the multi-stakeholder context that characterizes Internet governance, parents and children (and their representatives) should be recognized and included as significant stakeholders. Specifically, **children's participation in Internet governance processes — according to their evolving capacity, directly and/or via appropriate forms of representation, including research — should be supported and rendered efficacious**. This will require specific efforts in terms of educational awareness-raising and empowerment, as well as the provision of civic and institutional mechanisms for inclusion and voice. This could be done, for example, through mainstreaming online concerns in the work of existing independent child rights bodies (human rights commissions or ombudspersons for children).[52] The effect of this should be both to include children's participation, and also to draw on their expertise and experiences so as to develop ever-more effective governance processes to the benefit of all.

- This can be achieved in part through supporting **a constructive dialogue**, formal and informal, between Internet governance and child rights organizations in order to recognize and address the ways in which the activities of each affects those of the other. Also important will be the development of **mechanisms to represent and implement children's rights online.** These could include codes of practice, guidelines, regulations, checklists and audits, processes for complaint and redress, participatory practices, impact assessments, monitoring and evaluation, and so forth. To develop these, Internet governance organizations could explicitly draw on the experience of child rights organizations (or children's commissioners or ombudspersons) based on their established work in other domains. Many international Internet governance bodies are new players in a complex and fast-changing governance domain, in some contexts lacking established authority or finding it difficult to prove their legitimacy through effective governance outcomes. Since questions of child protection seem especially likely to trigger critical concerns over Internet governance in terms of its remit, accountability and forms of redress (concerns that are particularly difficult for unstable, supranational or self-regulatory organizations to allay,[53] it is vital that Internet governance bodies find ways to establish their legitimacy in relation to all stakeholders, including children and those who represent children's rights.

- To underpin the above efforts, **an evidence base is required**. The risks and opportunities afforded to children by the Internet are far from simple or universal, and they remain too little understood. To understand how the Internet is reconfiguring the conditions for children's lives, Internet governance child welfare organizations must understand the interaction between the relevant affordances of

[52] For examples of national consultations with children on issues related to privacy, freedom of expression, online violence and bullying, see the European Network of Ombudspersons for Children Consultation Document: European Commission's Communication on the Rights of the Child (2011–2014) available at: http://ec.europa.eu/justice/news/consulting_public/0009/contributions/public_authorities/023_enoc_part4.pdf.

[53] See Puppis and Maggetti (2012).

the Internet (for instance, how it eases circulation of content or designs in safety or restrictions) and the contexts of children's lives (cultural, economic, social and family factors). Understanding how children's rights are affected by Internet design, provision and governance must be continually updated by conducting rigorous cross-national research, because the technology is continuously evolving, because children's own understandings and practices continue to develop, and because of the shifting practices of design, distribution and use across diverse contexts that embeds technology in children's lives in consequential ways. The simplest place to begin would be to ensure transparency regarding the numbers of child Internet users. Hence, Internet governance organizations should ensure that important information about children is not hidden behind household statistics or ignored in measures of individuals (often documented only from the age of 14+ or 16+). In short, Internet governance organizations should ensure that important information about children's Internet access and use is collected so that it is known how many children use the Internet and which inequalities or other problems exist.

Authors' Note

This chapter was developed with the support of the UNICEF Office of Research — Innocenti. The findings, interpretations and conclusions expressed herein are those of the authors and do not necessarily reflect the policies or views of UNICEF. The authors gratefully acknowledge insights, suggestions and contributions from Alexandre Barbosa, Monica Bulger, Patrick Burton, Richard Collins, Heather Dawson, Mélanie Dulong de Rosnay, Divina Frau-Meigs, Lee Hibbard, Goran Holmqvist, Eva Kaplan, Olga Khazova, Katell Le Goulven, Esperanza Magpantay, Kirsten Sandberg, Tamara Shepard, Elisabeth Staksrud and Amanda Third. Thanks to Alexandra Chernyavskaya for research assistance in the preparation of this chapter. Last, the authors have been guided by the insights of the international experts consulted during the preparation of this chapter, as well as by the helpful comments of an anonymous reviewer.

WORKS CITED

Ainsaar, Mare and Lars Loof. 2012. *Online Behaviour Related to Child Sexual Abuse. Literature Report*. Stockholm: Council of the Baltic Sea States, ROBERT: European Grooming Project. www.innocenceindanger.de/wp-content/uploads/ 2014/05/Online_behaviour_related_to_sexual_abuse.pdf.

Albury, Kath. 2013. "Young People, Media and Sexual Learning: Rethinking Representation." *Sex Education* 13: 32–44.

Bakan, Joel. 2011. *Childhood Under Siege: How Big Business Ruthlessly Targets Children*. London: Vintage.

Barbosa, Alexandre F. 2014. *ICT Kids Online Brazil 2013. Survey on the Internet Use by Children in Brazil.* São Paolo: Brazilian Internet Steering Committee. http://cetic.br/media/docs/publicacoes/2/tic-kids-online-2013.pdf.

Bartholet, Elizabeth. 2011. "Ratification by the United States of the Convention on the Rights of the Child: Pros and Cons from a Child's Rights Perspective." *The ANNALS of the American Academy of Political and Social Science* 633 (1): 80–101.

Bauman, Sheri, Donna Cross and Jenny Walker, eds. 2013. *Principles of Cyberbullying Research: Definitions, Measures, and Methodology*. New York and Abingdon: Routledge.

Beger, Gerrit and Akshay Sinha. 2012. *South African Mobile Generation. Study on South African Young People on Mobiles*. New York: UNICEF. www.unicef.org/southafrica/SAF_resources_mobilegeneration.pdf.

Bildt, Carl. 2013. "Speech by Former Foreign Minister Carl Bildt at the Seoul Conference on Cyberspace, 2013."

boyd, d. 2014. *It's Complicated — The Social Lives of Networked Teens*. New Haven and London: Yale University Press.

Brown, Helen. 2009. "Consumer Kids by Ed Mayo and Agnes Nairns — Review." *The Telegraph*, March 13. www.telegraph.co.uk/culture/books/bookreviews/4985897/Consumer-Kids-by-Ed-Mayo-and-Agnes-Nairns-review.html.

Brown, Ian and Christopher T. Marsden. 2013. *Regulating Code: Good Governance and Better Regulation in the Information Age*. Information Revolution & Global Politics. Cambridge, MA: The MIT Press.

Castells, Manuel. 2001. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford and New York: Oxford University Press.

CIGI. 2014. *Finding Common Ground: Challenges and Opportunities in Internet Governance and Internet-Related Policy*. www.cigionline.org/publications/common-ground.

———. 2015. "Global Commission on Internet Governance." www.cigionline.org/activity/global-commission-internet-governance.

Collin, Philippa, Kitty Rahilly, Ingrid Richardson and Amanda Third. 2011. *The Benefits of Social Networking Services: A Literature Review*. Melbourne: Young and Well Cooperative Research Centre.

Committee on the Rights of the Child. 2013. "General Comment No. 16 (2013) on State Obligations Regarding the Impact of the Business Sector on Children's Rights." United Nations. April 17. www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf.

Council of Europe. 2007. *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*, CETS No. 201. Council of Europe Treaty Office. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=1&DF=&CL=ENG.

CRIN. 2014. *Access Denied: Protect Rights — Unblock Children's Access to Information*. www.crin.org/sites/default/files/access_to_information_final_layout.pdf.

Davidson, Julia and Elena Martellozzo. 2010. *State of the Nation Review of Internet Safety: Presentation of Findings*. The Telecommunications Regulation Authority, Kingdom of Bahrain. http://tra.org.bh/media/document/State%20of%20the%20nation%20review%20full1.pdf.

Decherney, Peter and Victor Pickard, eds. 2015. *The Future of Internet Policy*. Abingdon: Routledge.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

ECPAT International. 2015. "Written Statement Submitted by Foundation ECPAT International (End Child Prostitution, Child Pornography and Trafficking in Children for Sexual Purposes), a Nongovernmental Organization in Special Consultative Status." New York: United Nations General Assembly. http://ecpat.de/fileadmin/user_upload/Arbeitsschwerpunkte/Sexuelle_Gewalt_in_online_Situationen/20150313_Statement_ECPAT_International.pdf.

FOSI. 2011. *State of Online Safety Report*. 2011 Edition. Washington, DC: FOSI. www.fosigrid.org/images/grid/pdfs/State-of-Online-Safety-Report-2011-Edition.pdf.

Frau-Meigs, Divina and Lee Hibbard. 2015 (forthcoming). "Mainstreaming Children's Well-being and Sustainability Through Education 3.0 and Internet governance." GCIG Paper.

Frau-Meigs, Divina and Jordi Torrent, eds. 2009. *Mapping Media Education Policies in the World: Visions, Programmes and Challenges*. New York: United Nations Alliance of Civilizations and Grupo Comunicar. http://unesdoc.unesco.org/images/0018/001819/181917e.pdf.

Gasser, Urs. 2014. "Taking Children Seriously: A Call for the Enhanced Engagement of Children in the Discourse on Digital Rights." In *25 Years of the Convention on the Rights of the Child. Is the World a Better Place for Children?*, 117–21. New York: UNICEF. www.unicef.org/publications/files/CRC_at_25_Anniversary_Publication_compilation_5Nov2014.pdf.

Gasser, Urs, Sandra Cortesi, Momin Malik and Ashley Lee. 2012. *Youth and Digital Media: From Credibility to Information Quality*. Massachusetts, MA: Harvard University, Berkman Center for Internet & Society.

Gasser, Urs, Colin M. Maclay and John G. Palfrey, Jr. 2010. *Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations*. Berkman Center Research Publication No. 2010-7, Harvard Public Law Working Paper No. 10-36. Cambridge, MA: Berkman Center for Internet & Society at Harvard University. https://cyber.law.harvard.edu/publications/2010/Digital_Safety_Children_Young_People_Developing_Nations.

Gibbons, Elisabeth D. 2015. "Accountability for Children's Rights: With Special Attention to Social Accountability and Its Potential to Achieve Results and Equity for Children." Working Paper, UNICEF Human Rights Unit, Programme Division. www.unicef.org/policyanalysis/rights/files/Accountability-for-Childrens-Rights-UNICEF.pdf.

Gillespie, Alisdair A. 2013. "Adolescents, Sexting and Human Rights." *Human Rights Law Review* 13 (4): 623–43.

GSMA. 2013. *Children's Use of Mobile Phones. An International Comparison 2013*. Japan: GSM Association and NTT Docomo Inc. www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA_AND_NTT_DOCOMO_Childrens_Report_WebPages_R1.pdf.

Horton, Jr., Forest Woody. 2013. *Overview of Information Literacy Resources Worldwide*. Paris: UNESCO. http://unesdoc.unesco.org/images/0021/002196/219667e.pdf.

Internet Safety Technical Task Force. 2008. *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*. Massachusetts, MA: Harvard University, Berkman Center for Internet & Society. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

Intersessional Panel of the Commission on Science and Technology for Development. 2014. *The Mapping of International Internet Public Policy Issues*. Geneva: ITU. http://unctad.org/meetings/en/SessionalDocuments/CSTD_2014_Mapping_Internet_en.pdf.

ITU. 2013. *Measuring the Information Society*. Geneva, Switzerland: ITU. www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf.

———. 2014a. *Measuring the Information Society Report*. Geneva, Switzerland: ITU. www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf.

———. 2014b. *The World in 2014. ICT Facts and Figures*. Geneva, Switzerland: ITU. www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf.

Jones, Lisa M., Kimberly J. Mitchell and David Finkelhor. 2012. "Trends in Youth Internet Victimization: Findings from Three Youth Internet Safety Surveys 2000–2010." *Journal of Adolescent Health* 50 (2): 179–86.

Kurbalija, Jovan. 2014. *An Introduction to Internet Governance*. 6th edition. Geneva, Switzerland: Diplo Foundation. www.diplomacy.edu/resources/books/introduction-internet-governance.

Lansdown, Gerison. 2005. *The Evolving Capacities of the Child*. Florence, Italy: UNICEF Innocenti Research Centre. www.unicef-irc.org/publications/pdf/evolving -eng.pdf.

———. 2011. "Every Child's Right to Be Heard: A Resource guide on the UN Committee on the Rights of the Child General Comment No. 12." London: Save the Children UK and UNICEF.

La Rue, Frank. 2014. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/69/335*. New York: United Nations General Assembly. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/512/72/PDF/N1451272.pdf?OpenElement.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts and Stephen Wolf. 2012. *Brief History of the Internet*. Geneva, Switzerland: Internet Society. www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Commercialization.

Lenhart, A. 2015. *Teens, Social Media and Technology Overview 2015*. Washington, D.C.: Pew Research Center.

Lippman, Laura and W. Bradford Wilcox. 2014. "World Family Map 2014: Mapping Family Change and Child Well-Being Outcomes." *Child Trends*. www.childtrends.org/?publications=world-family-map-2014-mapping-family-change-and-child-well-being-outcomes.

Livingstone, Sonia. 2011. "Regulating the Internet in the Interests of Children: Emerging European and International Approaches." In *The Handbook on Global Media and Communication Policy*, edited by R. Mansell and M. Raboy, 505–24. Oxford: Blackwell.

Livingstone, Sonia and Monica E. Bulger. 2013. *A Global Agenda for Children's Rights in the Digital Age. Recommendations for Developing UNICEF's Research Strategy*. Florence, Italy: UNICEF Office of Research — Innocenti.

———. 2014. "A Global Research Agenda for Children's Rights in the Digital Age." *Journal of Children and Media* 8 (4): 317–35.

Livingstone, Sonia and Jasmina Byrne. 2015. "Challenges of Parental Responsibility in a Global Perspective." In *Digitally Connected: Global Perspectives on Youth and Digital Media*, edited by Sandra Cortesi and Urs Gasser, 26–29. Cambridge, MA: Berkman Center for Internet and Society, Harvard University. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2585686&download=yes.

Livingstone, Sonia, Leslie Haddon and Anke Görzig. eds. 2012. *Children, Risk and Safety Online: Research and Policy Challenges in Comparative Perspective*. Bristol: Policy Press.

Livingstone, Sonia, Leslie Haddon, Anke Görzig and Kjartan Ólafsson. 2011. *Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9–16 Year Olds and Their Parents in 25 Countries*. London: EU Kids Online, LSE. http://eprints.lse.ac.uk/33731/.

Madden, Mary, Amanda Lenhart, Maeve Duggan, Sandra Cortesi and Urs Gasser. 2013. *Teens and Technology 2013*. Washington, DC: Pew Research Center. www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_TeensandTechnology2013.pdf.

Mansell, Robin. 2012. *Imagining the Internet: Communication, Innovation, and Governance*. Oxford: Oxford University Press.

Martellozzo, E. 2011. *Online Child Sexual Abuse: Grooming, Policing and Child Protection in a Multi-media World*. London: Routledge.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Information Revolution & Global Politics. Cambridge, MA: The MIT Press.

Nairn, Agnes and Haiming Hang. 2012. *Advergames: It's Not Child's Play. A Review of Research*. Family and Parenting Institute. www.agnesnairn.co.uk/policy_reports/advergames-its-not-childs-play.pdf.

NETmundial. 2014. "NETmundial Multistakeholder Statement." http://netmundial.br/netmundial-multistakeholder-statement/.

Nordic Youth Forum. 2012. *Youth Have Their Say on Internet Governance*. Gothenburg: Nordicom.

Nye, Joseph S., Jr. 2014. *The Regime Complex for Managing Global Cyber Activities*. Waterloo, ON: CIGI. www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/The%20Regime%20Complex%20for%20Managing%20Global%20Cyber%20Activities.pdf.

OECD. 2011a. *How's Life? Measuring Well-being*. Paris: OECD Publishing. www.oecd-ilibrary.org/economics/how-s-life_9789264121164-en.

———. 2011b. *The Protection of Children Online*. OECD Digital Economy Papers. Paris: OECD. www.oecd-ilibrary.org/content/workingpaper/5kgcjf71pl28-en.

———. 2012. *Connected Minds: Technology and Today's Learners*. Paris: OECD. www.oecd-ilibrary.org/content/book/9789264111011-en.

Ofcom. 2013. *Children and Parents: Media Use and Attitudes Report*. London: Ofcom. http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/october-2013/research07Oct2013.pdf.

O'Neill, Brian, Elisabeth Staksrud and Sharon McLaughlin, eds. 2013. *Children and Internet Safety in Europe: Policy Debates and Challenges*. Gothenburg, Sweden: Nordicom.

Popovac, Masa and Lezanne Leoschut. 2012. *Cyber Bullying in South Africa: Impact and Responses*. CJCP Issue Paper 13. Claremont: Centre for Justice and Crime Prevention and UNICEF. www.lse.ac.uk/media@lse/research/Research-Projects/Researching-Childrens-Rights/pdf/Issue-Paper-13---Cyberbullying-in-SA---Impact-and-Responses.pdf.

Puppis, Manuel and Martino Maggetti. 2012. "The Accountability and Legitimacy of Regulatory Agencies in the Communication Sector." In *Trends in Communication Policy Research: New Theories, Methods and Subjects*, edited by Manuel Puppis and Natascha Just, 77–94. Bristol: Intellect.

Raftree, Linda and Keshet Bachan. 2013. *Integrating Information and Communication Technologies into Communication for Development Strategies to Support and Empower Marginalized Adolescent Girls*. New York: UNICEF. www.unicef.org/cbsc/files/ICTPaper_Web.pdf.

Rees, Gwyneth and Gill Main, eds. 2015. *Children's Views on Their Lives and Well-Being in 15 Countries: An Initial Report on the Children's Worlds Survey*. York: Children's Worlds Project (ISCWeB). www.isciweb.org/_Uploads/dbsAttachedFiles/ChildrensWorlds2015-FullReport-Final.pdf.

Rideout, Victoria J., Ulla G. Foehr and Donald F. Roberts. 2010. *Generation M2: Media in the Lives of 8- to 18-Year-Olds*. Menlo Park, CA: The Henry J. Kaiser Family Foundation. https://kaiserfamilyfoundation.files.wordpress.com/2013/04/8010.pdf.

Rutgers, Catherine, ed. 2014. *Guidelines for Industry on Child Online Protection*. Geneva, Switzerland: International Telecommunications Union. www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

Sabella, Russell A., Justin W. Patchin and Sameer Hinduja. 2013. "Cyberbullying Myths and Realities." *Computers in Human Behavior* 29 (6): 2703–11.

Samuels, Crystal, Qunita Brown, Lezanne Leoschut, Janine Jantjies and Patrick Burton. 2013. *Connected Dot Com: Young People's Navigation of Online Risks. Social Media, ICT's and Online Safety*. South Africa: Centre for Justice and Crime Prevention and UNICEF. www.unicef.org/southafrica/SAF_resources_connecteddotcom.pdf.

Shmueli, Benjamin and Ayelet Blecher-Prigat. 2011. "Privacy for Children." *Columbia Human Rights Law Review* 42: 759.

Siebert, Jennifer. 2007. "Protecting Minors on the Internet: An Example from Germany." In *Governing the Internet. Freedom and Regulation in the OSCE Region*, edited by Christian Moller and Arnaud Amoroux, 147–62. Vienna, Austria: Organization for Security and Co-operation in Europe. www.osce.org/fom/26169?download=true.

Soldatova, Galina, Elena Rasskazova, Ekaterina Zotova, Maria Lebesheva, Marina Geer and Polina Roggendorf. 2014. *Russian Kids Online: Key Findings of the EU Kids Online II Survey in Russia*. Midrand, South Africa: Foundation for Internet Development.

Staksrud, Elisabeth. 2013. *Children in the Online World: Risk, Regulation, Rights*. New edition. Aldershot: Ashgate.

Third, Amanda, Delphine Bellerose, Urszula Dawkins, Emma Keltie and Kari Pihl. 2014. *Children's Rights in the Digital Age: A Download from Children Around the World*. Melbourne: Young and Well Cooperative Research Centre.

UN. 1989. *Convention on the Rights of the Child*. www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx.

———. 2015. *Committee on the Rights of the Child*. United Nations Human Rights. www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx.

UNESCO. 2015. *Keystones to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy and Ethics on a Global Internet*. Paris: UNESCO. http://unesdoc.unesco.org/images/0023/002325/232563e.pdf.

UNICEF. 2014. *25 Years of the Convention on the Rights of the Child. Is the World a Better Place for Children?* New York: UNICEF. www.unicef.org/publications/files/CRC_at_25_Anniversary_Publication_compilation_5Nov2014.pdf.

———. n.d. "Fact Sheet: A Summary of the Rights under the Convention on the Rights of the Child." www.unicef.org/crc/files/Rights_overview.pdf.

UNICEF and Danish Institute for Human Rights. 2013. *Children's Rights in Impact Assessments*. www.unicef.org/csr/156.htm.

UNICEF, UN Global Compact and Save the Children. 2013. *Children's Rights and Business Principles*. http://childrenandbusiness.org/.

UNICEF Innocenti Research Centre. 2012. *Child Safety Online: Global Challenges and Strategies*. Florence, Italy: UNICEF Innocenti Research Centre. www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.

van der Gaag, Nikki. 2010. *Because I Am a Girl. The State of the World's Girls 2010. Digital and Urban Frontiers: Girls in a Changing Landscape*. London: Plan International. http://plan-international.org/girls/pdfs/BIAAG_2010_EN2.pdf.

Wartella, Ellen, Vicky Rideout, Alexis R. Lauricella and Sabrina L. Connell. 2013. *Parenting in the Age of Digital Technology. A National Survey*. Evanston, IL: Center on Media and Human Development. School of Communication. Northwestern University. http://cmhd.northwestern.edu/wp-content/uploads/2015/05/1886_1_SOC_ConfReport_TeensHealthTech_051115.pdf.

Wartella, Ellen, Vicky Rideout, Heather Zupancic, Leanne Beaudoin-Ryan and Alexis Lauricella. 2015. *Teens, Health, and Technology. A National Survey*. Evanston, IL: Center on Media and Human Development. School of Communication. Northwestern University. http://cmhd.northwestern.edu/wp-content/uploads/2015/05/1886_1_SOC_ConfReport_TeensHealthTech_051115.pdf.

Webster, S., J. Davidson, A. Bifulco, P. Gottschalk, V. Caretti, T. Pham et al. 2012. *European Online Grooming Project. Final Report*. Brussels: European Commission Safer Internet Plus Programme.

Whittle, H., C. Hamilton-Giachritsis, A. Beech and G. Collings. 2013. "A Review of Young People's Vulnerabilities to Online Grooming." *Aggression and Violent Behavior* 18 (1): 135–46.

Wilcox, Brian L., Dale Kunkel, Joanne Cantor, Peter Dowrick, Susan Linn and Edward Palmer. 2004. *Report of the APA Task Force on Advertising and Children*. American Psychological Association. www.apa.org/pi/families/resources/advertising-children.pdf.

WSIS. 2003. *Declaration of Principles. Building the Information Society: A Global Challenge in the New Millennium*. www.itu.int/net/wsis/docs/geneva/official/dop.html.

———. 2005. "Tunis Agenda for the Information Society." WSIS Geneva 2003-Tunis 2005. www.itu.int/wsis/docs2/tunis/off/6rev1.html.

ABOUT THE AUTHORS

Sonia Livingstone is a full professor in the Department of Media and Communications at the London School of Economics and Political Science. She has published 19 books, including *Children and the Internet: Great Expectations, Challenging Realities* (2009); *Harm and Offence in Media Content: A Review of the Empirical Literature* (2009); *Media Regulation: Governance and the Interests of Citizens and Consumers* (2012); *Children, Risk and Safety Online: Research and Policy Challenges in Comparative Perspective* (2012); and *Digital Technologies in the Lives of Young People* (2014). She has advised the United Nations Children's Fund (UNICEF), the Organisation for Economic Co-operation and Development, the European Parliament, the International Telecommunication Union (ITU), Council of Europe, the European NGO Alliance for Child Safety Online (eNACSO) and others on children's Internet safety. She is research director of the 33-country network EU Kids Online, funded by the European Commission's Better Internet for Kids Programme (www.eukidsonline.net), and is executive board member and evidence champion for the United Kingdom's Council for Child Internet Safety (UKCCIS). See www.sonialivingstone.net.

John Carr is one of the world's leading authorities on children and young people's use of the Internet and associated new technologies. He has been a senior expert adviser to the ITU and an expert adviser to the European Union. John is also a former member of Microsoft's Policy Advisory Board for Europe, the Middle East and Africa. In addition, John has been engaged professionally to advise several major high-tech companies. Since it was founded in 1999, John has been Secretary of the UK Children's Charities' Coalition on Internet Safety, comprising all the major professional child welfare organizations in Great Britain. He is an executive board member of the European NGO Alliance for Child Safety Online and an adviser to global NGO ECPAT International.

Jasmina Byrne is a senior researcher working in the UNICEF Office of Research — Innocenti, Florence, Italy. She leads UNICEF Office of Research's work on children and the Internet and has overseen and contributed to several UNICEF studies related to child safety online, cyberbullying and child rights on the Internet (see www.unicef-irc.org). In addition, she is responsible for developing and leading UNICEF's global research agenda on family and parenting support. Prior to joining Innocenti, Jasmina was head of the UNICEF child protection program in Indonesia. She has 20 years' international experience in managing complex child rights and protection programs, including research, policy development, program design and evaluation in Southeast Asia, Europe and Southern Africa with UNICEF, Save the Children, the International Committee of the Red Cross and UN Women.

CHAPTER TWO:

EDUCATION 3.0 AND INTERNET GOVERNANCE: A NEW GLOBAL ALLIANCE FOR CHILDREN AND YOUNG PEOPLE'S SUSTAINABLE DIGITAL DEVELOPMENT

Divina Frau-Meigs and Lee Hibbard

ACRONYMS

C4D	Communication for Development
CLEMI	Centre de Liaison de l'Enseignement et des Médias d'Information
CNNum	Conseil National du Numérique
CoE	Council of Europe
CRC	Convention on the Rights of the Child
CSR	corporate social responsibility
GigaNet	Global Internet Governance Academic Network
ICTs	information and communication technologies
IGF	Internet Governance Forum
IT	information technology
ITU	International Telecommunication Union
MIL	media and information literacy
MOOC	massive open online course
NGO	non-governmental organization
OECD	Organisation for Economic Co-operation and Development
SDGs	Sustainable Development Goals
UNAOC	UN Alliance of Civilizations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children's Fund
WISE	World Innovation Summit for Education
WSIS	World Summit on the Information Society

INTRODUCTION

The Internet is rapidly transforming the world's economic, cultural and social environment. There are numerous examples of its impact on connected users and their communities, in the Global North as well as in the Global South. The Internet's irreversible presence as a driver of economic, social and political development has profound implications for those who can or cannot take advantage of its opportunities. The industry is gearing up to the next billion Internet users, making education key. Yet in global Internet governance debates, the theme of education is barely acknowledged, as if this sector was still untouched by Internet evolutions and still under a latent subsidiarity principle that makes it the prerogative of states. In fact, in a globalizing environment, transnational corporations specializing in information technology (IT)-based education are encroaching on this highly subsidized public service. When mentioned, the scope of education is either narrowly reduced to compulsory education or broadly defined to include capacity building and lifelong learning.

In addition, children do not appear as a stakeholder group in Internet governance.[1] When decisions about their online lives are made by adults, they mostly concern protection from harm, as children are construed as a vulnerable group.[2] This is in deep contrast with their screen time, which begins at ever younger ages.[3] This also does not take into account the increasing numbers of children who access the Internet via multiple devices. Indeed, the precise numbers of children worldwide who are accessing the Internet is difficult to ascertain. In 2013, the International Telecommunication Union (ITU) focused on digital natives (15–25, with several years of experience in using the Internet), and found that: "In the developing world, the proportion of 15–25 year olds using the internet is more than double that of other age brackets…Overall, digital natives represent just 5.2% of the world population (approx. 36 million worldwide)" (ITU 2013; see also Livingstone, Carr and Byrne 2015). Taking into account a similar number of children between zero and 15, these data taken together indicate that an estimated 600 million young people are concerned, out of a global population of approximately 3.5 billion users (and 7 billion people worldwide, 1.7 billion of whom are under 15). These large numbers signal the urgency of the task ahead, as younger and younger children go online with more frequency. This is especially the case for developing countries (in Africa, Asia and Latin America), where Internet access and use are most likely to take place in years to come, and where the digital divide persists, aggravated by the global migrants crisis.

This chapter examines education and its digital transition from education 2.0 (where information and communication technologies [ICsT] are support tools) to education 3.0 (where media and information literacy [MIL] and Internet governance are the new basics), in line with the post-2015 Sustainable Development Goals (SDGs) of the United Nations. It posits that Internet governance offers a new form of legitimacy for children and young people, whose

[1] In the World Summit on the Information Society (WSIS) Tunis Agenda, children are not mentioned as a stakeholder group; however, they are referred to as being in need of protection in paragraph 90.q.

[2] Internet Governance Forum (IGF) and EuroDIG workshops in Vilnius (2010) and Stockholm (2012), respectively, dealt with child protection and risk management. Note also IGF meetings in Sharm-el-Sheikh (2009) on child protection, data privacy and freedom of expression.

[3] A Common Sense Media study looked at the media use of children aged zero to 8. See http://digitalkidssummit.com/2014/09/29/72-of-american-children-0-to-8-years-use-mobile-media-revisiting-common-sense-medias-2013-report/.

curiosity and resilience mitigates their current "protected" status. Active participation in Internet governance can empower them to become actors and not only subjects of policies. This can be achieved by developing a frontier field integrating the existing Internet studies with MIL, redefined to comprise Internet governance principles, protocols and processes. This new field can be integrated in the school curriculum as a key educational discipline. Such a digital transition to education 3.0 can provide children with competencies for participation, cooperation, creativity and social innovation. This, in turn, can lead to their individual and collective well-being (Frau-Meigs 2013b).

Consequently, in a holistic, systemic manner, the chapter proposes both a short-term strategy for children's immediate role in the governance process and a long-term strategy to prepare children to face a digital world, with MIL and education 3.0 at the core, which will, in turn, reinforce their role in the governance process. Hence the chapter is organized in two parallel tracks that consider the multi-stakeholder governance within education, on the one hand, and the Internet governance ecosystem outside education that can impact positively education 3.0, on the other hand. These two tracks of education and Internet governance should not ignore each other any more as they are potentially mutually reinforcing.

Based on the definition contained in the 2005 report of the Working Group on Internet Governance,[4] this chapter is inspired by the current Internet governance ecosystem of actors and events, in particular the WSIS, the IGF and NETmundial, which have helped to establish a consolidated list of principles and processes from which it is possible to build policy.[5] The main Internet governance processes are considered to be multi-stakeholder, open, consensus driven, transparent, accountable, inclusive and equitable, distributed, collaborative, and enabling of meaningful participation (including involvement from non-technical civil society). The core principles currently posited are universality, openness, interoperability, neutrality and diversity (Frau-Meigs 2012a).

The challenge is to establish the level of agency and autonomy of young people. There is considerable slippage between the categories of children, youth and minors. In the north, three major categories seem to be accepted, in terms of cognitive development: 0–8 (young children), 8–12 (pre-teens) and 13–17 (teens). There is a fourth category looming in the background: young adults (18–25), who are still very much considered as part of the millennial generation because they share similar characteristics to younger cohorts in their uses and expectations of the Internet. In the south, the conceptualization of childhood is non-linear and less driven by developmental psychology. In India, Southeast Asia and some African countries, for example, the life cycle has three or four broad phases, and childhood extends to young adulthood as a period of protracted learning (Asthana 2012). Children have responsibilities in the south that are not even considered in the north, where they are much more protected for a longer period. Considering children first and foremost also relates to the changing notion of family, which is encompassing new parenting combinations worldwide (nuclear, extended, recomposed, and so on), where children are not always nurtured by a close circle of caretakers around them.

That said, in both the north and south, the boundaries of childhood are also being renegotiated, in part because providers of online content and services establish ages for access and use in their agreements. Because most global platforms are US based or aligned with US practices, the major online threshold is actually determined by the permitted age of access to social networks, largely established at 13; this age restriction rule appears in the US Children's Online Privacy Protect Act.[6] This threshold can conflict with state regulations or laws about the age from which children can use services in many other countries, in particular in schools.

Taking this range of online childhoods into account in a holistic manner, children must be considered as having agency and responsibilities from an earlier age, while still needing to be protected from risks of different kinds. The unprecedented degrees of exposure to all sorts of materials and resources online are an additional element to take into account: in most countries, children have access to content traditionally reserved for adults, be it harmful content (such as violence and pornography) or specialized high-level content with abstract information. This can impinge on the latency of childhood, while, however, creating new opportunities for access to learning. Availability of media, in particular ICT-driven media, is a critical multiplier for primary degree necessities, such as food and hygiene. Second-degree necessities, also called "functionings" (Sen 1985), such as access to education and media, foster self-esteem and well-being, even in harsh poverty-stricken circumstances, because their value is dependent on the choices of the young people actually concerned, in their local circumstances. These functionings lead to real freedoms or "capabilities" that in turn foster the capacity for participation in community life and civic agency, at very early ages (ibid.). Consequently, development needs to be considered in the double meaning of the word: the development for children's individual well-

[4] "Internet Governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" (Working Group on Internet Governance 2005, 4, paragraph 10).

[5] The NETmundial process is a consolidation of prior events and discussions. See http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

[6] Its extension to a new category of "minors" (between the ages of 13 and 15) is being debated in the Do Not Track Kids Act of 2015.

being, and the development of collective sustainable well-being in a globalized world.[7]

MAINSTREAMING WELL-BEING THROUGH INTERNET GOVERNANCE PRINCIPLES IN TWENTY-FIRST-CENTURY EDUCATION

Countries worldwide are asked to make a rather brutal transition effort from analogical, pre-digital structures to digital ones. And this transition is not "transitory": the nature of digital technologies, based on networked production and collaborative innovation, is in constant evolution. This process requires acculturation to the realities of the online world. Mainstreaming well-being implies ensuring that the issues relevant to young people respond to their needs and capabilities, and are buttressed to Internet governance principles that are translated into age-relevant rules and practices.

This effort points to a great need for inclusion: the digitally excluded are not so just because of economic conditions, but also because of age, gender and lack of literacy skills to fully benefit from Internet access when they have it. They are at risk of being left behind. The lack of training and attendant degrees and the lack of familiarity with digital processes can lead to different forms of exclusion from society (Conseil National du Numérique [CNNum] 2013). This pattern has implications for the perceived usefulness of the Internet and the appreciation of its benefits and of its relevance for local functionings and sustainability. It also affects the engagement of young boys and girls in Internet activities for uses other than entertainment, such as education, career goals and job training.

The Internet-poor are no longer the digital "immigrants" of the early 2000s, when Marc Prensky (2001) coined the catchy phrase that opposed them to digital "natives." This metaphor may have applied to the early stages of the Internet but it needs to be revisited. Today's reality is that children are both native and naïve, given the advantages of easy adaptation to the technology and the limitations of self-taught learning online. Their skills, competencies, values and attitudes are very heterogeneous and based mostly on leisure activities, not on scholastic practice. The teachers now joining the profession, born since the advent of the Internet, also need to be trained. The same applies to parents, as they have very spotty capacities for employing technical tools to manage their children's access and use of the Internet (Dreyer 2014; EU Kids Online 2014). Both groups experience digital literacies "in the wild" (Frau-Meigs 2012c).

Policy makers should abandon the catchy phrase they have adopted to justify a "wait-and-see" approach, and not leave children to deal alone with mobile applications and Internet services provided by the industry. The earlier children are aware of Internet uses and issues, the better. The more included they are, the more they will know how to contribute to and participate in society through the informed use of technology. Internet governance principles and processes need to be adapted to education and the new constituency of children.

In this context, access is no longer just about physical infrastructure (sometimes called threshold access). It is about real or reach access, obtained through training and competencies, that may ultimately lead to access to opportunity, by which people can effect true change for themselves and their community. This last stage could be considered as sustainable access, with a full, networked presence and online participation leading to the production of meaningful content. Ensuring all these stages of access requires public intervention and a pedagogy for participation that cannot be delegated to the market alone. The proliferation of actors requires exchanges between decision makers and all the members of a community to engage in the protection and promotion of the best interests of children. The scenario of sustainable access is neither natural nor neutral, but is political, as it is driven by globalization and its ICT-driven media and networks. This places the governance of education at the crux of present and future change.

Schools and the Mainstreaming Gap

While certain Internet governance processes and actors (for example, the IGF and the Internet Corporation for Assigned Names and Numbers) are well embarked in the digital transition of accountability and transparency to the multi-stakeholder community, many international and national organizations and institutions, in particular in the field of education, are lagging behind. They are still dealing with the Internet as a tool in itself (education 2.0), not as an environment in itself (education 3.0).[8] The effort that is currently being made to find synergies between the WSIS review and the SDGs (and it should be noted that among the 17 goals, only one is directly related to ICTs) is evidence

[7] The authors' approach is based on research in childhood studies related to social cognition. Communication for development (C4D) is added, with a specific focus on policy and social innovation. For well-being and childhood studies, see Ben-Arieh et al. (2013). For "functionings" and C4D, see Sen (1985); see also Nussbaum (2011) and McAnany (2012, 205–18).

[8] The plans for digital equipment in schools since the 1980s and their evaluations and results demonstrate this, as exemplified in the French plan Informatique Pour Tous (1985), the Regroupement économique et social du Sud-Ouest 2007 plan and in Fichez (2000, 65–72); see also Frau-Meigs and Torrent, eds. (2009, introduction).

that the underpinning role and ecosystem of the Internet is not yet fully understood. There is a failure to recognize it as the major source of all transformations that will take place in the twenty-first century, in spite of the estimations of international education experts.[9] For example, the arrival of the "Internet of Things," connecting operators, non-human agents and big data, is greatly underestimated, in particular as the driving force behind education 3.0 (Frau-Meigs 2015).

When looking at what is being done about MIL in schools, the situation is very heterogeneous. MIL and related topics are generally absent from courses for teaching degrees and "in-career" training. In schools, these subjects are often left to the initiative of self-taught teachers as they are not part of the basic curriculum. As a result, they are blended with mother tongue and language courses, which makes it difficult to evaluate them per se.[10] The decision-making bodies for education do not completely understand them, which results in inaction, ineffective decision making, an underestimation of needs and costs, and an absence of critical rights (to access, data privacy and ethics).

Digital education is not equitably distributed within and among all countries, leading to a lack of social justice as the digitally excluded are also at risk of economic and social exclusion. If school systems fail to change their curricula, degrees and skill requirements, they risk becoming irrelevant and digital education will take place in spaces that are not open, public and fair (Gauthier 2015, 103–110). In terms of sustainable development and well-being, the cost of inaction is considerable. Decision makers, policy makers and teachers alike need to retool the pre-digital basic curricula to transition more fully to the digital culture, with its attendant constraints and opportunities.

Managing the digital transition implies revising all dimensions of schooling — from kindergarten to university, from student training to teacher training, from learning skills to learning methods and styles, and from the evaluation of teachers to the evaluation of children. The very content of school subjects must be revisited as well as the competencies, attitudes, values and finalities of the system. Many educational systems are being put to the test and heavily criticized for not being inclusive and for increasing differences in gender, age and access.[11]

On the one hand, there is a persistent negative discourse regarding the digital evolution in many countries and communities. Teachers and parents still often perceive the Internet as being in competition with school and home. Web 2.0 applications are perceived as dividing attention (for example, leisure time and games at school and at home), providing alternative tools to scientific sources of knowledge (for example, online courses and participatory Wikimedias) and increasing risks (for example, harassment, loss of basic literacies, and so on), perhaps even leading to the infringement of human rights (for example, privacy and intellectual property). Many tools available online (serious games, interactive platforms for e-learning, corporate tutorials, so on) are perceived as potentially diminishing the roles of teachers and impinging on the perimeter of schools and universities. Even when these tools are promoted because of their potential to motivate and re-engage students, they are perceived as removing the monopoly of education from the public sphere and as blurring the borders between scholastic learning and gaming.

On the other hand, there is also a very positive discourse about the Internet as a tool and driver of innovative pedagogies, for project-based learning and for the improvement of capabilities such as self-actualization, self-esteem, empowerment, online presence and so on. Research has revealed that, in the communities of practice, there is a lot of energy and creativity at work, for example, the "hole in the wall" computers in India with "minimally invasive education"; école 42, a French school set up on the "Born2code" notion; or the Institute of Play in New York.[12]

However, this positive discourse does not provide an incremental notion of change, it does not give any indication of scalability and sustainability and it fails to posit change management as a key training sector to enable teachers and students alike to move toward education 3.0 with education 3.0 tools. Many educators fear further gaps and divides between the information-rich and the information-poor. They feel that they are expected to manage contradictory goals (foster innovation and yet transmit heritage). In some countries, there is a call for "back to basics" (the 3Rs) and MIL is pitched against basic needs rather than

[9] See World Innovation Summit for Education (WISE) survey "School in 2030," completed by 645 experts and conducted on June 3–30, 2014 (www.wise-qatar.org/future-school-2030).

[10] See the 2014 French National Research Agency TRANSLIT project reports in 28 European countries (www.translit.fr).

[11] As exemplified by the many controversies concerning PISA [Programme for International Student Assessment] study results. In France, some recent work shows the weight of pre-digital era diplomas and the inequalities being generated by schools that no longer ensure the full provision of social and economic benefits; see Dubet, Duru-Bellat and Vérétout (2010), see also CNNum (2014).

[12] See www.hole-in-the-wall.com/, www.42.fr and www.instituteofplay.org.

being positioned as necessary for capacity building and the production of relevant local educational content.

Such contradictory discourses and experimentations prove that giving teachers and students computers is not enough: tools without skills do not lead to full capabilities.[13] Teachers have to become change agents, not subjects to change. Those who are increasingly convinced of the need to use ICTs lack support (European Schoolnet 2013; 2014). They have to be trained with regards to both MIL and change management within their own institutions, so that they can make their pedagogy, teaching styles and content relevant — as well as attractive — to young people. A process of bottom-up governance — where good practices can be exchanged, transferred and translated, and where tool kits and other resources for training are affordable — can lead to incremental degrees of change, adapted to the rhythm of education and compatible with their students and their communities.[14]

This process can be operationalized with the Internet governance principles and processes in education, in particular with MIL, as already exemplified in initiatives such as the Global Alliance for Partnerships on Media and Information Literacy and its regional chapters, which provides a response to arguments concerning whether MIL and e-skills could deprive schools in poor areas or countries of even basic educational infrastructure and divert attention from the lack of quality content provided by them. For scaling up digital literacy in line with open knowledge and the commons, e-learning strategies for lifelong learning and training (open educational resources, MOOCs, and so on) are likely forces to consider.[15] They are not adapted to all situations, though, and need to be blended with brick-and-mortar schools, as face-to-face interaction remains crucial for education.

Information Cultures Meet Computational Thinking via MIL

Since the 1980s, many "computers-in-schools" plans have performed poorly worldwide, for various reasons, most with a strong technological component: lack of integration of ICTs in the brick-and-mortar education system; insufficient teacher training conditions; confusion between learning finalities (transmission of knowledge) and technical finalities (professional training); industrial economic lobbying vs. educational public values; lack of clearly identified curriculum for new literacies (except for informatics as a discipline); and lack of relevant local content (Moeglin 2005).

Examples of Ongoing Laptop-driven School Initiatives

- One Laptop per Child (2007): Early MIT Media Lab-driven initiative for affordable educational laptops (US$100) for children in the United States, Southeast Asia, Latin America and Africa. Mixed results (in India, Nigeria and Thailand, for example) due to a lack of teacher training, in situ maintenance and local content.
- Uruguay and Plan Ceibal (2009): Uruguay was the first country in the world to give each child in primary school a free laptop computer; local content and teacher training were added.
- India and Datawind (2013): The Aakash tablet, the cheapest computer in the world, was sold by Datawind to the Indian government for school systems (with an app store to monetize content).

In order to reboot computing in a manner that is meaningful for young people and adults alike, it needs to be related to a strong societal and cultural drive, which is not to be separated from local needs and functionings. Traditionally, computing has been associated with three major domains: algorithms and data processing; human-machine interaction; and networked participation with human and non-human agents (Chapron and Delamotte 2010). The arrival of a fourth domain — as a result of social networks, big data and the Internet of Things — led designer John Maeda (2004) to qualify this form of computing as "a new material for expression," that is, as a medium rather than a tool. This vision drives education 3.0 and makes it possible to place computing within twenty-first-century literacies, not just as a set of e-skills, but as part of an enabling environment where "computational thinking" (Wing 2006) meets "information cultures" (Serres 2012).[16]

This thinking is supported by a paradigm shift resulting from the multi-layered transformation of the notion of

[13] See Strauss (2014).

[14] See www.clemi.fr (in French) for the role of CLEMI (Centre de Liaison de l'Enseignement et des Médias d'Information) in the education community in France. With Sorbonne Nouvelle University, CLEMI participated in a massive open online course (MOOC) (called DIY EMI; with DIY referring to "Do It Yourself" and EMI referring to MIL in French — Education aux médias et à l'information) for training teachers to build their own MIL projects, with support of ECO, a project funded by the European Commission Competitiveness and Innovation Framework. See https://hub5.ecolearning.eu/course/diy-do-it-yourself/ (in French and in English).

[15] See www.oercommons.org.

[16] The STEM (Science, Technology, Engineering and Math) alliance proposed by the New York Academy of Sciences addresses the computing issue by focusing on operational actions, which are mainly geared at using code for applications, captors and robots. See www.nyas.org/WhatWeDo/ScienceEd/GlobalSTEM.aspx.

Examples of New Frames of Reference for Schools Incorporating New Literacies

- France and *le plan de refondation de l'école par le numérique* (the plan to upgrade education via digitalization) (2013): MIL became part of the basic transversal competencies and together with computing/coding, is an additional subject for schools with the creation of a new direction for digital in education and CLEMI as the main operator.

- Belgium and Conseil Supérieur de l'Education aux Médias (the high authority for media education) (2013): Digital literacy was added to MIL competencies established in 2008.

- Finland and the Finnish National Board of Education (2015): It was decided that schools (for students aged seven to 15) will teach by subject and by topic, with a focus on "multiliteracies" as a cross-disciplinary theme and linked to the Finnish language, and a "co-teaching" approach to lesson planning, with input from more than one subject specialist, as well as coding included in math courses.

information that refers to news (media and communication), to documents (library and information sciences) and to data (code and informatics). This change is based on MIL as a "transliteracy," which is fostered by the convergence of computation (computer literacy), communication (media literacy) and info-documentation (information literacy). The competencies required for MIL are operational (code, compute, process), editorial (curate, evaluate, publish) and organizational (search, navigate) (Frau-Meigs 2012c).

Such MIL competencies come with a repertoire of online strategies, such as searching, curating, remixing, pooling, networking and gaming (Jenkins, Purushotma and Weigel 2009). They integrate computing and big data with media. They rely on critical thinking and creative skills to move toward transformative literacies based on competences, values and ethics. They go beyond current policies for IT or e-skills that put little stress on the shared values that make sense for children and educators alike (Frau-Meigs 2013a; van Deursen and van Dijk 2010).

These competencies rely on two major principles of Internet governance, openness and interoperability, to make it possible for young people to gain mastery over codes, content and data online. To facilitate such mastery, media platforms and social networks need to be interoperable and, as a result, (re-)mixable and ubiquitous. This mastery fosters reflexivity (looking back at diverse data), collaboration (mixing and remixing data with other people) and creativity (from learning by imitating to learning by doing and simulating). Consequently, children can move beyond the confines of the controlled spaces of tablets, apps and Internet services that shape their leisure experience and explore other activities, platforms and devices.

However, these Internet governance principles, if weakened or undermined, may affect the development of MIL and of education 3.0 at large. For instance, openness is being threatened by the current intellectual property system (which does not allow much space for exceptions in the context of education and research, in particular in the area of media content and software code) and by policies against network neutrality. Interoperability is affected by the economic battle that companies fight so their proprietary standards can be adopted in spaces such as the Internet Engineering Task Force. In general, there is a lack of legal certainty surrounding the use of the Internet. As a result, children and their parents do not always know how to behave in a lawfully responsible manner online (which may lead to unintentional criminal behaviour by young people); teachers and educators feel the same and are concerned about the validity of their online uses for the classroom (which may lead to a chilling effect and disuse or under-use).

Recommendation One: Make MIL twenty-first-century basics of the school curricula.

The Governance of Data for Education 3.0

MIL and other basic digital skills need to be put in the framework of innovative pedagogies supported by digital tools, structured around concepts such as constructivism that posit that the learner is a constructor of information. The recent arrival of MOOCs, with their attendant learning models, tends to recombine socialization and personalized learning styles (Frau-Meigs 2015). Like other online forms of teaching — albeit on an unprecedented scale — MOOCs build on learning analytics, defined as "the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimising learning and the environments in which it occurs" (Siemens 2011). A number of global companies in the ICT-driven learning business, also called "edtech," are pushing for their generalization, and they are gradually becoming more prevalent in schools and universities.

Learning analytics are double-edged for young people as learners: they can have a positive impact in the classroom as they can indicate to teachers where learners have difficulties and help them prepare appropriate and age-sensitive materials for them. As such, they can help bolster well-being by providing attention and fostering motivation in learning. But they can also present risks, as currently nothing prevents corporations from using them commercially in combination with external data on income, health, location, and so on. The governance of data for education should include thinking about who is going to manage and own the data, and for what uses, within and beyond education. Children's early awareness and understanding of these uses can ensure that they remain in control of such data in their lifelong evolution and manage them as "self data," in relation to their right to consent to any terms of service proposed to them.[17]

So as to ensure that this innovative tool does not bring about a great disservice to open education, institutions as well as individuals need to focus on the data generated by learning analytics and their commercial and non-commercial uses. Currently, there is no regulation of big data for education, yet their uses should be clearly specified, and in the best interests of the child as risks related to privacy, security and dignity are involved. The issue of protection of such data are important for the healthy development of learning analytics, geared to school and classroom use specifically.[18] The conditions of their availability (open, anonymous, private), members of the public who are authorized to use and consult them (child, family, teaching body, business), their relation to other available data (allowed or not allowed, for sale or not for sale), all need to be specified to preserve the public value of education, also vis-à-vis the public service value of the Internet.[19]

Teachers — and the teaching body in general — are resistant to the entrance of big data and digital learning in schools, as there is no policy for the protection of their work and of the well-being of children. They are concerned about the digital footprint of their students, which could lead to undue surveillance risks (these could apply to the monitoring of their own performance as well). This creates a loss in the potential of big data to become small data or self-data to help them and their students in their everyday work. The principles of transparency, accountability and ethics in Internet governance should be considered as a best practice in order to help the public management of such data. In particular, states and local authorities should pay attention to their use, in particular if it is capable of leading to segregation and competition among schools.

Recommendation Two: Regulate data management for learning.

Education on Internet Governance Processes and Principles and Human Rights

Children, like adults, are Internet users with human rights that apply online as well as offline.[20] Notwithstanding their right to be protected from harm, they should be able to exercise and enjoy their rights to privacy, opinion and information; assembly and association; education; and participation.[21] These universal human rights are also reinforced through the Convention on the Rights of the Child (CRC), in particular in terms of freedom of expression, the importance of the media and protection against materials detrimental to their well-being, and education and protection from violence.[22] The CRC states that adults and states have three public policy obligations with regard to children: protection (as they are vulnerable); provision (of first- and second-degree necessities such as health and education); and participation (whereby children should be associated to matters that concern them). These rights and obligations fit with the development of their capabilities and well-being and, in the context of Internet governance, should enable them to be heard and contribute to decision making and -shaping on matters affecting them without discrimination on any grounds (Frau-Meigs 2011; Liddicoat and Doria 2012).

Progressive interpretations of these rights by states, international and regional organizations, and national and regional courts, enable human rights to evolve in cyberspace in a seamless manner, regardless of frontiers or media types and formats. For example, access to and freedom to use the Internet can be considered as an increasingly integral part of the right to freedom of expression and access to information online (Association for Progressive Communications 2006). In the aftermath of the revelations of National Security Agency contractor Edward Snowden, anonymity and encryption are seen as enabling free expression (Article 19 2015). Similarly, the removal of online traces of children, as part of "the right to be forgotten," is important for children's right to privacy.

In Internet governance dialogues, children who understand both their human rights and the shared

[17] See the complaint of the Electronic Frontier Foundation about Google (www.eff.org/files/2015/12/01/ftccomplaint-googleforeducation.pdf).

[18] The leaking of personal data of students in Brazil, including their medical records, underlines the importance of data protection and of fostering the ethical understanding of MIL and digital literacy skills. See www1.folha.uol.com.br/educacao/2015/03/1604926-fichas-sobre-estudantes-de-colegio-tradicional-de-sp-vazam-na-internet.shtml.

[19] See CoE (2007).

[20] See United Nations (2012). The resolution affirmed that the same human rights people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and using the medium of one's choice.

[21] Respectively articles 12, 19, 20, 26 and 27 of the Universal Declaration on Human Rights.

[22] Respectively articles 13, 17 and 19 of the CRC.

values concerning the governance of the Internet have the potential to become powerful advocates of the Web they want. From an educational perspective, the view of the Internet as a global resource that should be managed in the public interest resonates with children's sensibilities about the world and society (Phatak-Shelat 2013, 2059–69; Elea 2015).

MIL and Internet studies need to be taught to young people as early as possible in order to prepare them as players, citizens and workers. In particular, they will need to know about Internet governance processes and principles and how they relate to their human rights, as well as being capable of developing advocacy skills in this domain. To do so, they need to be provided with a pedagogy for participation in education 3.0: contributive engagement is not an easy skill to acquire and needs to be elicited in very early stages of schooling, well before children reach legal decision-making age. In this manner, they will be able to make their feelings and opinions known to Internet governance actors and to monitor those who affect their lives daily (teachers, parents) and those who advocate for them in Internet governance events and forums.

Conflating the principles of Internet governance (universality, openness, neutrality, interoperability and diversity) with educational principles (access, competencies, inclusion and ethics) transforms the Internet and its governance into an educational field in itself. Shared values and human rights will hopefully converge until "code becomes law" (Lessig 1999), that is to say, until code upholds rights. Learning about and participating in the shaping of the Internet is therefore an integral component in the evolution of children's rights online, their well-being in education and their future employment opportunities.

Recommendation Three: Foster the active appropriation by children of their human rights and shared values including Internet governance principles and processes.

MIL and Internet Studies as a Frontier Field for Teaching, Learning and Researching

The parallel tracks of education and Internet governance can be multipliers for each other and are mutually reinforcing in education 3.0. But for this to be effective, there needs to be a continuum between primary, secondary and university education. MIL and Internet studies can provide such a continuum as young people can be exposed to basic uses and principles at an early age and encouraged to continue by participating in communities of practice where researchers, teachers and young people interact. MIL and Internet studies can be connected to digital and scientific humanities, combined with Internet-based "citizen sciences" (also known as "crowd sciences" or "networked sciences"). By learning about co-production and co-design with adults, young people can participate actively and see how education 3.0 brings together many fields and disciplines while contributing to future developments.

MIL — recombined with Internet studies, to empower teachers and students alike — needs to be supported by university research and training in this emerging field. Its perimeter, core concepts and curriculum must be developed in order to build the mechanics and levers that can prepare the next generation of professionals in the field.

MIL is a case of frontier research different from mainstream disciplines. Like other emerging fields, it addresses issues that are in flux and controversial: it embraces several notions and touches upon other existing disciplines; it deals with new questions and proceeds with atypical methodologies; and it conducts research with a high degree of uncertainty as it tries to respond to new problems caused by a fast-changing environment (Kuhn 1962; Larédo 2014). As with much frontier research, it is potentially transformative and can shed new light on phenomena, thereby suggesting new ways of thinking and proceeding, eventually producing a paradigm shift. MIL and Internet studies can transform existing sciences and bring about a better understanding of digital scientific humanities. They should be treated as a carrier for the evolution of these disciplines and fields.

MIL and Internet studies as a frontier field can create visibility and lend legitimacy to the area they cover *and* be mainstreamed into other disciplines, in a cross-cutting manner. There is already a more or less formal network of Internet and society centres that could help solidify this frontier field.[23] Other networks, such as the Global Internet Governance Academic Network (GigaNet), already provide analysis on Internet governance worldwide and could serve as a catalyst for research.[24]

The academia and research constituency is well-represented in Internet governance, but mostly consists of legal specialists and political science analysts. Education and youth are considered a "soft issue" that is secondary to the primary goals and principles of Internet governance. There should be a platform of researchers as key independent partners in local, regional and international Internet governance bodies and events to carry out research on all aspects connected with education 3.0.

[23] See http://networkofcenters.net/research/internet-governance.

[24] See GigaNet's four major objectives (www.giga-net.org).

Recommendation Four: Support Internet studies and MIL as a frontier field in research and education.

ENLARGING MULTI-STAKEHOLDER GOVERNANCE IN EDUCATION

Education needs to embrace the multi-stakeholder process of Internet governance so that children have a recognized place in the networked society, not only in schools but also in other spaces where they gather and learn. Traditional actors and institutions related to education outside schools such as universities, libraries or publishers have each evolved in their separate missions and need to reconnect and find new ways to interact with each other around children and young people. They also need to accommodate new entrants in the field to share the processes of participation and the inclusion of young people in education, and to point to new solutions for citizenship, capacity building and employability.

Re-aligning Existing Actors in Education Networks

The larger circle of educational providers (libraries, publishers, universities, and so on) are affected by the Internet's ever-dominating presence and rapid pace of development. New digital actors are emerging in and out of school spaces, such as media community centres and open facilities including "fablabs," and "makerspaces," equipped with operative technology (lasers, captors, 3D printers), where learning-by-doing is promoted and where young people meet adults with innovative pedagogies.[25] These different porous spaces stimulate MIL and the meshing of computational thinking with information cultures as they provide technology and education to a multi-generational public. Notwithstanding adult guidance and supervision, children can also be part of co-education and the co-construction of knowledge.

Libraries are a major stakeholder at the local and national rungs of Internet governance in education and can incorporate fablabs in their buildings. They play an important part in the transition to information cultures and literacies, in particular in developing countries or countries where digital inequalities are considerable, such as India (Jaeger et al. 2012). They can facilitate reading and writing for poor children who do not have access to Internet infrastructure, who cannot pay prohibitive prices for commercial tablets, who lack basic digital literacy or who need to be assisted by technologies because of a disability.[26] Initiatives such as Libraries Without Borders, which translates in French all the online courses of the Khan Academy, show the power of libraries in Internet governance for learners.[27] The International Federation of Library Associations and Institutions advances this potential for libraries in the Lyon Declaration on Information and Development.[28]

The publishing sector is changing its business models because of, *inter alia*, new entrants in education, such as Google, Apple, Facebook, Amazon and Microsoft. Yet the traditional publishing sector is necessary in order to assure academic quality, criteria for local content and scientific production, and certification (CNNum 2014). Publishers provide manuals and resources that reassure teachers and professionals as to the relevance of the materials they use for teaching. Publishers and editors can be seen as levers for MIL as transliteracy and for mainstreaming good practices. To this end, they must revise their strategies for editing and publishing in the digital era. Educational content online requires clear norms and standards, including those related to creative commons. An exception to intellectual property rights also needs to be negotiated for education 3.0, as part of Internet governance principles (openness, diversity).

To foster Internet governance in education, the role of publishing start-ups and intermediaries is important for local development and sustainability. In Brazil, for instance, repositories of online material (books, papers and pdfs) function as "shadow libraries" that allow students access to content they would not be able to obtain otherwise via commercial platforms such as Dropbox and Whatsapp.[29] Start-ups can use MIL and digital strategies to enhance public and open source content, with the help of digital tools such as software for course design, 3D printing for local dissemination, and so on. Young people and teachers can contribute to manuals and tool kits, through their online comments, in a process of co-design, defined as collaborative problem solving. This points to new directions for the public service value of private sector services and for private-public partnerships.

[25] Examples in France are numerous: le cube (www.lecube.com), le bal (www.le-bal.fr), la casemate (www.lacasemate.fr); see also the whole worldwide network of fablabs initiated by MIT in Singapore, Japan, Argentina, and so on.

[26] See Robobraille, a web-based service that converts documents into a range of accessible formats including Braille, mp3 and Daisy; see Biblus, the digital library companion of RoboBraille, which is a collaborative platform among all special schools for the visually impaired (www.robobraille.org).

[27] See www.librarieswithoutborders.org/index.php/what-we-do/our-programs/abroad/transversal-programs/item/280-the-khan-academy-in-france-and-the-francophone-world.

[28] See www.lyondeclaration.org.

[29] See Brazilian-led project "Shadow Libraries: the ecology of access to educational materials in developing world" (http://direitorio.fgv.br/projetos/shadow-libraries-the-ecology-of-access-to-educational-materials-in developing-world).

Universities are also essential for the training of future teachers, and young people should be encouraged to participate in events and activities at an early age, well before they register for a specific degree. They can incorporate fablabs and makerspaces in order to engage more with their local environment. In such porous spaces, the digital and scientific humanities, combined with Internet-based citizen sciences, can enable young people to get involved in the collection and interpretation of data, including data that are of interest to them. When young people are able to do so, such as, for example, exploring the data of their local authorities, they often investigate how they can improve their environment.[30] Open archives, e-government data and social networks that are set up for monitoring and training can have an impact on publishing, editing and research that incorporates emerging citizens. Young people, as a community of practice, can be incorporated into the networks and fablabs that are currently participating in a variety of local development initiatives (incorporating families, teachers, non-governmental organizations [NGOs], and so on). They may also promote their own interests beyond mere demand of the masses and market force demand-supply strategies as exemplified by associations such as les Savanturiers, where children follow the adventures of space exploration probes or look at environmental issues such as pollution to come up with alternative solutions.[31] They can move knowledge management away from the corporate sphere of organizational efficiency to their own process of sharing and of using information cultures for learning and researching by doing.[32]

Global multi-stakeholder education initiatives already exist. WISE addresses the "widening gap between the education systems currently in place and those required to meet the needs of future generations."[33] The UN Alliance of Civilizations (UNAOC) has a program for MIL as well as a program for Young Entrepreneurs for Social Change that addresses issues of conflict prevention and collaboration across borders.[34] Yet these initiatives tend to be absent from Internet governance forums and they do not address directly Internet governance issues within their own mandates.

Recommendation Five: Bring together multi-stakeholder governance actors, including children and young people, around the co-design of education 3.0.

Employment and Employability

Young people are among the most vulnerable groups in terms of unemployment. Their situation varies around the world but they are often exposed to cycles of poverty and cutbacks in public welfare, not to mention warfare and displacement. In Europe, recent reports point to a "lost" generation with attendant risks for cohesion, solidarity and political stability as evinced by the emergence of youth movements that have spread worldwide, such as Occupy or Indignados. This situation has consequences on families and puts stress on children, with increased risks of violence, neglect and illiteracy (United Nations Children's Fund [UNICEF] 2014; Child Helpline International 2013). It lays the emphasis on reducing "illectronism" (illiteracy in MIL and e-skills) and rebooting schools for employability (Frau-Meigs 2011). "Employability" is not about employment *strico sensu*, it is about creating the conditions for jobs, about fostering the functionings and capabilities that can lead a young person to be engaged in the workplace and make empowering life choices.

Mismatch: The Lack of Transition from School to Work

Many developed and developing countries are experiencing high numbers of school dropouts — young adults (aged 15–25) who have no job and little education or training, often without a school diploma, not to mention a university degree (Organisation for Economic Co-operation and Development [OECD] 2011). France, for example, has a 12 percent dropout rate before the end of compulsory education. These young people are estimated to each cost tax payers about €300,000 (Delahaye 2014). In Africa, dropout rates start in primary education, with household wealth and location (rural) impairing opportunities: they are highest in Chad (72 percent), Uganda (68 percent) and Angola (68 percent).[35]

At the same time, many new jobs that rely on MIL and e-skills are not filled. The data vary worldwide, but consistently show that one in five ICT positions are currently unfilled due to a lack of suitable workers. These jobs could reach as many as seven million worldwide by 2015 (International Data Corporation 2012). At the same time, greater numbers of low-qualification jobs are being occupied by young people who are over-qualified. This situation has been identified as a skills "mismatch" — the

[30] See DATAVIZ projects by Frequence-écoles that train young people in data gathering and data visualization (www.frequence-ecoles.org/tag/dataviz/).

[31] See les-savanturiers.cri-paris.org/.

[32] Knowledge management could be part of MIL and Internet studies as frontier field. It is itself a frontier field, established since the 1990s as a discipline that includes information systems and information sciences and, increasingly, media and communication, health administration and public policy.

[33] See www.wise-qatar.org.

[34] See www.unaoc.org.

[35] See www.unesco.org/new/en/dakar/about-this-office/single-view/news/42_of_african_school_ children_ will_drop_out_before_the_end_of_primary_education/; see also www.uis.unesco.org/Education/Pages/global-education-digest.aspx.

result of a poor transition from school to work (Global Agenda Council on Employment 2014, 11–15).

This mismatch is, in part, due to the fact that schools and universities still tend to associate computing and digital literacy to high levels of skills. Those advising children, and their parents, in schools and local job centres should be better trained at pointing to these opportunities for low levels of skills that, nonetheless, require some modicum of digital literacy, as even industrial mechanical jobs require basic e-skills. A lack of relevant certification and of appropriate training is also a key factor.

In the absence of adequate MIL and e-skills, the ICT industry finds its own solutions to fill these new positions, such as creating its own training centres, "second chance" schools, youth incubators and co-op arrangements with universities, whereby learners spend half their time on the job. A rising phenomenon everywhere, including in the Global South (in particular India and Africa), these start-ups include many young people in their ranks, with or without university degrees or diplomas. Start-ups combine work-based learning with theoretical learning in schools and facilitate access to hands-on work experience for young people, improving their views on the workplace and their job prospects.

In all industrial sectors, matching skills and jobs has become a priority. Young people can be affected by high rates of unemployment among their ranks, and there is a growing consensus that opportunities to learn on the job and to receive continuing training are necessary. The combined "learn as you earn" philosophy seems to be modifying the relationship between schools and universities.

In addition to upgrading jobs in the traditional industrial sectors, the Internet produces its own creative industries that are participatory by nature and call upon crowd-sourcing and crowd-funding. An array of careers available without a proper university degree certifying them as jobs are emerging: YouTuber, modder, game player, web designer, front-end developer, community manager, content strategist, fablab manager, trainer in mobile uses, and so on.[36] The online global youth culture tends to celebrate those young people among them who started well before the legal working age in many countries, often while still at school or in the process of dropping out of education, who made their success story in YouTubing or game playing.

However, among these emerging jobs, gamers and modders are in a situation of precarious labour, also called "playbour,"[37] which is part of the commodification of youth cultures worldwide. It tends to exploit young people (typically 18–25, sometimes younger) who play as labour, "gold farming" in online gaming factories (Barboza 2005). Some experts suggest that play will be to the twenty-first century what work was in the twentieth century: the definer of roles, status, lifestyle, learning, money making and value production (Kane 2010). The private sector is already tempted to use play as a kind of work ethic, with corporate efficiency about skills and consumption via the immersive experience of gaming. The regulation of commercial playbour and employment safeguards are necessary to protect children's activities online, promote well-being and encourage creative industries and start-ups.

The Creative Industries for Training and Learning

Among the Internet-based creative industries, there is the strong emergence of new businesses for training and learning, with a growing stake in education 3.0. In addition to the traditional businesses already engaged in e-learning (such as Microsoft and Pearson), there are new entrants leaning heavily on data analytics for edtech (such as Coursera and Cloudera). They are targeting universities and they are making inroads into primary and secondary school education (Innovative Technologies for Engaging Classrooms 2013).

The digital economy has a stake in education 3.0, not just to recruit the future workforce. The private sector is rapidly embracing this vast field, using international digital networks to advance its positions. Besides the United States and South Korea, some emerging countries, as well as the United Arab Emirates, are most active in developing these new businesses that recombine funding, technology and networked teacher training. They are aiming at globalization as a means of maximizing their profits and draining public funding in all regions (as the budgets for education in all countries amount to staggering figures in the range of billions of US dollars).[38] As states' budgets become more challenging to control and are in crisis over public spending, these companies propose their own learning solutions, which also implies privatizing part of public education and benefiting from public funding for their private strategies.[39]

[36] See job descriptions and specifications available at www.netpublic.fr/dispositif-emplois-davenir-en-epn/ (in French). A modder is a player who is encouraged to make "modifications" to games.

[37] Expression first coined by Julian Kücklich (2005), and negatively defined as "exploitable (info-)labour that feels like play."

[38] See World Bank statistics (http://data.worldbank.org/data-catalog/world-development-indicators).

[39] See United Nations Educational, Scientific and Cultural Organization (UNESCO) statistics on education for ranking of countries in terms of their GDP spending (http://www.uis.unesco.org/Library/Documents/ged07-fr.pdf).

These strategies involve engaging the young audience — a potential major consumer group of online goods — as early as possible. There is an additional lure for young people that has to do with the Internet industry's online discourse, which increasingly reconfigures education as learning by doing and by playing outside brick-and-mortar schools. It offers child-friendly do-it-yourself tutorials, dynamic online courses, YouTube scenarios, and so on. It is already capturing a lot of informal learning for children, which relies increasingly on peer-to-peer solutions (van Deursen and van Dijk 2010).

This discourse is casting a positive light on education as innovation and creativity, the allure of which is difficult to resist. Some select youth social entrepreneurs become corporate entrepreneurs, but this is not the reality for most young people. In fact, the corporations of the digital world are still seeking most of their troops and managers from the elite schools, preferably in engineering. Internet governance in education needs to think about the children left behind. In many developing countries, families bear the cost of education, adding to the digital and economic divide. The privatization of education without proper governance can create significant problems in both the north and south. The Internet governance principle of diversity must be called upon, for the sake of social justice and sustainability. It can put forward public-private partnership strategies for training teachers, including distance learning. It can promote transfer, by translations, the re-design of resources, and the localization of content that can benefit developing and developed countries alike.

Recommendation Six: Harness the potential of creative industries for learning and training.

SHARING THE RESPONSIBILITY OF THE INTERNET GOVERNANCE OF EDUCATION: PROTECTION, PROVISION AND PARTICIPATION REVISITED

In the multi-stakeholder process of Internet governance, three major stakeholders have been implicated since the beginning: the public sector and governments; the private sector and business; and the civic sector and civil society (NGOs, foundations, and so on). All three pillars need to be brought around the table to consider how Internet governance can support education 3.0, beyond the scope of educational institutions. Having all stakeholders share the responsibility of supporting its development, including their own participation, creates a continuum between all sectors of society.

Among these stakeholders, the role of the state is key to ensure that all the competing actors contribute to the process in a balanced and fair manner. States should ensure that human rights, MIL and education 3.0 interface with the processes of accountability and transparency. They should also move beyond the strict principle of subsidiarity that contains education, in particular by calling on inter-governmental organizations and forums such as the IGF, UNICEF, UNESCO and the CoE, to increase the public debate on education 3.0 and Internet governance so that the benefits of shared values can be redistributed to all.[40]

The Private Sector and the Unaccompanied "Solo" Kids Online

The issue of creative industries and playbour points to a complex online environment, with the need for increased safety and security concerns to be balanced with new participatory opportunities. Children are mostly alone on the Internet, dealing with commercial services and applications. This situation raises concerns about the profiling of information and the retention of personal data regarding children's activities for commercial purposes.[41]

As ever younger children access the Internet, the corporate sector has a vested interest in lowering the age barriers of Internet consent (from 13 down to eight), and uses the access to education argument for lobbying purposes.[42] The sector is effectively not treating young people online as children but as consumers (and even prescribers to their parents), whose uses attract a lot of attention in marketing research.[43] For this reason, one of the key issues that resonates with parents and young people alike relates to "terms of service," regularly denounced as being too abstract, not child-friendly, and effectively depriving young people of their agency and their property rights. Another key issue, which resonates with teachers more specifically, is the introduction of such commercial services in schools because they are not geared for pedagogical uses, and they can conflict with state regulations that protect children.

Online content and service providers, in particular, have a responsibility to respect the human rights of children on the Internet.[44] This responsibility implies exercising due diligence to protect them from harmful content and

[40] See the CoE Pestalozzi programme for teacher training in ICTs (www.coe.int/pestalozzi).

[41] See CoE (2008).

[42] See www.zdnet.com/article/mark-zuckerberg-facebook-minimum-age-limit-should-be-removed/.

[43] Statistics from the French Conseil économique, social et environnemental, the OECD and so on exemplify this focus on use.

[44] In line with Resolution 17/4 on human rights and transnational corporations and other business enterprises, adopted by the United Nations in June 2011.

behaviours, to respond to their complaints and to educate them with guidance.[45] They should be encouraged to listen to young people and, where necessary, adapt their services (for example, simpler terms of use, information about re-use of content, replying to questions about the safety, security and privacy policies of services). This promotes the critical thinking and confidence of children who are often alone on the Internet (for example, managing their image and reputation online).[46]

A healthy relationship between children and the providers of these services is needed. This dialogue can be initiated and fostered in a setting that is more equal-footed within the context of Internet governance. Defining the providers' ethical responsibilities when children use their services (irrespective of whether they are of the requisite right age or not) is crucial. This implies that companies revamp their corporate social responsibility (CSR), away from pre-digital "do-good" patronage, to ensure that it incorporates provisions for children and education. At the moment, not enough CSR initiatives target education as a main focus.[47]

CSR should be part of the dialogue ensuring that children are educated as online consumers. Terms of service, "consent" by minors, issues of filtering and blocking need to be part of a larger discussion that encompasses the data footprint, privacy, freedom of expression and education. This should empower schools and libraries where children need to have access to quality content and freedom of expression and creation. The self-regulation by the private sector is not enough, as parents often perceive it as biased in favour of corporate interests. The multi-stakeholder approach to co-regulation has been temporarily solved by parental controls, but such technical means places the onus solely on families and are only useful up to a certain age. Besides, they are not protective of the vast majority of children in the world where parenting situations are disturbed by separation, displacement, immigration, war, and so on.

Co-regulation lends itself also to protection by design, which blends in with participation and MIL: children and parents alike can be sensitized regarding their roles as critical participants online in order to control their screen time and to express choice. Children's roles should be fostered as sources of information and data collection to build proper sets of indicators (Ben-Arieh 2005). Protection by design can thus provide guidelines that are age-sensitive and set into internationally agreed upon industry standards.

Recommendation Seven: Reboot the CSR of the providers of Internet content and services to support education 3.0.

The Civic Sector and the Constituency of Young People

Civil society groups that have evolved around Internet governance since the WSIS have lost some of their capacity for disruptive innovation in global network negotiations (Belli 2014). This loss of influence is partly due to the limited capacity of civil society to renew itself and to produce Internet governance-savvy members who are trained in such complex consultations. Civil society has a vested interest in fostering youth participation as part of its own capacity to replenish its ranks and contribute to the shaping of the future of the Internet, in particular by fostering the children/youth caucus within the Internet governance ecosystem.

Currently, there is not a sustained presence of children in Internet governance as they are not a stakeholder group. The Dynamic Youth Coalition on Internet Governance was founded in 2009 at the Sharm El Sheik IGF but has been relatively inactive since. Various other existing regional youth forums (in, for example, Asia, Europe and Africa) have not proven to be very effective. The challenge is really how to move from tokenistic children's participation where they are brought to events to speak about a specific issue toward a genuine voice of many children from different backgrounds. Online platforms offer that option, but they exclude those children who do not have access. Children, with the help of adults, need to work on peer-to-peer strategies that are effective online and offline so that they can be their own spokespersons and drivers of policy. Such achievements cannot be reached without education and coaching, in the same way as adult participants are trained.

Some countries, such as Finland, are experimenting with children's parliaments. The Finnish Children's Parliament is comprised of approximately 380 children aged nine to 13.[48] In India, similar efforts are being made at a smaller scale in diverse locations, such as Shaishav in Bhavnagar.[49] In the United Kingdom, young people voted on a digital "Magna Carta," which has gained the

[45] See CoE (2012): young people should be afforded guidance "in order to manage their profiles and understand the impact that the publication of information of a private nature could have, in order to prevent harm to themselves and others."

[46] See ibid.: "social networking services play an increasingly important role in the life of children and young people, as part of the development of their own personality and identity, and as part of their participation in debates and social activities."

[47] Vivendi's action in Africa with music development and training for young people in Mali (www.vivendi.com/social-responsibility/) is an example of an initiative where education is an element of CSR.

[48] See http://ec.europa.eu/justice/news/consulting_public/0009/contributions/unregistered_organisations/139_finnish_childrens_parliament.pdf; see also Kotilainen (2009).

[49] Shaishav, which means childhood in Gujarati, is a volunteer organization committed to the rights of children and child labour; see www.Shaishavchildright.org.

attention of the media and could compel some Internet corporations to modify their behaviour. In the light of such developments, the absence of youth from Internet governance dialogues could challenge the legitimacy of the Internet process itself. Their presence among the constituencies of civil society could modify the traditional patterns of representation and deliberation.

To make their participation more equitable, more distributed and more meaningful, a double strategy is advisable: make children a driving force in Internet governance in order to encourage them to make the case for themselves and to participate in co-design and co-decision making; integrate youth in the agenda of like-minded associations that have created trust around their authentic treatment of children (for example, UNICEF, UNESCO, and so on). Accountability mechanisms also have to incorporate youth by means of advocacy for children (teens speak for pre-teens) and by training adults to listen and to be accountable to them.

Recommendation Eight: Engage children and young people in Internet governance as a more effective stakeholder group within the ranks of civil society.

The Public Sector and the Role of Public Action and Social Innovation

Within the framework of governance, the state is no longer a kind of monolith, but a network of many rungs and actors with more and more decentralized services, local authorities and public agencies that are empowered by digital networks. The public value of the Internet is a notion that is making its way, and modifying the very notion of public action, in association with social innovation defined as initiatives taken by citizens in their own hands, in areas the state does not consider as priorities (European Commission 2013). Many initiatives show social innovation revolving around principles of Internet governance that are congruent with principles of C4D and interactions between online opportunities and offline needs. Microcredit, supported online by crowd funding or crowd sourcing, belongs to such initiatives, aiming at sustainability with emphasis on local life and culture (Frau-Meigs 2013c; 2012b, 45–55).

Social innovation policies that encourage social entrepreneurship relate to governance at regional and local levels and are associated with the rise of civil society as an actor and a partner of more traditional public agents (Laville 1994; European Commission 2013; Klievink and Janssen 2014, 240–249). In Africa, Asia and Latin America, social innovation paves the way for the participation of young people as they form a large demographic in these regions.

Initiatives Showing That Internet Governance Principles Are Already Being Applied with and for Children and Create New Forms of Mobilization and Education

- Ushahidi ("testimony" in Swahili), created by Juliana Rotich, is of one of the most used open source apps in Africa. It uses crowdsourced geolocation and mobile phone data to provide web crisis reporting and information. [50]
- Apps4Africa, organized by Mariéme Jamme, CEO of SpotOne Global Solutions, is a yearly competition that mentors and supports young people to shape Africa's tech revolution.[51]
- Youth Ki Awaaz is India's largest online community media platform run by young people for young people to express themselves.[52]
- PLURAL+ is a Youth Video Festival, with international awards in three age categories (9–12, 13–17 and 18–25).[53]

To encourage social innovation, national laws need to create an enabling environment for start-ups and small companies (part of civil society in the WSIS process). In many countries, strict bankruptcy laws, ponderous administration procedures and prohibitive banking loans make it very difficult to start new enterprises, in particular if a previous venture has failed. These risks discourage young people. Many governments still do not recognize social innovation in creative industries. For example, the National Plan for Cultural Development in Brazil speaks of creative industries, but focuses on provisions to traditional sectors, such as music and television, and does not support the video games sector.

Such examples suggest that policy makers at all levels of government, inside and outside education, need updated training for change management and knowledge management, with full accountability. The collateral challenge is to develop indicators that hold societies and governments accountable for more than safekeeping of young people. Decision makers should stop postponing children's "well-becoming" into the future (adulthood) and focus on the immediacy of their well-being. Applied

[50] See www.ushahidi.com/.

[51] See www.africagathering.org/team/executive/marieme-jamme/.

[52] See www.youthkiawaaz.com/.

[53] See wwww.pluralplus.unaoc.org.

to policy making, this suggests closer consideration of the principles of Internet universality as applied to young people, such as access, freedom of expression, local content, quality literacy, privacy and ethics (UNESCO 2015).

Recommendation Nine: Invite public authorities to consider and collaborate on education 3.0, in particular to develop indicators and accountability mechanisms for next-generation (age-sensitive) policies and social innovation.

CONCLUSION AND NEXT STEPS

Well-being and capacity building are necessary elements of sustainability and development for the next billion Internet users, many of whom will connect as children. Creating the right environment for them with regards to the Internet requires education and research. It is incumbent on all stakeholders to promote a healthy and positive agenda for children — the contours of which need to be discussed and co-designed with them. This agenda should encourage children to be active citizens of the Internet.[54] It should promote their well-being and the exercise of their rights and freedoms. It should stimulate their creativity and collaboration. It should address citizenship and responsibilities. It should connect schools and job markets. It should engender a vibrant civil society where the Internet is really a bottom-up social space, the governance of which is constructed democratically.

The way forward is threefold: MIL and Internet studies as a frontier field; a multi-stakeholder structure of networked actors in education; and a mobilization in favour of education 3.0 in Internet governance. A road map for the Internet governance of education should define priorities, with critical milestones over the next five to 10 years, in line with the UN post-2015 SDGs, such as:

- Education 3.0 responds to the crucial needs of citizenship, capacity building *and* employability. This requires that a minimum number of national curricula across continents make MIL and Internet studies into a core discipline of the education system in schools (that is, not as a subject that acts as a conduit but as a discipline in itself), coupled with human rights.

- Education 3.0 addresses children’s level of autonomy and empowerment. This implies accepting that online agency is higher than it is offline (that is, starts from a younger age). Part of this response means turning “solo kids” online into the collective efforts of young people with advocacy skills who can express themselves, assemble and associate, as part of the exercise of their human rights.

- The Internet governance multi-stakeholder community supports the sustainable digital development needs of children and young people. This implies that a minimum number of national, sub-regional, regional and global Internet governance spaces are created and mobilized that engage and recognize the voice of children and young people in the dialogue and design of Internet governance policies.

These milestones should be discussed and coordinated at the international level by the United Nations, in particular by disseminating this chapter as well as in organizing dialogue across continents. To this end, the creation of the position of UN Special Rapporteur on education 3.0 for children and young people’s sustainable digital development could help to coordinate and promote coherent and dynamic engagement of all stakeholders, one that facilitates a shared vision in and beyond education as put forward in the 10 recommendations of this chapter.

Recommendation Ten: Create the position of UN Special Rapporteur on education 3.0 for children and young people’s sustainable digital development.

Authors’ Note

This chapter reflects the opinions and views of its authors only. We gratefully acknowledge the valuable reviews and generous comments from Jasmina Byrne, John Carr, Sirkku Kotilainen, Eve Leckey, Sonia Livingstone, Marilia Maciel and Manisha Shelat in the preparation of this chapter.

[54] See CoE (2016).

WORKS CITED

Article 19. 2015. "UN expert launches robust defence of online anonymity and encryption." May 28. www.article19.org/resources.php/resource/37979/en/un-expert-launches-robust-defence-of-online-anonymity-and-encryption#sthash.aBgnvh5f.dpuf.

Association for Progressive Communications. 2006. "APC Human Rights Charter." www.apc.org/en/node/5677.

Asthana, Sanjay. 2012. *Youth Media Imaginaries from Around the World*. New York, NY: Peter Lang.

Barboza, David. 2009. "Ogre to Slay? Outsource It to Chinese." *The New York Times*, December 9. www.nytimes.com/2005/12/09/technology/09gaming.html?pagewanted=print.

Belli, Luca. 2014. "A heterostakeholder cooperation for sustainable internet policymaking." *Internet Policy Review* 4 (2). doi:10.14763/2015.2.364.

Ben-Arieh, Asher. 2005. "Where are the children? Children's role in measuring and monitoring their well-being." *Social Indicators Research* 74: 573–96.

Ben-Arieh, Asher, Ferran Casas, Ivar Frønes and Jill E. Korbin, eds. 2013. *Handbook of Child Well-Being. Theory, Indicators, Measures and Policies*. Heidelberg, Germany: Springer.

Chapron, Françoise and Eric Delamotte, eds. 2010. *La Culture informationnelle*. Lyon: Presses de l'ENSSIB.

Child Helpline International. 2013. *Voices of young Europe FWD*. June.

CNNum. 2013. *Citoyens d'une société numérique - accès, littératie, médiations, pouvoir d'agir : pour une nouvelle politique d'inclusion*. Paris: CNNum.

———. 2014. *Jules Ferry 3.0 – Batir une école créative et juste dans un monde numérique*. Paris: CNNum.

CoE. 2007. "Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet." https: //wcd.coe.int/ViewDoc.jsp?id=1207291.

———. 2008. "Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet." https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2820.02.2008%29&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

———. 2012. "Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services." https://wcd.coe.int/ViewDoc.jsp?id=1929453.

———. 2016. "Recommendation CM/Rec(2016)2 of the Committee of Ministers to member states on the Internet of citizens." https://wcd.coe.int/ViewDoc.jsp?id=2413803&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

Delahaye, Jean-Paul. 2014. *Evaluation partenariale de la lutte contre le décrochage scolaire*. Paris: Ministère de l'éducation nationale. www.education.gouv.fr/file/2014/85/8/Rapport-Evaluation-partenariale-de-lutte-contre-le-decrochage-scolaire_331858.

Dreyer, Stephan (von). 2014. "User Empowerment in child protection by & through Technology? Overview of the technical solutions." Presented at European Platform of Regulatory Authorities (EPRA) workshop, "Empowering users: rating systems, protection tools and media literacy across Europe." Strasbourg: EPRA.

Dubet, François, Marie Duru-Bellat and Antoine Vérétout. 2010. *Les sociétés et leurs écoles, Emprise du diplôme et cohésion sociale*. Paris: Seuil.

Elea, Ilana, ed. 2015. *Agents and Voices: A Panorama of Media Education in Brazil, Portugal and Spain*. Goterborg: International Clearinghouse on Children, Youth and Media.

EU Kids Online. 2014. *Findings, methods, recommendations*. London, UK: LSE. http://eprints.lse.ac.uk/60512/.

European Commission. 2013. *Guide to Social Innovation*. DG Regional and Urban Policy and DG Employment, Social Affairs and Inclusion. Brussels: European Commission. http://s3platform.jrc.ec.europa.eu/documents/10157/47822.

European Schoolnet. 2013. *Survey of Schools: ICT in Education*. European Union. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/KK-31-13-401-EN-N.pdf.

———. 2014. "ICT and Skills for Learning, Adult and Work life." Briefing papers, issue 7. May. www.eun.org/observatory/surveyofschools.

Fichez, Elisabeth. 2000. "L'industrialisation de la formation." *Terminal* 83: 65–72.

Frau-Meigs, Divina. 2011. *Media Matters in the Cultural Contradictions of the Information Society: Towards a human-rights based governance*. Strasbourg: CoE.

———, ed. 2012a. "Introduction" Contested Governance, *RFEA* 134: 114-124.

———. 2012b. "La diversidad cultural y la sociedad de la información: nuevas configuraciones y tendencias emergentes en cuestiones transnacionales." In *Quaderns del CAC* 38 (15): 45–55.

———. 2012c. "Transliteracy as the new research horizon for media and information literacy." *Meduske studije/Media Studies* 3 (6): 9–20.

———. 2013a. "Transliteracy: sense-making mechanisms for establishing e-presence." In *Media and Information Literacy and Intercultural Dialogue*, edited by Ulla Carlsson. Gothenburg: International Clearinghouse on Children, Youth and Media.

———. 2013b. "Child and Adolescent Well-Being From the Perspective of Media and Communication Studies." In *Handbook on Child Well-being*, edited by Asher Ben-Arieh et al., 437–84. Heidelberg: Springer.

———. 2013c. "La sociedad de la pantalla en la 'era ciberista': las industrias creativas en la agenda del desarrollo sostenible." In *Comunicación e Industria Digital. Tendencias, escenarios y oportunidades*, edited by Xavier Protzel. Lima: Felafacs.

———. 2015. "Augmented Media and Information Literacy (MIL). How can MIL harness the affordances of Digital Information Cultures?" In *Reflections on Media Education Futures*, edited by Sirkku Kotilainen and Reiio Kupiainen, 9–16. Gothenburg: International Clearinghouse on Children, Youth and Media.

Frau-Meigs, Divina and Jordi Torrent, eds. 2009. *Mapping Media Education Policies Worldwide: Visions, Programmes, Challenges*. New York, NY: UN Alliance of Civilizations-UNESCO.

Gauthier, Roger-François. 2015. "Des curricula au cœurs des défis : études de cas, Chine, Inde, Japon, Singapour." L'éducation en Asie, *Revue Internationale d'éducation* 68: 103–10.

Global Agenda Council on Employment. 2014. *Matching Skills and Labour Market Needs: Building Social Partnerships for Better Skills and Better Jobs*. World Economic Forum.

Innovative Technologies for Engaging Classrooms. 2013. *Designing the Future Classroom*." Issue 1. Brussels: European Schoolnet.

International Data Corporation. 2012. "Climate Change: Cloud's Impact on IT Organizations and Staffing." https://news.microsoft.com/download/presskits/learning/docs/idc.pdf.

ITU. 2013. *Measuring the Information Society*. www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf.

Jaeger, Paul T. John Carlo Bertot, Kim Thompson, Sarah M. Katz and Elizabeth Decoster. 2012. "The Intersection of Public Policy and Public Access: Digital Divides, Digital Literacy, Digital Inclusion, and Public Libraries." *Public Library Quarterly* 31: 1–20.

Jenkins, Henry, Ravi Purushotma and Margaret Weigel. 2009. *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century*. Cambridge, MA: MIT.

Kane, Pat. 2010. "Playbour: exploitation or civic possibility?"www.theplayethic.com/2010/03/possibilitiesofplaybour.html.

Klievink, Bram and Marijn Janssen. 2014. "Developing multi-layer information infrastructures: advancing social innovation through public-private governance." *Information SystemsManagement* 31: 240–49.

Kotilainen, Sirkku. 2009. "Promoting Youth Civic Participation with Media Production: The Case of Youth Voice Editorial Board." In *Mapping Media Education Policies in the World*, edited by Divina Frau-Meigs and Jordi Torrent, 243–59. New York, NY: AoC.

Kücklich, Julian. 2005. "Precarious Playbour: Modders and the Digital Games Industry." *The Fibreculture Journal* 5. http://five.fibreculturejournal.org/fcj-025-precarious-playbour-modders-and-the-%09digital-games-industry/.

Kuhn, Thomas. 1962. *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press.

Larédo, Philippe. 2014. "Supporting Frontier Research, which institutions and which processes." In *The Changing Governance of Higher Education and Research*, edited by Dorothea Jansen and Insa Pruisken, 189–207. Heidelberg: Springer.

Laville, Jean-Louis, ed. 1994. *L'économie solidaire, une perspective international*. Paris: Desclée de Brouwer.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York, NY: Basic.

Liddicoat, Joy and Avri Doria. 2012. "Human Rights and Internet Protocols: Comparing Processes and Principles." ISOC/APC paper. www.apc.org/en/pubs/human-rights-and-internet-protocols-comparing-proc.

Livingstone, Sonia, John Carr and Jasmina Byrne. 2015. *One in Three: The Task for Global Internet Governance in Addressing Children's Rights*. GCIG Paper Series No. 25. Waterloo, ON: CIGI and Chatham House.

Maeda, John. 2004. *Creative Code*. New York, NY: Thames and Hudson.

McAnany, Emile G. 2012. "Social Entrepreneurship and Communication for Development and Social Change. Rethinking Innovation." *Nordicom Review* 33: 205–18.

Moeglin, Pierre. 2005. *Outils et médias éducatifs*. Grenoble: PUG Grenoble.

Nordic Youth Delegation. 2012. "We need Internet Governance in education." European Dialogue on Internet Governance. http://2014.eurodig.org/eurodig-interactive/videos youtube.com/watch?t=10&v=3QvS75UqzWk.

Nussbaum, Martha. 2011. *Creating Capabilities: The Human Development Approach.* Cambridge, MA: Harvard University Press.

OECD. 2011. *Equity and Quality in Education — Supporting Disadvantaged Students in Schools*. www.oecd.org/edu/school/equityandqualityineducation-supportingdisadvantagedstudentsandschools.htm.

Phatak-Shelat, Manisha. 2013. "Media literacy and well-being of young people." In *Handbook of Child Well-Being*, edited by Asher Ben-Arieh, Ferran Casas, Ivar Frønes and Jill E. Korbin, 2059–69. Heidelberg: Springer.

Prensky, Marc. 2001. "Digital natives, digital immigrants." *On the Horizon* 9 (5).

Sen, Amartya. 1985. *Commodities and Capabilities.* Amsterdam: North Holland.

Serres, Alexandre. 2012. *Dans le labyrinthe. Évaluer l'information sur internet*. Caen: C&F editions.

Siemens, George. 2011. *"Learning and Academic Analytics."* August 5. www.learninganalytics.net/?p=131.

Strauss, Valerie. 2014. "All students should learn to code. Right? Not so fast." *The Washington Post*, May 29. www.washingtonpost.com/blogs/answer-sheet/wp/2014/05/29/all-students-should-learn-to-code-right-not-so-fast/.

UNESCO. 2015. "Universality Principles of the Internet: Rights, Openness, Access and Multistakeholderism (ROAM)." www.unesco.org/new fileadmin/MULTIMEDIA /HQ/CI/CI/pdf/internet_draft_study.pdf.

UNICEF. 2014. *Children of the Recession: The impact of the economic crisis on child well-being in rich countries*. Innocenti Report Card 12. Florence: UNICEF Office of Research — Innocenti.

United Nations. 2012. "The Promotion, Protection and Enjoyment of Human Rights on the Internet." A/HRC/20/L.13. www.ohchr.org/Documents/.../A.HRC.20.L.13_en.doc.

Van Deursen, Alexander and Jan A. G. M. van Dijk. 2010. "Measuring Internet Skills." *International Journal of Human-Computer Interaction* 26 (10): 891–916.

Wing, Jeannette M. 2006. "Computational thinking and thinking about computing." *Communications of the ACM* 49, no. 3: 33–35.

Working Group on Internet Governance. 2005. *Report of the Working Group on Internet Governance*. June. www.wgig.org/docs/WGIGREPORT.pdf.

ABOUT THE AUTHORS

Divina Frau-Meigs is professor of media and information and communications technology sociology at the Université Sorbonne Nouvelle, France. She holds several degrees, from the Sorbonne University, Stanford University and the Annenberg School for Communications (University of Pennsylvania). She is a specialist in cultural diversity, Internet governance and media and information literacy, as well as a researcher in the media uses and practices of young people. She holds the United Nations Educational, Scientific and Cultural Organization (UNESCO) chair "Savoir-devenir in sustainable digital development." She is the coordinator of the French National Agency Project TRANSLIT, on the convergence between media and digital literacies (www.translit.fr). She is responsible for the implementation of the European project ECO, within the framework program "Competitiveness and Innovation," which aims at producing MOOCs (massive open online courses), in particular to provide training in the fundamentals of digital humanities (www.ecolearning.eu). She is an expert with the European Union, the Council of Europe, UNESCO and a number of governments and institutions. She represents civil society interests (academia and research) in the Internet Governance Forum and in other global arenas.

Lee Hibbard is the co-ordinator on Internet governance at the Council of Europe, which is an international organization comprising 47 countries, set up to promote democracy and protect human rights and the rule of law in Europe. He is responsible for the Council of Europe's Internet Governance Strategy 2016–2019, including the setting up of a platform between governments and major Internet companies on their respect for human rights online. In recent years, Lee facilitated public policy on a range of issues including human rights for Internet service providers, network neutrality, freedom of expression on the Internet, and the empowerment and protection of children online.

CHAPTER THREE:
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

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

INTRODUCTION

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 chapter 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 chapter.

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

[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/.

framework is used to make a first measurement of the strengths and weaknesses of the MCI.

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

[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).

for this chapter — 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 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 chapter 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 application service providers (UNESCO 2012), determining

[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.

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.

[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.

What Remains Missing?

Implementation of the MCI

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

[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).

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 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

[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/.

- 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.

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.

<table>
<tr><th>La Rue Framework Standard</th><th>Is it addressed by the MCI? How?</th></tr>
<tr><td>State blocks or filters websites based on lawful criteria.</td><td>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.</td></tr>
<tr><td colspan="2"><b>Comment:</b> Refer to Section III, “FoE: Marco Civil’s Flagship” and “FoE and Intermediary Liability” for further details on FoE and intermediary liability.</td></tr>
<tr><td>State provides lists of blocked and filtered websites.</td><td>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.</td></tr>
<tr><td colspan="2"><b>Comment:</b> 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]</td></tr>
<tr><td>Blocked or filtered websites have explanation on why they are blocked or filtered.</td><td>Refer to Arts. 19 and 20 of the MCI.</td></tr>
<tr><td colspan="2"><b>Comment:</b> 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.</td></tr>
<tr><td>Content blocking occurs only when ordered by competent judicial authority or independent body.</td><td>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.</td></tr>
<tr><td colspan="2"><b>Comment:</b> 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.</td></tr>
<tr><td>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.</td><td>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.</td></tr>
<tr><td colspan="2"><b>Comment:</b> 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.</td></tr>
<tr><td>Defamation is not a criminal offence.</td><td>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.</td></tr>
<tr><td colspan="2"><b>Comment:</b> 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).</td></tr>
</table>

[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 chapter. 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 chapter 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 6. 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, 167–81. 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, Bruce. 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.

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.

CHAPTER FOUR:
A PRAGMATIC APPROACH TO THE RIGHT TO BE FORGOTTEN

Kieron O'Hara, Nigel Shadbolt and Wendy Hall

ACRONYMS

AEPD	Agencia Española de Protección de Datos
CJEU	Court of Justice of the European Union
DPAs	data protection authorities
DPD	Data Protection Directive
EEA	European Economic Area
EFTA	European Free Trade Association
ICO	Information Commissioner's Office
PDMA	Personal Data Management Architecture
PDSs	Personal Data Stores
PIMS	Personal Information Management Services
URL	uniform resource locator

INTRODUCTION

In May 2014, the world of privacy regulation, data handling and the World Wide Web changed dramatically as a result of judgment C-131/12 in the Court of Justice of the European Union (CJEU).[1] The so-called Google Spain decision confirmed that EU data protection legislation gives data subjects the right to request search engines to de-index webpages that appear in the search results on their names. The search engine is not obliged to agree to such requests — certain conditions have to be met and tests applied — but it is not free simply to ignore them. The decision drew on the European Union's 1995 Data Protection Directive (DPD)[2] and the Charter of Fundamental Rights of the European Union,[3] and is consistent with a general direction toward more aggressive protection of privacy rights in Europe, as evidenced by the annulment of the Data Retention Directive, also in 2014 (CJEU 2014). Nevertheless, despite these antecedents, it has been seen as a major step in establishing a right to be forgotten.

The right to be forgotten is primarily a legal concept, therefore much of the discussion in this chapter will be to do with the law. This is not a legal opinion, however, and the authors are not lawyers. The right to be forgotten covers moral and political issues, and raises technical and institutional problems. Our issue as engineers of the Web is not only how we respond to the politico-legal debate, but also how to influence it by theorizing about the art of the possible. Any "solution" to the conundrums of privacy, deletion and free expression that, for example, balkanizes the Internet, will arguably produce worse effects than the problems it attempts to solve. This chapter is set, broadly, in the current context of data protection. It will not speculate on how the proposed revisions to the EU data protection law will affect the position (Zanfir 2014), nor does it demand particular changes to or interpretations of the law. It will, however, consider the possibility of a technological contribution to what is currently being fixed by a relatively controversial process.

The chapter consists of four substantial sections between this introduction and a conclusion. The first considers the nature of the right to be forgotten, and what it could mean, closing with the debate that developed around it as the European Union began to consider revising the DPD. The next section will look at C-131/12, the decision of the CJEU about an appeal made by Google Spain against a judgment of the Spanish data protection authority, the Agencia Española de Protección de Datos (AEPD). This is the most visible assertion of data rights in the European Union in this area. The third section will consider a few of the many issues that this contentious judgment has raised. Fourthly, given this judgment and the controversy it has provoked, a discussion will be presented of the potential of one particular technology to deliver (some of) the aspirations of the right to be forgotten, and a framework of norms in which that potential would be maximized.

THE RIGHT TO BE FORGOTTEN, BEFORE GOOGLE SPAIN

Traditionally, the right to be forgotten has not been understood as a natural right; we have no offline analogue. It does not appear, for example, in the *Declaration of the Rights of Man and of the Citizen* (1789). When, in one's medieval village, one committed a faux pas, the upshot of centuries of folk wisdom was that one would have to live with the consequences. In the splendid story from *One Thousand and One Nights* called "The Historic Fart," Abu Hassan flees from his wedding in shame after emitting "a thunderous fart which echoed from wall to wall and silenced every voice in the room." He travels in the East for 10 years, homesick but too embarrassed to return. When he finally plucks up the courage to go back, hoping that everyone has forgotten, he discovers that far from having been consigned to obscurity, his solecism has become a temporal standard. A child asks his mother when he was born; she replies that he must be 10, because he was born in the year Abu Hassan farted. "And with these words, hope died in his heart forever. He fled the land and was never seen again."

He might well have wished for a mechanism to suppress memories of his embarrassment, but the humour of the

[1] See http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

[2] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX: 31995L0046.

[3] See www.europarl.europa.eu/charter/pdf/text_en.pdf.

story revolves around the ways in which collective memory sometimes seizes upon apparently inconsequential events, over whose interpretation and (accurate or inaccurate) recollection their protagonists have no control.

Psychological Forgetting

Forgetting, of course, *takes place*, and has its uses (Schacter 2001). One might put misdeeds behind one, or live them down. The passage of time helps, as does the creation of a worthier identity. One could even imagine the science fiction experiment of "editing" experience to remove unpleasant memories, as in the film *Eternal Sunshine of the Spotless Mind*. But this doesn't help us understand a right to be forgotten, for two key reasons. First, the locus of forgetting is the rememberer; the right to be forgotten, by contrast, is a right *to be* forgotten, not a right to forget. If Z commits a faux pas in front of X and Y, X may forget, but Y may not (and then may remind X); Z's forgetting the event is neither here nor there. Not only is the forgetting of Z's faux pas a random event, but it is very unlikely to happen simultaneously over all rememberers; the collective memory, taken as the union of the memories of its members, is quite robust against forgetting.

Second, forgetting in this psychological sense is morally neutral. It may be that one's good deeds help one's youthful indiscretions be forgotten by a society, and that shows a mature society. However, it is just as likely that the memory of the indiscretion will hinder the creation of a positive reputation, or that a later bad deed will eclipse the collective memory of all one's past good deeds, as Shakespeare laments in Sonnet 25: "The painful warrior famousèd for worth/ After a thousand victories once foiled/ Is from the book of honour razèd quite." So even if society has mechanisms for forgetting, they will not always serve the purposes of the individual or of society. Clearly, this fact about psychological forgetting distinguishes it from the right to be forgotten, which all agree is morally charged (whether positively or negatively).

Thus, the disanalogy between the right to be forgotten (collective forgetting) and psychological forgetting must be kept in mind. In psychology, the individual forgets; in the digital world, the individual is, or hopes to be, forgotten. In the former case, the individual's memory is wiped, while in the latter, the individual hopes to wipe the "memory" of others. Nevertheless, the mechanisms of psychological forgetting (or the failures of the mechanisms of memory) are still relevant.

From an information processing view,[4] there are three basic operations that make up memory:

- registration (the transformation of input into a form in which it can be stored);
- storage (the holding of information in memory); and
- retrieval (extracting stored information).

Forgetting could be seen as another basic operation (that of clearing up used and out-of-date material), but it is more usually conceptualized in this framework as a failure in one of the three other operations. In an Internet-based analogue, failure of registration is not the issue — the assumption of the current debate over the right to be forgotten is that the information is stored somewhere online, and the issue is access to it.

Hence, the psychology of forgetting reminds us that the two relevant concepts are failures of *availability* (i.e., the information is no longer stored) and failures of *accessibility* (i.e., it is stored but cannot be retrieved). These map onto the ideas of deleting information from the Web and removing (some) links to it, making it harder to find, and correspond to, respectively, (a right to) erasure and (a right to) de-indexing or de-linking. Removal of all links is effectively indistinguishable from erasure, while removal of some links reduces the likelihood of retrieval. Clearly, the fewer links removed, the less the likelihood of retrieval is reduced.

Justice, Forgiveness and Bureaucracy

A related concept to forgetting is forgiveness (Margalit 2002). Forgiveness goes beyond forgetting; it requires remembering, while ceasing to judge harshly. Paul Ricoeur (2006, 19) argues that forgiveness is not intended "to extinguish memory: on the contrary, the goal it has of cancelling the debt is incompatible with that of cancelling memory." Horrendous deeds should not be forgotten, but we conduct our affairs in such a way that there is a route for their perpetrators to become useful members of society. Forgiveness, whatever its moral overtones, implies a learning process such that the original crime will not be committed again.

It has traditionally been hard to institutionalize forgiveness; it often seems to rely on individual case-by-case judgment that resists translation into systems. The urge to forgive can manifest itself against the background of a rigid, impartial system; the social justice of a system that is "blind" can throw up examples of individual injustice. Bureaucracies emerge to handle complexity, records are kept and the past becomes harder to shake off. The plot of Charles Dickens's *Bleak House*, for example, revolves around the mysterious past of Lady Dedlock, the truth of which is painstakingly revealed from legal documents hitherto lost or concealed, with tragic consequences.

It may be that an individual can reinvent himself or herself — in American terms, by "going West" to new territory where the memory of the original wrongdoing is less vivid. Improved communications and transport links mean that

[4] For a review, see, for example, Gross and McIlveen (1999).

one is not confined to particular locations. In Victor Hugo's *Les Misérables*, Jean Valjean shakes off his convict past through travel to new places. It is no coincidence that the novels just cited are of the mid-nineteenth century, when urbanization, globalization and the professionalization of bureaucracy were beginning to have important effects on the lives of ordinary people. Collective memory became decoupled from particular locations and geographical communities, and its content and durability far less contingent.

Power and social status are also important in determining which features of one's past or reputation will be acted upon in the present or future. Both Valjean and Lady Dedlock are in positions of power, but are undone by impersonal and unstoppable forces of the law that are devoid of compassion. In satires such as *Moll Flanders* and *Vanity Fair*, perceptions of the flighty pasts of young ladies are subtly altered by marriages, social position and wealth.

Forgiveness suggests that the debt of the past misdeed has indeed been paid, and that the perpetrator needs to move on, "to find faith in the everyday again and mastery over their time" (Augé 2004, 88). This is part of the justification for a right to be forgotten. There are many examples of permanent records that affect the individual's social standing after taking a punishment or suffering online humiliation.[5] In the United Kingdom, for instance, a 14-year-old boy found himself on the national news because he had "sexted" a naked image of himself to a girl who had shared it with others (BBC 2015). His action was logged on a police database as an instance of the crime of making and sharing indecent images of a child (i.e., himself), with potentially disproportionate consequences for him in later life (for example, if he attempts to work with children).

The injustice to the boy was illuminated against the rule-based machinery in which he was caught, rules drafted by politicians concerned with the specific problem of online pedophilia and necessarily insensitive to the details of an everyday situation — ultimately, the same problem faced by Jean Valjean. This illustrates a paradox inherent in the right to be forgotten. If machinery for institutional forgetting is in place, it will be just as insensitive to the individual situation as the machinery for institutional remembering. In such a case, the subject acts upon their own initiative to show that the past information is outdated according to some definition, but without having to make the case to wider society that they have also moved on in the sense of being a different, better or more socially attuned person. Forgiveness morphs back into forgetting, as the focus of the system is on the information, not the person. The right to be forgotten would be a means of an individual's regaining his "faith in the everyday," but it would be his choice to pursue. Offline, forgiveness is a decision of others; a right to be forgotten — like all rights — is a matter for the individual. In a world of mass data collection, forgiveness may simply not scale. To facilitate individuals' moving on, the power to decouple information from its social effects may have to be devolved to individuals (through a right to be forgotten, or other powers of deletion), not to wider society.

Forgetting and the Law

In more recent years, targeted forms of institutional forgetting, explicitly associated with a forgiving or a debt-paying process, have been enshrined in legal practice for more or less utilitarian reasons. The rehabilitation of offenders has often been facilitated by reducing access to information about convictions once the sentence has been served. The UK Rehabilitation of Offenders Act (1974) allows offenders to withhold evidence of "spent" convictions in certain contexts, such as applying for a job or conducting civil proceedings; a conviction is considered spent after a specified period of time (which depends on the severity of the original sentence) has elapsed since the sentence was served, as long as the offender has not since reoffended. It is, however, a very weak protection. In Germany, criminals' names can be withheld from news reports once the sentence is served, which led to a high-profile case when two convicted murderers sued Wikipedia for naming them in its account of the crime. The German courts have developed a number of criteria for balancing the interests of offenders in protecting their personality rights and ability to reintegrate into society, and the interests of publishers, historians and journalists in writing publicly about such events (Siry and Schmitz 2012). In the criminal justice setting, the UK Law Commission proposed a requirement that the media take down material that might prejudice a fair trial if a juror were to find it (Law Commission 2013), but the government declined to implement the proposal in full, recognizing the "disquiet" the proposal had generated (Oswald 2014).

Such forgetting is seen as benefiting both the individual and society via the individual's rehabilitation and reintegration. Amitai Etzioni (1999) has argued against this, that disclosure of convictions —for example, of sex offences — is a justifiable invasion of offenders' privacy, given the dangers to communities from their presence within. In the UK Rehabilitation of Offenders Act, a crime that received a sentence of four years or more can never be spent, presumably on the grounds that information about a serious offence must remain in the public domain for reasons of public safety. Similarly, certain classes of responsible people, ranging from those working with children, to those involved in the humane destruction of animals, to financial managers, to (somewhat bizarrely) butlers, must disclose all convictions when applying for jobs, even if the convictions are spent.

[5] See Mayer-Schönberger (2009) for several examples.

Such laws are part of the tapestry of legislation, regulations and rights that might fall under the rubric of a right to be forgotten grounded in the general right to privacy, in the context of the public exposure of an individual's personal life (Ambrose and Ausloos 2013). However, despite the term *droit à l'oubli* that is sometimes applied to them, they cannot collectively be seen as constituting a general right to be forgotten, if only because of their narrow coverage, focusing on convictions for criminal behaviour, and limited to specific contexts such as employment issues. The impetus for the development of a right to be forgotten has come, in recent years, rather more strongly from a different route, via data protection, which is concerned with managing the effect on individuals of information about them that is or has been publicly available.

The Debate over Data Protection Reform

The adoption of the Charter of Fundamental Rights of the European Union in 2009 made clear, for the first time, the status of data protection within the European Union. The European Convention of Human Rights, ratified in 1953, has traditionally provided the European human rights framework, and contains a right to a private life, but no specific mention of data protection. The DPD of 1995 provides for data protection, of course, but in the context of ensuring the free flow of information across borders in the single European market, rather than defending or demarcating particular rights. The charter is the first document to include data protection as a human right.

The debate over the right to be forgotten was transformed in the early part of this decade by a series of muscular speeches by European Commissioner Viviane Reding (2010), in the context of moves to revise the now antiquated DPD. Her speeches, floating the right to be forgotten as a key part of Europe's data protection regime, caused an immense amount of comment. Initial debate focused on how far-reaching the proposal might be — would it mean, for example, a right to erase? Could one get unauthorized (or even authorized) photographs of oneself taken down from others' social media sites? Would it ensnare private citizens in a bureaucratic net? Or, alternatively, did it refer to better enforcement of the very much more minor rights that are enshrined already in the DPD — for example, rights to have data deleted if it is held for longer than it should be, or to object to unauthorized use? Reding (2012) claimed that a right to be forgotten would clarify and strengthen existing rights.

The distinction between memory failures of availability versus failures of accessibility is replicated on the Internet. One paper made the distinction among the following:

- a right to erasure after due process and time;
- a right to a "clean slate" (i.e., regulating the use of data so that it is not used against you after a sufficient period has elapsed); and
- a right to free expression without the danger that your utterances or behaviour will be used against you in future.

The first is a reduction of availability, while the second and third are reductions of accessibility (Koops 2011). Most commentators argued, or assumed, that a right to be forgotten, if it was to extend beyond the current data protection right to erase false content, must be tantamount to a right to erasure (Bernal 2011; Markou 2014). Meanwhile, web scientists estimated how technically feasible some of the more draconian interpretations might be, usually with negative results (O'Hara 2012).

The lack of a defined context produced something of a vacuum that was filled with commentary (some thought that the use of the term "right to be forgotten" was inflammatory and probably going to be misleading [Markou 2014]). Jeffrey Rosen (2012) called this a "proposal to create a sweeping new privacy right," which "represents the biggest threat to free speech on the Internet in the coming decade." A leading Google lawyer called the right to be forgotten "foggy thinking" (Fleischer 2011). Meanwhile, many scholars argued that some kind of right to be forgotten was already implicit in the network of data protection jurisprudence (Zanfir 2014), although there was little guidance to date about how a data controller might strike the balance between the right to be forgotten and exceptions where that right could be overridden (Ambrose and Ausloos 2013), and some in Europe argued that these rights, if they existed, were limited in scope and no big deal anyway (Ausloos 2012). Mayer-Schönberger argued that all data should have an expiration date, so that forgetting became a default — although it was hard to see how that suggestion would help with issues such as the greater powers of the search engines and social networks (not to mention governments) to set the terms of data collection, and so his idea probably serves the purpose of (first-person) forgetting, more so than the desire *to be forgotten* (Mayer-Schönberger 2009).

The root of this dispute was the philosophical divergence between the United States and the European Union on privacy. In the former, it is taken to facilitate liberty, while in the latter it supports dignity, and conceptions differ according to how privacy should interact with other norms and institutions to produce different desired effects (Post 2001; Whitman 2004). Furthermore, the US First Amendment is one of the most complete protections of free speech, and is prioritized over many other rights. For instance, the right to free speech was recently taken as the basis for calling some restrictions on political campaign finance unconstitutional, for example, in the cases of *Citizens United v Federal Election Commission* 2010 and *McCutcheon et al v Federal Election Commission* 2014 (Mutch 2014). There would seem little doubt that a right to be forgotten, however it was enacted, would fall foul of First Amendment rights — hence Rosen's response.

THE GOOGLE SPAIN DECISION

The Google Spain decision C131-12 (European Commission 2014) was based on a case brought by Google Spain against the AEPD. The AEPD had, from 2007 on, pursued a couple of hundred similar cases in which individuals protested that data about them online, although true, was excessive or outdated (Daley 2011). These are cardinal sins in the data protection world — the DPD specifically requires that data should be "adequate, relevant and not excessive in relation to the purposes for which they are processed;… such purposes must be explicit and legitimate and must be determined at the time of collection of the data; [and] the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified" (Recital 28).[6] Nevertheless, this was something of a lone crusade for the AEPD, which was not generally supported or copied by other data protection authorities (DPAs).[7]

The cases the AEPD took on often resulted from digitization, of newspaper archives or public gazettes, for example. Minor but embarrassing judgments (a conviction for urinating in a public street, for example) became prominent for certain citizens via Google searches. Sometimes the newspaper archive did not tell the full story. A charge or a conviction would be reported, but the acquittal or the successful appeal would not, so the archive, although it told the truth, could not be said to have told the whole truth, and taken *in toto* could be seriously misleading.

The problems are sometimes less with the content of the webpages, and more with the style of presentation of the search results. For example, given that result ordering is crucial, there are many cases where the charge/conviction features prominently in the first couple of pages of search results, but the acquittal/appeal appears so low down that a searcher would be unlikely to get that far. Sometimes, the problem is not that the webpage's information is misleading, but the extract from the page that accompanies the result gives a false impression.

The objection raised by the person who brought the key case against Google Spain was against information he argued to be outdated and irrelevant to his current professional life. Some time previously, after some issues with his tax authority, his home had been repossessed and auctioned off. The auction was publicized in a newspaper in order to help maximize revenue for the auction. Once the newspaper's archive was digitized, the auction notice resurfaced, and the complainant argued that his privacy was being infringed because the proceedings had been fully resolved for several years, they were irrelevant to his current life and indeed had the potential to harm his professional career. He therefore argued that the newspaper should take down the piece from its archive, and that Google Spain should cease to index it in searches on his name. Although the AEPD rejected his case against the newspaper, whose archival function it respected, it found in his favour with respect to the search engine (thereby implicitly endorsing the complainant's assessment of the information), and Google Spain took the case to a resolution in the CJEU.

It is fair to say that many observers thought that the AEPD was not going to succeed in the case, particularly when the advocate-general, the CJEU's special adviser on legal matters, upheld crucial parts of Google Spain's case (European Commission 2013; Lynskey 2013). However, the court chose to reject the advocate-general's non-binding view, and came down in favour of the AEPD's original decision.

The Substance of the Judgment

In its judgment, the CJEU rejected all four key aspects of Google Spain's defence. Its responses to the italicized defences are summarized in the next four paragraphs.

- *Search is not data processing: it involves locating, indexing and even temporarily storing data, but not processing.* The DPD is clear that processing happens when data is "collected," "organized," "stored," "retrieved," "disclosed," etc. (article 2(b)), and the court was clear that this was indeed happening.

- *The European Union has no jurisdiction over the case, as the search engine was run from the United States by Google Inc., while Google Spain, which does fall under its jurisdiction, does no processing.* The CJEU ruled that Google Spain is an EU establishment, as it is based in Spain (this was not in contention). Furthermore, Google Inc.'s processing of the data took place in the context of the activities of Google Spain (on the territory of the member state Spain) that were "intended to promote and sell… advertising space offered by the search engine which serves to make the service offered by that engine profitable." Hence the search engine's data processing, even though it happened in the United States, took place within the context of Google Spain's business (it wouldn't have happened otherwise), which, the court argued, brought the processing within the European Union's jurisdiction.

- *Neither Google Spain nor Google Inc. is a data controller; they are merely passive intermediaries that make no*

[6] In general, article 6 of the DPD provides five data quality principles. Data must be: processed fairly and lawfully; collected for specific and explicit purposes; adequate, relevant and not excessive relative to those purposes; accurate and up to date; and kept in a form where data subjects are identifiable for no longer than required for the purpose.

[7] See, for example, Information Commissioner's Office (ICO) (2011), which is somewhat lukewarm toward the evolving proposals.

distinction between personal data[8] *and other kinds of data, have no control over it, and make no decisions relating to its management.* This was the key contention, with which the advocate-general concurred, arguing that to be a controller, "the data processing must appear to him as processing of personal data, that is 'information relating to an identified or identifiable natural person' in some semantically relevant way and not a mere computer code" (European Commission 2013). However, the CJEU rejected the argument because the search engine "determined the purposes and means of processing" *within the context of the activities of Google Spain*. This processing, controlled by Google Inc., was the subject of the case, not the processing performed by third-party webmasters, and it consisted in the creation of "a structured overview of the information" relating to the individual searched for, which could not be created in the absence of the search engine. The processing of personal data by search engines is distinct from and additional to that of the third parties, and also plays a decisive role in its dissemination.

- *The information was already public, and there was no right (and Google had no power) to erase it.* The court agreed that the information did not have to be taken down, assuming it was true. However, it also concluded that Google Spain was performing an extra privacy-relevant function, by bringing links to public information together on a single webpage. In this, the CJEU followed the US Supreme Court, which had recognized the privacy interest in collecting public information, and the privacy protection of what was termed *practical obscurity*. A 1989 judgment argued that FBI rap-sheets need not be released under Freedom of Information requests because "a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that, when the request seeks no 'official information' about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is 'unwarranted'."[9] In other words, someone wanting to know about the FBI could have access to the information, but not someone wanting to know about the person. The CJEU's argument was roughly parallel (Goodman 2015). The public information upon which the search results would be based was to be unchanged, and the information could be made available through the search engine as long as the searcher's interest was not in the person involved, as evidenced by the search terms she used.

The Upshot of the Judgment

The victory of the AEPD showed that data subjects had the right to apply to Google to remove outdated, inaccurate or excessive information from Google searches within Europe, as long as they were searches for information on the data subject him- or herself. So, for example, if one had committed some youthful misdemeanour that was referred to in a webpage, then one could go to Google with a request to de-index that specific uniform resource locator (URL) from searches on one's name. The webpage would remain online, and it could be reached via a different search — for instance, if one searched for examples of the specific misdemeanour, the offending webpage might legally appear in the search results. In the judgment, "forgetting" does not involve deletion, and so a right to be forgotten is distinct from a right to erasure. In that sense, the concept is somewhat closer to the notion of forgiving and moving on discussed earlier. Erasure is already a data protection right "where personal data storage is no longer necessary or is irrelevant for the original purposes of the processing for which the data was collected" (article 32 of the DPD). Furthermore, as this is a right, it is not necessary for the data subject to show that he has been harmed or the information is prejudicial; it is sufficient that he objects. However, it is accepted that archives have special requirements to hold information and to keep full records.

The key parameter to be provided to Google would be the URL of the webpage, not the information itself. If the offending information was present on a series of webpages, Google would only be obliged to de-index the particular pages of the URLs it had notified.

Google can turn down any such request. In that event, the complainant has the right to go to their national DPA (or straight to court), which can override Google's judgment. The judgment suggested a number of grounds for refusing a data subject's request. Although the economic interest of the search company was not deemed sufficient reason to overturn a European citizen's data protection rights, those rights would have to be balanced on a case-by-case basis against rights to freedom of expression and of the media, and also against the interests of the public in having access to the information via a search on the subject's name. The status of the complainant as a public figure would therefore be a contributory factor. Google has no obligation to inform third-party webmasters of its decision to remove a webpage from searches (though it often does), and those third-party webmasters therefore might, as far as the law is concerned, remain ignorant of a decision.

The decision only counts in the jurisdiction of the European Union, and applies to any searches carried out in the context of a business or enterprise established in the European

[8] Personal data is defined in the DPD as data from which an individual is identifiable. Different data protection acts implement the DPD across the European Union, and these differ in their interpretation of "identifiable." For instance, the UK Data Protection Act specifically defines "identifiable" as "identifiable by the data controller," which weakens its privacy-protecting provisions relative to other acts.

[9] See https://supreme.justia.com/cases/federal/us/489/749/case.html.

Union, even if the actual servers carrying out the search are outside the European Union. Google Spain is certainly established in the European Union (as is Google Ireland, which sells the advertising), and so the California-based searching falls under the European Union's jurisdiction. The court said nothing about what the limits were to that judgment, but the most probable interpretation is that a search from a non-EU webpage — say, google.ca, which is based in Canada and intended for Canadian users — would be unaffected by the ruling. However, searches within the European Union — for example, on google.co.uk, google.be, google.fr and of course google.es — would be affected across all EU domains. Where Google has agreed to de-index an item in one domain in the European Union, it will follow suit across Europe.

It is finally important to point out that the key part of the CJEU's judgment was the finding that Google was a data controller. This role brings with it responsibilities under EU data protection legislation, and conversely if the court had *not* found that Google was a data controller, it would have been powerless. A data controller is defined as: "…the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data" (DPD, article 2(d)).

The advocate-general noted that Google makes no distinction between the personal data and the non-personal data that it processed, and that it does not treat personal data as personal (for example, it does not try to identify people from the data it processes). However, the CJEU ruled that those factors are not relevant to the question; Google processes personal data, whether or not it is aware that the data is personal, for purposes of its own, using means determined by itself, and for that reason it is a data controller. *But for that*, it would not fall under the jurisdiction of EU data protection law.

The Implementation of the Judgment

Following the judgment, Google attempted to drive the debate on privacy, data, free speech and a right to be forgotten by setting up a neutral advisory council of philosophers, politicians and entrepreneurs. It reported in 2015 (Advisory Council 2015), shortly after guidance was released by the Article 29 Working Party of EU DPAs (WP29 2014). The two documents set out somewhat divergent views. The WP29 document emphasized the judgment that search engines are data controllers, whose processing of personal data is in addition to the processing done by third-party websites. It played down the potential impact of the ruling, but at the same time made the strong claim that "de-listing should…be effective on all relevant domains, including .com." On the other hand, it suggested that the balance between the rights (and interests) of data subjects, and those of the data controller and the public, was perhaps finer than the CJEU had implied, and set out a series of criteria that would be relevant to making a judgment. The Google Advisory Council report also recommended criteria, but generally supported a weaker interpretation of the judgment. It recommended that publishers of information should be kept in the loop, informed of a de-listing where possible and given an opportunity to challenge a judgment. It also challenged the WP29 interpretation of the ideal geographical scope of the judgment, concluding that "removal from nationally directed versions of Google's search services within the EU is the appropriate means to implement the Ruling at this stage" (Advisory Council 2015, 20). The council wasn't shy of asking a private corporation to make judgments in this space, because "assessing legal removal requests is already the norm for, and expected behavior of, search engines and other intermediaries in contexts outside data protection" (ibid., 18). Both reports recommended transparency in principles if not in the details of actual judgments.

However, simultaneously, Google constructively worked with DPAs to develop a procedure for dealing with the issues created by the judgment. The agreed procedure with Google is outlined below. It is likely that other search engines established within the European Union will implement something similar if they haven't already, since they will fall under the scope of the ruling.

If someone objects to a webpage appearing in a name-based search for them, they first contact the search engine to ask them to de-index the page from searches based on their name. There is a fairly Byzantine process in Google to do that — Google recommends that they contact the third-party webmaster first — but ultimately they are asked to fill in a form giving the reasons to de-index. Based on the information provided, Google makes a decision. In June 2015, the statistics released by Google showed that in the year following the judgment, there were 272,940 requests to remove 991,074 pages across the European Economic Area (EEA),[10] of which 58.6 percent were rejected by Google.[11]

If the person is unsatisfied by Google's decision, they can contact their national DPA, which makes an assessment and informs the search engine of its preliminary view. Information provided by the UK DPA, the ICO, reveals that the number of complaints at this stage in the process is currently small and manageable: in the first year, there were about 250 (Bourne 2015). In the United Kingdom, Google had 34,346 requests to take down 134,931 pages, of which it rejected 62.4 percent, which equates to 1.17

[10] Actually, it is across the European Union and the European Free Trade Association (EFTA). Switzerland is a member of EFTA but not the EEA, while at the time of writing Croatia is a member of the European Union but only a provisional member of the EEA. Both are covered by Google's de-indexing regime. However, the EEA is a useful shorthand.

[11] For up-to-date figures released by Google, see www.google.com/transparencyreport/removals/europeprivacy/?hl=en.

percent of failed complaints to Google going forward to the DPA.

In the United Kingdom, the ICO bases its decisions to uphold or reject Google's judgment on at least the following criteria (ibid.).[12]

- Does the search result relate to a natural person (an individual), and does it come up against a search on that person's name? Pseudonyms and nicknames will also be considered if the complainant can show that such names are linked to their basic identity.

- Does the individual play a role in public life? The ICO makes judgments here on a case-by-case basis, while recognizing that the public interest in information about public figures is stronger. One important question it will ask is whether the information whose de-indexing is requested could help protect the public against improper professional conduct.

- Does the data relate to an individual's working life? Not all personal data is private, and the less the data reveals about someone's private life, the more likely the ICO is to accept its availability in search results. Again, this judgment will depend on whether the individual in question is a public figure, although even such people have rights to privacy.

- Was the original published in a journalistic context? The law provides protection for journalism that is not available to search engines, so in that context, the ICO will take public rights to know and media rights to freedom of expression into account.

- Does the data relate to a criminal offence? The ICO takes into account public policy with respect to rehabilitation of offenders, and the existence of mechanisms outside Web search to protect the public. It handles these on a case-by-case basis, but is likelier to favour de-indexing for cases that are more minor, and that happened longer ago. The balance between public safety in particular (as many right-to-be-forgotten cases concern previous criminal convictions) and privacy is one that exercises the ICO in its thinking.

Some media outlets deliberately provide extra links to stories that have been de-indexed, for example via a central page linking to all such stories, either as a protest against a threat to their business models, or as a principled stand for free speech. This is perfectly legal, and is far less of a threat to privacy as the searcher would need to know the substance of the story in order to find something relevant to an individual. Such pages, as a matter of fact, provide researchers with interesting material for trying to work out what kinds of requests are made. On the other hand, if the outlet republishes the content on a new page, then this will also circumvent the judgment (as it would be a different URL), and could lead to the search engine re-indexing the to-be-forgotten page. This, in contrast, is a notable threat to privacy.

ISSUES ARISING FROM THE JUDGMENT

An enumeration of several issues, positive and negative, arising from the judgment, can be found in Kieron O'Hara (2015). This section will briefly review a few of the most pressing and salient issues — in particular, the debate between privacy and free speech; the judgment's implicit view of the status of search results; the jurisdictional issues that European data protection activism has thrown up; the transparency of the de-indexing process; the potential difficulty individuals have with information that is proliferating or being spread; and the barriers to entry that may have been created.

Privacy versus Free Speech

The law is not new. The CJEU's task was to determine what was already implicit within the DPD, and it has argued that it merely interpreted DPD in the context of search. There is no extra right to erasure created, and information de-indexed remains online, findable by going direct to the site, and by following existing hyperlinks. Indeed, it can be found by standard search, as long as the search term is not the name of the data subject (it could be the name of another data subject who has not objected to the page). In this sense, the judgment has driven a wedge between rights of erasure or deletion, and rights to restrict access to information. The right to be forgotten falls under the latter, consistent with earlier critiques that erasure was not consistent with forgetting (Markou 2014), while also disappointing those who wished erasure or deletion rights to go further (Mayer-Schönberger 2014; Bernal 2011).

So, for instance, it could be argued that the financial difficulties of the original complainant should be accessible to, say, future employers or potential business partners. Employers could not be sure of getting that information by searching on his name after the Google Spain judgment (of course, they could not be sure of getting the information before Google Spain either, depending on what had been prominently linked to on the Web). But if they are entitled to that information, they can still go to official bankruptcy records to check. The difference is that in the latter case, there is a targeted search within the accepted scope of the employer's interests, while in the former there is a

[12] The following bullets are taken directly from an ICO presentation of its policy toward right-to-be-forgotten cases (Bourne 2015). An anonymous referee for this chapter pointed out that, although the ICO sets out its policies in terms of the aspects of the context that it will take into account, its resources are limited, and it may struggle to live up to these ideals if it were presented with a large number of cases.

generalized search for any information, which may turn up relevant or irrelevant material.

One of the judgment's most controversial suggestions is that rights to privacy "override, as a general rule" (paragraph 81) freedom of information and expression rights. This is debatable, but the claim does help counterbalance a major asymmetry between privacy and free speech. In making a free speech argument, no one asks Google to show that it (or anyone) has been harmed by the de-indexing of certain pages; the cry of "censorship" is enough. The CJEU, in rejecting the requirement for the data subject to show harm, levels the playing field between privacy rights and free speech rights. Granted, rights to privacy might have to be balanced against others' rights (for example, the right to free speech), in which case the level of harm might become a factor in the deliberation. But it should not be a necessary condition in a rights-based discourse.

Yet, some of the arguments that a right to be forgotten is a major blow to free speech have involved exaggerated claims that trade on the asymmetry. Speaking at an event, one prominent Internet scholar argued that a right to be forgotten was censorship. "It's like saying the book can stay in the library, we just have to set fire to the catalog" (quoted in Roberts 2015). The simile is overdrawn. It is more like saying the book can stay in the library, but we will remove the single catalogue entry that refers directly to X's name, while all the other catalogue entries remain in place (and we also, for good measure, keep the book in its right place on the shelves, so that you can also find it if you know the author's name). That is not to say that such a measure would not also be controversial, but it clearly does not support the analogy. Similarly, Jimmy Wales' argument, in his dissenting comments from the Google Advisory Council report, that publishers' works "are being suppressed" (Advisory Council 2015, 27) is an overstatement of the actual effect on the publishers, if we take "suppression" to mean the prevention of publication.

Not all commentators have gone so far. In his dissenting comments to the Google Advisory Council report, Frank LaRue argued that "we cannot make a difference between the information that exists, on files, official records or news papers, and that is obtained through a search engine" (ibid., 28). This seems like a category mistake — the information obtained through a search engine *is* the information that exists on files, etc. However, that is no reason not to distinguish between means of getting that information, given the privacy interest in dossiers of public information as recognized in the practical obscurity doctrine (Goodman 2015). There is little sign that this doctrine would constrain search engines in the United States, but it seems incorrect to suggest that there is no difference in either functional or privacy terms between 1,000 catalogues of 1,000 documents, where each catalogue contains one document that refers to Person X, and a single list of the 1,000 documents that refer to X. The judgment assumes a significant difference between these two circumstances.

The judgment should not inhibit serious journalism. A researcher in search of information about someone will have to invest more resources in finding public information, because the efficacy of "fishing expeditions" to find unspecific information is reduced. If the researcher or journalist is looking for something of any specificity at all, then they should be able to craft an effective set of search terms. The privacy threat to an individual is flagged by the use of the individual's name as a search term. Yet, as argued above, there is no pre-Internet right to be forgotten, and so erasure is not supported by the judgment. History, in the sense of what information is available on the Internet, is unchanged.

On the other hand, search engines play another important role with respect to journalism, in getting journalistic output before the public. Removal from search results could have a serious effect on the dissemination of journalism, as well as its pursuit. However, there are exemptions for journalism in the DPD, and DPAs will weigh the public interest in having access to the information. As noted above, the ICO in the United Kingdom, for example, will take that issue (and other issues, such as the public interest in knowing about perpetrators of serious crimes) into account.

And as noted, a determined searcher is unlikely to be disadvantaged for too long. There are many ways around the restriction, which means that the immediate effects of the judgment will be relatively minor. The judgment does not go as far as many privacy campaigners had originally demanded (Bernal 2011), and favours impeding the search for information over the more radical measures of policing and restricting misuse, or erasure (Oswald 2014).

Opening the Corporate Black Box

The judgment rejects the claim that search is a neutral "black box" that merely reflects the structure of the Web at a particular time. A search is a construct that mediates between the user and the Web of documents, and its ordering is a key factor in the likelihood of a link to a page being followed. Google, as a giant corporation employing many fine minds, will be able to cope with the further overhead created by a right to be forgotten. It has, after all, mapped the world, its search algorithms are already able to weed out items such as copyright material, link farms and users of the robot.txt exclusion protocol, and at the time of writing it is planning to de-index revenge porn on request (Singhal 2015). Necessarily, much about these algorithms is confidential (otherwise spammers could game them), but that very confidentiality speaks against search engines being trusted, neutral interfaces to the Web.

Google's marketing and market dominance depend on trust in the system, which in turn rest on a myth of completeness; its search is marketed as a non-selective neutral instrumentation of the conversations on the Web. Even some who want a strong right of erasure argue that Google's formal indifference to content should not be interfered with (Markou 2014). But, of course, Google doesn't index the entire Web, and eliminates and ignores many sources of information, and so this myth should be dispelled. Google is not the Web, although it is of course a marvellous tool for navigating the mass of information, possibly indispensable in the age of digital networks. Neither is the Internet or the Web a privileged version of history. Even when an aggregation of pages provides a true narrative, it is not necessarily the whole truth (as with a newspaper archive publishing a conviction for an offence but not the successful appeal).

Google is a partial view of a partial repository of information. For serious engagement with history, or attempts to hold people to account for their actions, or defence of the public against harm, Google, like Wikipedia, is an excellent starting point, but a starting point alone. It is not the whole Web, and the Web is not the whole truth.

Jurisdiction

The Internet and the Web have often been held up as exemplars of a new type of space, independent of the constraints and confines of the nation state, perhaps most famously in John Perry Barlow's *Declaration of the Independence of Cyberspace*. More prosaically, issues to do with regulation and law enforcement across different jurisdictions have often been problematic, and regulators have tended to work at a slower pace than innovators. Data protection law is a classic case where different interpretations of EU and US law, and the right to be forgotten, as well as other privacy issues, have long threatened to drive a wedge between the two jurisdictions (Whitman 2004; Bamberger and Mulligan 2011; Ambrose and Ausloos 2013; Bygrave 2014).

The CJEU's judgment has been implemented by Google only on its EU and EFTA domains, such as .es, .uk, .fr, .de and so on. The main .com site, which is US-facing, does not de-index pages on data protection/right-to-be-forgotten grounds. The rationale for this decision is that Google has a large share of the European search market, most of which goes on the national domains such as google.co.uk. Someone wishing to use google.com in Europe is diverted to the national domain, and it takes a little persistence to get to google.com (or indeed any other non-EU national domain). It is not much of a barrier to the determined (indeed, you can make google.com your home page to circumvent the defaults), but the power of default (plus linguistic preferences) means that most searchers end up using their national domain. This minor (but, in practice, significant) barrier reduces the radicalism of a right to be forgotten, and meets the *desideratum* that it protects Europeans in Europe, where data protection rights are recognized, while not protecting anyone elsewhere. For most Europeans, their reputations matter most in Europe, and so the level of protection is useful and not insignificant.

This view is not universally held. Following the Google Spain judgment, little has been heard of Google's defence that the European Union should have no jurisdiction over the actions of a US company operating equipment in California, but presumably that feeling has not gone away (a Republican Congress might one day consider the argument). On the other side, the Article 29 Working Party went beyond the CJEU's judgment to demand that it should also apply to the .com domain, as this was (easily) reachable from Europe.

> In order to give full effect to the data subject's rights as defined in the Court's ruling, de-listing decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient mean to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com. (WP29, 2014)[13]

The argument over jurisdiction continues, and will remain live for some time. At the time of writing, Google is reported (Fioretti 2016) to be about to implement a judgment from the Commission nationale de l'information et des libertés, the French DPA, to extend the right-to-be-forgotten procedure to all domains globally, having initially resisted it (Fleischer 2014). It will only apply, at present, to searches within European territory (so a European search on google.com would be de-indexed, but not one from outside Europe).[14] However, in practical terms, it is hard to see how the European Union could enforce global compliance. Furthermore, the same logic could be applied to EU-based search engines by more repressive governments.

The position of enforcing a right to be forgotten in EU territory — and not elsewhere — is enforceable, largely effective given the percentage of searches done on European domains in Europe (where most Europeans

[13] See also Sabine Leutheusser-Schnarrenberger's dissenting argument to the same effect in Advisory Council (2015, 26).

[14] See www.reuters.com/article/us-google-eu-privacy-idUSKCN0VJ29U.

have their main privacy interests), and not over-restrictive. It respects the different intuitions, rules and norms that obtain outside Europe, while simultaneously remaining consistent with the CJEU's reasoning and the imperative for data protection within the European Union. It also appropriately constrains a right to be forgotten.

Transparency

The original judgment gave little guidance as to the criteria for the decision to de-index or not, although since then the Article 29 Working Party has provided non-binding guidance (WP29 2014). Google's Advisory Council has also given its advice on the topic (Advisory Council 2015, 7–14). Google itself has made decisions on hundreds of thousands of requests, of which only a tiny percentage have been referred to DPAs. Teams of lawyers, paralegals and engineers deal with the many "easy" cases, while hard cases are referred to the executive level (Fleisher and Schechner 2015). Google, as noted, releases statistics on its decisions, which have stabilized at an acceptance rate of about 40 percent. It is certainly important that jurisprudence should emerge (Jones 2015).

There is no doubt that the decisions Google has been asked to make (and this is not a power it sought) are important ones involving censorship and information flow. It is not ideal that such decisions be privatized at all,[15] but even given that privatization was the solution, it is essential that decisions be transparent. Google's Global Privacy Counsel has argued that it is "building a rich programme of jurisprudence," but this program is, in the words of an open letter to Google by 80 scholars requesting greater transparency, "built in the dark" (Goodman, Powles et al. 2015).[16] There is, of course, tension between the needs of transparency and privacy, but aggregate statistics — for example, of categories of successful and unsuccessful claimants, or of the types of requests made and granted (crime victims? health information? false accusations? old and minor misdemeanours? political opinions no longer held?) — should be possible to generate without threatening privacy. At the time of writing, Google is considering this request (Collins 2015).

It is also possible that third-party publishers might be more readily involved in the judgment process (especially the media, given the protections for journalism in the DPD, although one would not wish accidentally to inform, say, a revenge porn site that a subject had invoked their right to be forgotten). This would allow input of more relevant information, from the publisher, into the decision-making process. It would also allow publishers to take a case to the DPA, which is important, given that most DPAs have the dual function of protecting privacy and freedom of information. The risk, however, with this option is that it would also allow publishers to identify and republish de-indexed pages with a new URL, which would take them out of the scope of the judgment, and would then require the individual to make a new approach to the search engine.

Onus on the Individual

The system as it has evolved places the onus of work on privacy-aware individuals, and in this sense is part of a general trend (Van der Sloot 2014). In particular, they have to specify particular URLs to be considered, and the statistics show that the average individual specifies about three or four. Yet, these individuals are less interested in making access to particular webpages harder than lowering the likelihood that someone specifically interested in them in particular can easily get hold of outdated or excessive information about them, or information that puts them in a false (usually bad) light. So interconnected is the Web that information is likely to be distributed across several pages, and may feature in a range of contexts. It may also be disseminated maliciously.

The key variable is not the webpage, but the information, yet the individual is not allowed to specify the association or information that is embarrassing, misleading or outdated. If information proliferates, they can only try to keep track of which URLs the information appears on, and contact search engines accordingly. It does not seem to be the case that it is *easy* to reduce access to information, particularly if it is widely distributed (*pace* Jones 2015). Indeed, despite the arguments of the judgment's opponents, there is little evidence about how much individuals have benefited from it. Maybe de-indexed pages simply get posted under alternative URLs routinely, to reappear in search results. Without extensive evaluation, it cannot be known how effective a protection the system provides.

Barriers to Entry to Search

The final point that will be emphasized in this chapter is that, although Google can cope perfectly well with the extra burden, this is because it is a well-resourced company. DPAs, in contrast, could not deal with all requests directly. At a point when the European Commission is concerned about competition issues in search (European Commission 2015), it may be a perverse effect to increase the barriers to entry to the search market by insisting on the implementation of a right to be forgotten by search engines other than Google. Having said that, it may also be the case that Google's machinery for dealing with de-indexing requests has been over-engineered and that there

[15] There is debate on this. Even on the Google Advisory Council some, such as Leutheusser-Schnarrenberger, argued that "this is a typical relationship between a private user on the one hand … and a private company on the other hand ... [whose] right to decide cannot be taken away" (Advisory Council 2015, 25), while La Rue took the opposite view (ibid., 29).

[16] Disclaimer: one of the authors of this chapter, Kieron O'Hara, was a signatory to the letter.

would be cheaper, more transparent and less burdensome ways of dealing with them (Powles and Floridi 2014). Ultimately, it will be essential to explore the means to increase transparency, and to make the interactions between search engines and complainants (and DPAs) more routine, in order that a right to be forgotten can be implemented without large-scale resources.

Data Protection in the Digital Age

This section has discussed a number of issues arising from the Google Spain judgment, but their effects can be detected beyond both the individual case, and the relatively narrow class of cases to which the judgment applies. The issues of privacy, free expression, transparency and the asymmetries of power that have been discussed here all play out in a number of ways as our digital technologies record ever more data, and increasingly many of our actions and interactions are symbolized and recorded, becoming visible and shareable in new and unfamiliar ways.[17] Our means of negotiating these difficult and uncertain waters will vary widely, and will include changes in law, social norms, business models and education. In the final section of this chapter, we will consider one possible technological approach that has been advocated in the context of these wider themes of data protection in the digital age, and sketch (lightly) a possible approach to rebalancing power.

PERSONAL DATA MANAGEMENT: EMPOWERING AND MAINTAINING TRUST

Currently, the discussion has been at the level of law. However, it is also possible that technology could play a part in the solution. There are a number of potential technological fixes for (parts of) the problem, including improving accountability for the misuse of information, enriching search with sentiment analysis, and a clearer process for reporting and dealing with disputes. This section will consider one particular technology that may be part of the solution, given the appropriate supporting background of regulation, digital literacy and social norms.

However, our aim is not primarily to argue for the introduction of this technology. This is a thought experiment — the idea is to show that a different relationship, mediated by technology, between data subjects and data consumers is possible, and that many of the issues arising from the right-to-be-forgotten judgment, and from problems with privacy in general, could be addressed in a different world. We will develop the thought experiment to highlight what is lacking in the current regime. In particular, if the world contained a vibrant market for personal data management, then more equitable relationships, with fewer information asymmetries, could be sustainable.

Personal Data Management Architectures

The Web was designed as a decentralized information and communication tool, but recently this model has been frayed by the economic forces of network effects, technological lock-in and low marginal costs of adoption, which have favoured large corporations able to amass giant user bases for their walled gardens (Zittrain 2008). Data is harvested from users and consolidated in giant databases where analytics produce monetizable insight to the benefit of data gatherers. People are decoupled from their data, unable to manage, curate or police it, and identity management and partitioning are hard, leading to a lack of trust (Coll 2015).

One class of technologies with the potential to rebalance asymmetries and restore trust are architectures that allow the data subjects some measure of control over, or input into the exploitation of, their personal data, including both data they have collected themselves and data collected or inferred about them. Let us call these Personal Data Management Architectures (PDMAs), intending the term to be agnostic over particular architectures, affordances and business models. It includes, but is not restricted to, Personal Data Stores (PDSs) and Personal Information Management Services (PIMSs) (Heath, Alexander and Booth 2013; Nguyen et al. 2013; Ctrl-Shift 2014; Van Kleek and O'Hara 2014; Abiteboul, André and Kaplan 2015). There is some skepticism about the PDS model of information management, often on the grounds of security or usability (Lemley 2000, Narayanan et al. 2012). The technology is certainly not mature, and although there are a number of products available there is still much work to do. Furthermore, regulation and business models do not work to its advantage. This chapter does not address these problems directly, but as a thought experiment let us assume that next generation data management is possible, with a mature industry in which security and interface issues have been largely resolved. To reiterate, our aim is not to provide a road map of how to get from here to a PDMA world, but rather to envisage a different relationship between data consumers and data subjects.

The services PDMAs might provide include user-centric consent management tools, preventing external access to data except under approved conditions, negotiating privacy policies, handling credentials and even allowing access to rich sources of data from personal data collection devices (for example, health-care monitors such as the FitBit) for payment, free services or other benefits. It is important to note that such services *do not* depend on the PDMA storing data, and it should not be assumed that they will necessarily provide storage services (although PDSs do, and there is no reason why a PDMA might not store

[17] Two interesting and contrasting critiques of this new tendency are Hildebrandt (2015) and Zuboff (2015).

some data). They might merely point to data, or handle our interactions around it.

The PDMA could act as a privacy and identity assistant, with an understanding of context (such as interaction history), mapping multiple identities to different activities, and establishing trust credentials from those requesting access to the data. Forced identity consolidation as favoured by the walled gardens would no longer be appropriate (or possible), and data would have portability across at least some contexts. The PDMA would manage interactions so that external parties need not be aware that, for example, the employee of a well-known bank, the player of World of Warcraft, the denizen of a fetish site and the campaigner for immigration rights are all the same person. There is also no implication in this account that anyone would be restricted to a single PDMA. One could partition identity across PDMAs, and use them for different purposes.

PDMA technology is certainly not mature, and may never make a market breakthrough, but in this speculative section let us assume that innovation capable of providing the above-mentioned services is with us. Assuming a mature market of critical mass emerges, the Web, currently centralizing around the major platforms, could be re-decentralized by socially aware PDMAs.

PDMAs and the Right to Be Forgotten

PDMAs might help with the de-indexing issues raised in this chapter by being the locus for dialogue and interaction with search engines, publishers and DPAs. This arrangement would require the development of new norms and possibly new regulation, but would not require a critical mass of PDMA users to work. All that is assumed in this section is a PDMA ecosystem that would allow privacy-aware individuals to manage their relations with search engines. Nothing precludes PDMAs being used alongside other technologies to interface with search engines.

The following functions or practices, integrated with the PDMA, would help craft a holistic approach to the issues raised by the Google Spain judgment.

Storing details of information or data to which its owner would wish to reduce public access by exercising their data protection rights. This would include URLs of webpages with excessive or outdated information, but might also include a specification of the problematic event(s) or information. Given that information, the PDMA could periodically search for pages that referred to it. Discovery of a prominently placed webpage with the offending information would prompt the PDMA to contact the relevant search engine automatically, or to send an alert to the user.

Associating with this database of URLs the metadata that search engines would require to assess whether the criteria for de-indexing were met — for instance, how old the information in question might be, whether the PDMA-owner was a public figure, and so on.

Cooperating with search engines. When a search came up on a person's name, a search engine could also look for PDMAs owned by people named by the identifying string, and proactively look for offending URLs in the search results, and even look for pages containing the offending information. Of course, the engine would not be obliged to de-index those pages, but could test them against its de-indexing criteria if it had access to the relevant metadata as well through the PDMA. Currently, there is no mechanism to allow search engines to do this.

Hosting dialogue with search engines, third-party publishers and DPAs. Whenever the PDMA's owner invoked a right to be forgotten, they must expect dialogue, explanation and discussion of the importance or otherwise of the information, its context, its prominence in the search results, the motives for publication, the age of the incident reported and the owner's status with respect to the public space. Such a dialogue would of course require careful monitoring of access and management of credentials. If the PDMA hosted this dialogue, there would be a central venue for the debate, and if another search engine found itself with the same right-to-be-forgotten case before it, it could immediately visit the discussion, to see, for example, how the DPA treated the case, and what courses of action other search engines had taken, thereby reducing the costs of enforcement of the right to be forgotten across the search industry.

Informing publishers. This is a risk, of course, but the above dialogue could also lead to a successful request to erase the webpage altogether, if it was sufficiently misleading or false to ring standard data protection alarm bells, if it wasn't covered by exemptions for journalism or archives, and if the jurisdiction of the website's owner was within Europe. The publisher may or may not be given access to the nature of the offending information, depending on how sensitive it was. Even so, at least the publisher would be able to annotate the database of URLs within the PDMA to give his side of the story. Such annotations would be available to search engines, the PDMA's owner and ultimately the DPA (if alerted by another party), to enable a balanced decision to be made about de-indexing, both now and in future cases.

The PDMA, therefore, could handle the database of problematic URLs, the nature of the information to be de-indexed, the metadata, the discussion, the interaction with the search engine and DPA, and the requests for de-indexing — all in a handy place that can be readily accessed during a search on the individual's name. And if a search engine wished to consider problematic pages proactively, then it could include relevant PDMAs in its search whenever it received a search request on a name or identifier. These functions would improve the interaction between data subjects and search engines in a number of ways.

First, it would reduce the effort for an individual to patrol the Internet (PDMAs generally have the aim of reducing data management demands while increasing an individual's power over their data). The onus of complaint would remain on the individual, but searching for content could be automated, and so the effort required would be lower. The PDMA could handle communication with the search engine itself, or it could merely warn a data subject of a problem. It could also structure the complaint, based on the metadata it held about the offending incident or information.

Second, by doing this it would help rebalance the power asymmetries between data users and data subjects, even if only to a small degree. Third, it would lower the barriers to entry to the search market, by providing a guide for new entrants to previous decisions and actions by search engines, publishers and DPAs. Fourth, it would lower the burden on DPAs to collect discussion and argument in one place. Fifth, it would provide a route to introduce third-party publishers into the debate to defend their position. If search engines played an active role in consulting PDMAs and annotating their databases — perhaps a big "if" — then the gains would be larger. The cause of transparency would be served, while much of the uncertainty that currently surrounds this issue — for data subjects, search engines, other data controllers and DPAs alike — could be dispelled. Search engines' cooperation is also the simplest means of genuinely reducing the onus on the individual (rather than merely automating their responsibilities).

Why would search engines collude in redrafting the social contract between data user/gatherers and data subjects? One reason might have to do with one of the other issues discussed above, that of opening up the corporate black box. Much of the search engine myth depends on an assumption of formal indifference. They, in theory, do not care what their users say or do, or what they search for; they are non-judgmental. They want as much data about as many actions as possible, however subjective, to get a full picture of the range of human endeavour, noble or embarrassing, idealistic or cynical, significant or trivial, selfless or prurient. All that matters is that the data is captured.

This is an important picture, but it is an ideal. As noted earlier, formal indifference is an ideal that Google tries to approach, rather than expects to achieve — it weeds out link farms, copyright material, child porn and revenge porn. There are campaigns to suppress more content, such as real-life torture videos (Overton 2015). Yet beyond these special categories of content, data protection legislation provides a series of quality principles (see footnote 8). Augmenting the semantically neutral calculations about the links to a page, a commentary based around data protection principles — is this information outdated? Is it excessive? — is also potentially helpful for searchers. It is arguable that if information has been judged (either by an internal process in the search engine, or more formally by a DPA) to commit one of the data protection sins, then its value to a searcher is correspondingly less than it otherwise would be. Thus the search engine, by taking this into account, is adding value to its searches, not diminishing them. Which searcher would prefer misleading information to relevant information? The information in the Google Spain decision, after all, had been found misleading by three courts and regulators.

Currently, search engines' business models are usually focused around data processing, surveillance and advertising, but at the heart of the business is the search function, which competes on quality. Formal indifference is not a guarantor of quality; the moment search takes account of malicious content, a distinction is made between the "useful" web of content, and the "parasitic" web of spam. The Google Spain judgment has introduced the data protection framework as a competing quality vector, which may ultimately work to search engines' advantage.

The mechanisms embedded in PDMAs described above would ease the requirements on search engines that took this line, by streamlining debate with aggrieved data subjects and DPAs, giving a voice to third-party publishers, recording the rationale for decisions and avoiding duplication of decision making.

Not all search engines would have to adopt this position; those that did, or those, such as Google, that found themselves legally obliged to, would find valuable resources for the task. It would also not be the case that each search engine would have to come to the same conclusion about whether a particular item should be de-indexed or not. Not only would different national DPAs sometimes differ, but search engines might have different policies about when the quality of search results was compromised.

CONCLUSION

The privacy/free speech issues that Google Spain has raised, together with the potential jurisdictional conflicts, are not intractable, as our speculative thought experiment about new norms for interaction between search engines and individuals, mediated by PDMAs, shows. In particular, if search engines agreed to include consideration of statements about the quality of information on websites collected in PDMAs during searches on names, many of the conflicts based around the use of law to protect privacy, and much of the unfinished business of the present situation, would be ameliorated.

Of course, there would be a question as to why search engines might adopt such a code. One answer could be based on a revision of business models — the task (and cost) of remaining DPD-compliant might be eased by interaction with PDMAs, and there may be other benefits (for example, access to greater quantities of other data) that follow. Another reason might be that search engines' own assessments of the quality of search results they put out could be augmented by the five data protection principles of data quality. Or it may be that the intangible benefits of goodwill and a proper respect for privacy and data protection would bring the tangible business benefits of corporate social responsibility.

Clearly, the use of PDMAs in the maximal sense would reduce the onus on the individual. Individuals are interested in protecting their reputation, and in informational self-determination, not in the identification of specific webpages, and are unlikely to have the resources to police the Web and detect every single threat to their privacy. An ecosystem in which search engines cooperated with individuals using PDMAs would no doubt not be perfect either, but the balance would at least be redressed and the task less Sisyphean.

It would also help open the corporate black box to sunlight and scrutiny. This would help lower the barriers to entry, as the PDMA would be an early port of call for a search engine, which would then be able to access any existing discussion relating to a particular complainant and make an earlier, speedier, more informed and less risky decision without the need to employ a complex evaluation process in all cases. Transparency may be an issue, however, as too much information revealed to the outside world about an interaction could identify someone as an objector to the dissemination of a particular piece of information, which in turn might alert third parties to what that information was, thereby counterproductively revealing what was to have been concealed (known as the Streisand effect). However, it would still be possible for search engines to flag all searches that may have been amended because of the right to be forgotten, as Google does now, and to release accurate and fine-grained statistical information.

The past is over; its interpretation is not. In our digital age, searches are not preambles to the interpretation and understanding of the past, neutral providers of raw materials. Search is itself a vital part of the interpretative process. This important truth must stay in the forefront of our minds as we work to regulate in this space.

It must also be remembered that this kind of forgetting (and certainly anything stronger) is a conscious decision to interrupt the flow of information. This is an active process, and so it is paramount to make sure that it takes place within a framework of accountability. It should also be ensured that records of the past remain accessible to challenge contemporary narratives and current tropes. Given the controversy that surrounds it, the scope and power of any implemented right to be forgotten should surely be, in the first instance at least, limited and constrained. The lack of an offline analogue, the potential clash with free expression, and the potential for the powerful to erase traces of wrongdoing all point in that direction. In this chapter, it is argued that the CJEU's judgment, as currently interpreted and implemented, meets these desiderata, and that the technological resources to cement a new and more equitable relationship between data consumers and subjects within this framework are not out of reach.

Acknowledgements

This research was carried out under the UK Engineering and Physical Sciences Research Council programme grant Social Machines (SOCIAM), grant number EP/J017728/1. The authors would like to thank Anni Rowland-Campbell of Intersticia, Iain Bourne and Julia Parr of the ICO, and two anonymous reviewers for comments on this chapter.

WORKS CITED

Abiteboul, Serge, Benjamin André and Daniel Kaplan. 2015. "Managing Your Digital Life." *Communications of the ACM* 58 (5): 32–35.

Advisory Council. 2015. *The Advisory Council to Google on the Right to be Forgotten*. www.google.com/advisorycouncil/.

Ambrose, Meg Leta and Jef Ausloos. 2013. "The Right to be Forgotten Across the Pond." *Journal of Information Policy* 3: 1–23.

Augé, Marc. 2004. *Oblivion*. Minneapolis: University of Minnesota Press.

Ausloos, Jef. 2012. "The Right to be Forgotten — Worth Remembering?" *Computer Law and Security Review* 12 (2): 143–52.

Bamberger, Kenneth A. and Deirdre K. Mulligan. 2011. "Privacy on the Books and on the Ground." *Stanford Law Review* 63 (2): 247–316.

BBC. 2015. "Sexting Boy's Naked Selfie Recorded As Crime By Police." BBC News, September 3. www.bbc.co.uk/news/uk-34136388.

Bernal, Paul Alexander. 2011. "A Right to Delete?" *European Journal of Law and Technology* 2 (2). http://ejlt.org/article/view/75.

Bourne, Iain. 2015. "Where Now for the 'Right to be Forgotten'?" Paper presented at the Second Conference on Trust, Risk, Information and the Law, Winchester, April.

Bygrave, Lee A. 2014. "Data Privacy Law and the Internet: Policy Challenges." In *Emerging Challenges in Privacy Law: Comparative Perspectives*, edited by Normann Witzleb, David Lindsay, Moira Paterson and Sharon Rodrick, 259–89. Cambridge: Cambridge University Press.

CJEU. 2014. *The Court of Justice Declares the Data Retention Directive to be Invalid*. CJEU press release, April 8. http://curia.europa.eu/jcms/jcms/P_125951/.

Coll, Liz. 2015. "Personal Data Empowerment: Time for a Fairer Data Deal?" London: Citizens' Advice Bureau. www.citizensadvice.org.uk/Global/CitizensAdvice/Corporate%20content/Publications/Personal%20data%20empowerment%20report.pdf.

Collins, Katie. 2015. "Google 'Considers' Further 'Right to be Forgotten' Transparency." *Wired*, May 14.

Ctrl-Shift. 2014. "Personal Information Management Services: An Analysis of an Emerging Market." London: Nesta. www.nesta.org.uk/sites/default/files/personal_information_management_services.pdf.

Daley, Suzanne. 2011. "On its Own, Europe Backs Web Privacy Fights." *The New York Times*, August 9.

Etzioni, Amitai. 1999. *The Limits of Privacy*. New York: Basic Books.

European Commission. 2013. *Opinion of Advocate General Jääskinen*. June 25. http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=EN.

———. 2014. *Factsheet on the "Right to be Forgotten" Ruling (C131-12)*. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

———. 2015. *Antitrust: Commission Sends Statement of Objections to Google on Comparison Shopping Service; Opens Separate Formal Investigation on Android*. European Commission press release, April 15. http://europa.eu/rapid/press-release_IP-15-4780_en.htm.

Fioretti, Julia. 2016. "Google to scrub web search results more widely to soothe EU objections." Reuters, February 10. www.reuters.com/article/us-google-eu-privacy-idUSKCN0VJ29U.

Fleischer, Peter. 2011. "Foggy Thinking About the Right to Oblivion." *Peter Fleischer: Privacy...?* (blog), March 9. http://peterfleischer.blogspot.co.uk/2011/03/foggy-thinking-about-right-to-oblivion.html.

———. 2014. "Implementing a Global, Not European, Right to be Forgotten." *Google Europe* (blog), July 30. http://googlepolicyeurope.blogspot.fr/2015/07/implementing-european-not-global-right.html.

Fleisher, Lisa and Sam Schechner. 2015. "How Google's Top Minds Decide What to Forget: as 'Right to be Forgotten' Ruling Turns One Year Old, Google Offers Glimpse Into its Decision-Making Process." *Wall Street Journal*, May 12.

Goodman, Ellen P. 2015. "Practical Obscurity and the Right to be Forgotten: 'Pretty Much' Privacy is Enough." *medium.com* (blog), February 4. https://medium.com/@ellgood/practical-obscurity-and-the-right-to-be-forgotten-pretty-much-privacy-is-enough-c321bdaffa08.

Goodman, Ellen P., Julia Powles et al. 2015. "Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data." *medium.com* (blog), May 14. https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd.

Gross, Richard and Rob McIlveen. 1999. *Memory*. London: Hodder & Stoughton.

Heath, William, David Alexander and Phil Booth. 2013. "Digital Enlightenment, Mydex, and Restoring Control Over Personal Data to the Individual." In *Digital Enlightenment Yearbook 2013: The Value of Personal Data*, edited by Mireille Hildebrandt, Kieron O'Hara and Michael Waidner, 253–69. Amsterdam: IOS Press.

Hildebrandt, Mireille. 2015. *Smart Technologies and the End(s) of Law*. Cheltenham, UK: Edward Elgar.

ICO. 2011. "The Information Commissioner's (United Kingdom) Response to 'A Comprehensive Approach on Personal Data Protection in the European Union'." European Commission. January 14. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ico_infocommoffice_en.pdf.

Jones, Meg Leta. 2015. "Forgetting Made (Too) Easy." *Communications of the ACM* 58 (6): 34-5.

Koops, Bert-Jaap. 2011. "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to be Forgotten' in Big Data Practice." Social Science Research Network, December 20. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719.

Law Commission. 2013. *Contempt of Court (1): Juror Misconduct and Internet Publications*. HC 860. London: The Stationery Office.

Lemley, Mark A. 2000. "Private Property: A Comment on Professor Samuelson's Contribution." *Stanford Law Review* 52: 1545–57.

Lynskey, Orla. 2013. "Time to forget the 'Right to be Forgotten'? Advocate General Jääskinen's opinion in C-131/12 Google Spain v AEPD." *European Law Blog*, July 3. http://europeanlawblog.eu/?p=1818.

Margalit, Avishai. 2002. *The Ethics of Memory*. Cambridge, MA: Harvard University Press.

Markou, Christiana. 2014. "The 'Right to be Forgotten': Ten Reasons Why it Should be Forgotten." In *Reforming European Data Protection Law*, edited by Serge Gutwirth, Ronald Leenes and Paul de Hert, 203–26. Dordrecht: Springer.

Mayer-Schönberger, Viktor. 2009. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

———. 2014. "Omission of Search Results is Not a 'Right to be Forgotten' or the End of Google." *The Guardian*, May 13.

Mutch, Robert E. 2014. *Buying the Vote: A History of Campaign Finance Reform*. New York: Oxford University Press.

Narayanan, Arvind, Solon Barocas, Vincent Toubiana, Helen Nissenbaum and Dan Boneh. 2012. "A Critical Look at Decentralized Personal Data Architectures." arXiv. http://arxiv.org/abs/1202.4503.

Nguyen, M.-H. Carolyn, Peter Haynes, Sean MacGuire and Jeffrey Friedberg. 2013. "A User-Centred Approach to the Data Dilemma: Context, Architecture, and Policy." In *Digital Enlightenment Yearbook 2013: The Value of Personal Data*, edited by Mireille Hildebrandt, Kieron O'Hara and Michael Waidner, 227–42. Amsterdam: IOS Press.

O'Hara, Kieron. 2012. "Can Semantic Web Technology Help Implement a Right to be Forgotten?" *Computers and Law* 22 (6).

———. 2015. "The Right to be Forgotten: The Good, the Bad and the Ugly." *IEEE Internet Computing* 19 (4): 73-79.

Oswald, Marion. 2014. "Seek and Ye Shall Not Necessarily Find: The Google Spain Decision, the Surveillant on the Street, and Privacy Vigilantism." In *Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment*, edited by Kieron O'Hara, M.-H. Carolyn Nguyen and Peter Haynes, 99–115. Amsterdam: IOS Press.

Overton, Iain. 2015. "What Will It Take to End the Pornography of Videoed Torture?" *The Guardian*, September 7.

Post, Robert C. 2001. "Three Concepts of Privacy." *Georgetown Law Journal* 89.

Powles, Julia and Luciano Floridi. 2014. "A Manifesto for the Future of the 'Right to be Forgotten' Debate." *The Guardian*, July 22.

Reding, Viviane. 2010. "Privacy Matters: Why the EU Needs New Personal Data Protection Rules." Speech presented for the European Commission, November 30. http://europa.eu/rapid/press-release_SPEECH-10-700_en.pdf.

———. 2012. "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age." Speech presented at the Digital Life Design Conference, Munich, January 24. http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm.

Ricoeur, Paul. 2006. "Memory — Forgetting — History." In *Meaning and Representation in History*, edited by Jörn Rüsen, 9–19. Oxford: Berghahn Books.

Roberts, Jeff John. 2015. "The Right to be Forgotten From Google? Forget it, Says U.S. Crowd." *Fortune*, March 12. http://fortune.com/2015/03/12/the-right-to-be-forgotten-from-google-forget-it-says-u-s-crowd/.

Rosen, Jeffrey. 2012. "The Right to be Forgotten." *Stanford Law Review* 88.

Schacter, Daniel L. 2001. *The Seven Sins of Memory: How the Mind Forgets and Remembers*. New York: Houghton Mifflin.

Singhal, Amit. 2015. "'Revenge Porn' and Search." *Google Public Policy* (blog), June 19. http://googlepublicpolicy.blogspot.co.uk/2015/06/revenge-porn-and-search.html.

Siry, Lawrence and Sandra Schmitz. 2012. "A Right to be Forgotten? How Recent Developments in Germany May Affect the Internet Publishers in the US." *European Journal of Law and Technology* 3 (1). http://ejlt.org/article/download/141/222.

Van der Sloot, Bart. 2014. "Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation." *International Data Privacy Law* 4 (4): 307–25.

Van Kleek, Max and Kieron O'Hara. 2014. "The Future of Social is Personal: the Potential of the Personal Data Store." In *Social Collective Intelligence: Combining the Powers of Humans and Machines to Build a Smarter Society*, edited by Daniele Miorandi, Vincenzo Maltese, Michael Rovatsos, Anton Nijholt and James Stewart, 125–58. Cham, Switzerland: Springer.

Whitman, James Q. 2004. "Two Western Cultures of Privacy: Dignity Versus Liberty." *Yale Law Journal* 113 (6).

WP29. 2014. *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*. Brussels: Article 29 Data Protection Working Party.

Zanfir, Gabriela. 2014. "Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right." In *Reforming European Data Protection Law*, edited by Serge Gutwirth, Ronald Leenes and Paul de Hert, 227–49. Dordrecht: Springer.

Zittrain, Jonathan. 2008. *The Future of the Internet — And How to Stop It*. New Haven, CT: Yale University Press.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30: 75–89.

ABOUT THE AUTHORS

Kieron O'Hara is a senior lecturer and principal research fellow in electronics and computer science at the University of Southampton. His interests are in the philosophy, sociology and politics of technology, particularly the World Wide Web; key themes are trust, privacy, transparency and openness. He is the author of several books on technology and politics, the latest of which, *The Devil's Long Tail* (Oxford University Press, 2015), looks at online extremism. He has also written extensively on political philosophy and British politics. He is one of the leads on the UK Anonymisation Network, which disseminates best practices in data anonymization, and writes the Digital Citizen column for *IEEE Internet Computing*.

Sir Nigel Shadbolt is professor of computer science at the University of Oxford and principal of Jesus College. He is also the chairman and co-founder of the Open Data Institute. Since 2009, Sir Nigel has acted as an information adviser to the UK government, helping transform public access to government information, including the widely acclaimed data.gov.uk site. With more than 500 publications, he researches and publishes on computer science, artificial intelligence, open data and web science. He has also worked in philosophy, psychology and linguistics. Since 2000, he has secured 17 projects as principal investigator with a value of more than £20 million. He is currently principal investigator on a £6.14-million EPSRC-funded program grant researching the theory of social machines — Web-scale problem-solving systems comprising large numbers of humans and computers. In 2013, he was awarded a knighthood for services to science and engineering.

Dame Wendy Hall, DBE, FRS, FREng, is professor of computer science at the University of Southampton. She was dean of the Faculty of Physical Science and Engineering from 2010 to 2014 and head of the School of Electronics and Computer Science from 2002 to 2007. The influence of her work has been significant in many areas, including digital libraries, the development of the Semantic Web, and the emerging research discipline of Web Science. She is now executive director of the Web Science Institute at Southampton. She was president of the Association for Computing Machinery from 2008 to 2010, a member of the Prime Minister's Council for Science and Technology from 2004 to 2010 and a founding member of the Scientific Council of the European Research Council. She is currently a member of the Global Commission on Internet Governance and the World Economic Forum's Global Agenda Council on Artificial Intelligence and Robotics.

CHAPTER FIVE: UNDERSTANDING DIGITAL INTELLIGENCE AND THE NORMS THAT MIGHT GOVERN IT

David Omand

ACRONYMS

DGSE	Direction générale de la security extérieure
DPI	deep packet inspection
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
FBI	Federal Bureau of Investigation
GCHQ	Government Communications Headquarters
IP	Internet Protocol
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
SIGINT	signals intelligence
UNSC	United Nations Security Council
WMD	weapons of mass destruction

INTRODUCTION

The Snowden material has exposed — to unprecedented and uncomfortable international gaze — the world of digital intelligence and the technical success of US agencies and those of its close intelligence allies in adapting their processes to the opportunities the Internet provides. The protection of personal information from unlawful exploitation, and the legality, proportionality and adequacy of regulation of digital intelligence access and intelligence sharing have become major international political issues. This chapter[1] looks at the dynamic interaction between demands from government and law enforcement for digital intelligence, and at the new possibilities that digital technology has opened up for meeting such demands. Inevitably, the chapter has an "Anglo-Saxon" bias, given that American influence on the Internet so far has been so great, an understandable situation given the origins of the Internet and the sources of investment and innovation that have driven it thus far. The Snowden allegations have highlighted what many nations see as this US "home field" advantage in economic terms, as well as in the scale and reach of modern digital intelligence giving the United States a "hard power" advantage. The alleged range of targets of US intelligence included the chancellor of Germany and the president of Brazil and set off firestorms of diplomatic protests led by those nations. The disclosures also put the long-standing "Five Eyes" (the United States, the United Kingdom, Canada, Australia and New Zealand) partnership in signals intelligence (SIGINT) under unparalleled scrutiny and became an issue in the New Zealand general election. The debate in the European Union over personal privacy in a data-rich world in which the private sector harvests significant amounts of personal information was already complex,[2] but the Snowden allegations have made this and other international debates intense and at times toxic.[3] That, in turn, has led to some nations exploiting the issues for protectionist purposes to benefit their domestic industry in terms of data localization and procurement restrictions from US suppliers. Overall, the adequacy of the previous regimes of legal powers and governance arrangements is seriously challenged just at a time when the objective need for intelligence on the serious threats facing civil society is apparent. This chapter suggests areas where it might be possible to derive international norms, regarded as promoting standards of accepted behaviour that might gain widespread, if not universal, international acceptance, for the safe practice of digital intelligence.

ORIGINS OF DIGITAL INTELLIGENCE

The interception of written communications — and, when necessary, their decipherment — and the monitoring of patterns of communication are practices of considerable antiquity. SIGINT derived from electromagnetic emissions developed during World War II and the Cold War into a recognized major intelligence capability. The Internet is a major source of comparable intelligence power today.

Recent years have seen the development of powerful tools of digital intelligence driven by the dynamic interaction of two coincidental developments: on the one hand, the increasing public, corporate and government use of the Internet and digital data, making possible an unprecedented supply of information about individuals and their activity, movements and location; and on the other hand, the evolution of national demands for intelligence on non-state actors, in particular for the United States and its allies on terrorists after the attacks on New York and Washington, DC on September 11. Supply and demand have interacted dynamically with technological advances and popular apps, making possible new opportunities for accessing information, helping to meet insistent demands for information about suspects that have in turn driven

[1] The contents of this chapter and opinions given in it are the sole responsibility of the author in his capacity as visiting professor at King's College London. They should not be taken as an expression of the views of the British government, which continues neither to confirm nor deny allegations made in the media about the operational activity of British intelligence in the light of the material leaked by former National Security Agency (NSA) contractor Edward Snowden. Edward Snowden.

[2] Discussion of a controversial new draft European Union Regulation on Data Protection and a specific new Data Protection Directive for law enforcement continues. See http://ec.europa.eu/justice/data-protection/.

[3] The European Parliament, for example, has called for suspension of the "safe harbour" arrangements for sharing data on European citizens with the United States and the suspension of the US/EU Terrorist Finance Tracking Programme that had generated significant intelligence, helping to detect terrorist plots and trace their authors.

the development of more ingenious uses of digital data to derive intelligence. This dynamic interaction is set to continue.

Supply-side Considerations

The digital revolution has wrought profound changes in the technological environment in which intelligence agencies operate, in particular, the growth in global communications with the network of packet-switched networks[4] that comprises the Internet and carries the World Wide Web. The adoption of open Internet and network protocols allowed rapid innovation in applications attractive to business and consumers alike and the development of public key cryptography[5] made online monetary transactions feasible. The resulting popularity of the Internet as a means of personal communication as well as business, the development of the Web (and, more recently, the so-called dark Web[6]) and the ability to cheaply transfer, store and mine digital data have all transformed the opportunities for obtaining secret intelligence. Understanding the changing nature of the potential *supply* of intelligence from the Internet thus involves recognizing the potential represented by:

- the digitization of communications and the advent of packet-switched networks to carry all forms of digital communications;

- the availability of relevant data (such as communications traffic records and Internet metadata[7]) already in digital form, which means that it is economically viable to store data in bulk and to examine it and combine it with other datasets to identify matches and patterns of interest to an intelligence analyst seeking to discover new leads on a target;

- the growth in voice and video communications carried over the Internet, with Voice over Internet Protocol applications (such as Skype and FaceTime) replacing many terrestrial telephone calls using subscriber dialling;

- the widespread use of mobile devices to access the Internet and their impact on the interception of "data in motion";[8]

- the impact of cheap data storage and processing on the digitization of back offices of both companies and government departments (such as passports, national insurance records, bank account details, airline reservations and so on), making "stored data" a valuable source of digital intelligence;

- the use by governments and armed forces of Virtual Private Networks using the Internet Protocol (IP) carried on the Internet and mixed with other packet-switched communications, rather than traditional dedicated high-frequency/very high-frequency/ultra high-frequency wireless networks;

- the commercial use of strong encryption in enabling secure financial transactions and communications and in securing mobile devices from unauthorized access;

- the use of a range of technologies that can provide locational data on mobile devices;

- the use of Cloud services both for storing consumer-related information and for enabling mobile devices to use advanced programs such as mapping, aerial photography and street views too large to be stored on the device itself; and

- the widespread use of social media, texting, tweeting and blogging, all of which may provide information on the identity and associations of suspects.

No doubt, in the near future, digital "wearables" will also be popularized as consumer goods (an example is the bracelet that takes pulse and heart rate measurements and links to the owner's mobile phone — and, in the future, possibly directly to the doctor's office to warn of impending trouble). In the future, the Internet will be connected to a wide range of other devices (the so-called "Internet of things" or, more recently, "the Internet of Everything"), again increasing the stock of information that is relatable

[4] Packet switching describes the type of digital communication network in which relatively small units of data called packets are routed by computers (servers) through a network based on the destination address contained within each packet, normally directed to take the least congested and therefore cheapest route at that instant.

[5] Public key encryption was first discovered by mathematicians at the UK signals intelligence agency, Government Communications Headquarters (GCHQ). See www.gchq.gov.uk/history/Pages/Recent-History-technology-challenges.aspx.

[6] The dark Net, or dark Web, describes networks that are only accessible by trusted peers, with measures to ensure that the addresses and identities of participants are not discoverable, for example, to allow markets for narcotics and other criminal transactions to be operated with transactions in Bitcoin.

[7] Packet-switched networks rely on "headers" being attached to data packets that identify their destination and routing and enable the entire message to be recomposed on arrival, even when individual packets have taken different routes through cyberspace. Traffic data is normally defined by an analogy with old-fashioned telephone billing that lists who called whom, when, from where and for how long. The Internet age extends the metadata to include such information as the browsing history of an individual or their digitized list of contacts.

[8] A useful, if crude, distinction can be drawn between intelligence agencies intercepting communications and information about communications — data in motion — and agencies accessing data held in digital data bases, including in the Cloud — stored data.

to an individual and from which useful intelligence might be derived.

On the other hand, the Internet and its digital applications also offer added potential for those who wish to *hide* their communications:

- The huge growth in the volume of data[9] carried by global communications networks reduces the probability of interception of any given email, text or other message[10] and packet switching means that only parts of a message may be recovered. Microsoft has over a billion users of its Cloud services with 1.3 billion email addresses sending four billion emails a day and uploading 1.5 billion photographs a month. Skype calls via the Internet are taking up two billion minutes per day.

- There is a wide choice of social media platforms, chat rooms, drop boxes and other apps, not just the most well-known ones, and many are hosted overseas, complicating the surveillance task, especially if it becomes known which are less able to be accessed by the authorities.

- The provision of communications channels in multiplayer role games enables virtual "meetings" inside games.

- The availability to the user of very strong commercial encryption such as Pretty Good Privacy that, if implemented correctly, means that for all practical purposes the content of an encrypted message does not represent a cost-effective target for the authorities.

- The development of anonymizing software, such as Tor,[11] which hides the IP address of the user's device from an intercepting agency.

- The ease with which, given digital communications, steganography[12] can be used to conceal messages or malware even when the communication is intercepted.

The public is only now beginning to recognize — stimulated by the controversy over digital privacy that the Snowden affair has generated — the business model that makes the Internet economically viable, and cheap to the user, indeed largely free at the point of use. Personal information of users can be collected and monetized, and sold for marketing and other purposes. This complex metadata ecosystem has driven the massive take-up of easily available software applications (now universally just called apps) for mobile devices and the rapid adoption of social media (of which there are thousands of different variants available worldwide). Such developments have transformed the ease and variety of ways of interacting digitally between individuals and within groups, and have made multimedia ubiquitous — video, photograph, graphic and text all combined. A further relevant development has been the provision of Cloud services, not just for easily accessible data storage, but also to enable mobile devices to access very powerful software programs too large to fit on individual devices, such as search and inference engines able to recognize context and thus be faster and more efficient, translation to and from multiple languages and voice-activated inquiries. The benefits to the consumer are faster, more appropriate responses to search engine requests, relevant "pop-up" advertisements on websites and apps and free or cheap services. The private sector is thus expert at harvesting, for its own commercial purposes, data on the Internet usage of its customers, which is of considerable interest to intelligence and law enforcement for the reasons explained in the demand-side section below.

Demand-side Considerations

The basic purpose of intelligence is to improve the quality of decision making by reducing ignorance. Secret intelligence achieves that purpose in respect of information that others are trying their best to prevent from being discovered. The traditional requirements for secret intelligence drawn up by governments for their intelligence agencies were dominated by security concerns over potentially (or actually) hostile states. The priorities were acquiring intelligence on the military capabilities (organization, order of battle, equipment and doctrine) and intentions of states and their armed forces, and providing early warning of emerging threats. National security, including counter-intelligence and counter-subversion work, has been the staple diet of intelligence and security agencies around the world. These demands for military and diplomatic

[9] According to an NSA document revealed by Snowden, the NSA touches about 1.6 percent of total Internet traffic, estimated at 1826 petabytes of information a day. However, of the 1.6 percent of the data, the document states that only 0.025 percent is actually selected for review, so the net effect is that NSA analysts look at 0.00004 percent of the world's traffic in conducting their mission (less than one part in a million) (Ball 2013).

[10] Examples include financial and commodity market trading, streaming video services (such as Netflix, as well as educational services) and massively multiplayer online role-playing games.

[11] Tor, or The Onion Router, was developed by the US Navy to make impractical the identification of the sender of communications traffic, and its use by dissidents under repressive regimes such as in Iran has been encouraged. It is now a main route to the criminal websites to be found on the dark Web.

[12] The hiding of messages from plain sight, for example, concealed at very small scale beneath digitized photographs or graphics or in the code of instructions for a program.

intelligence of course continue, in particular to support current military operations and where national enmities and rivalries persist. To a large degree, however, meeting even these traditional tasks nowadays requires, for the reasons stated earlier, access to and understanding of digital communications and Internet use.

Most intelligence services around the world have also experienced a sea change over the last decade toward helping improve decision making for the purpose of public safety and security. Agencies have increasingly been called upon to target individuals, so-called non-state actors, to help counter international and domestic terrorism, proliferation of weapons of mass destruction (WMD),[13] narcotics and people trafficking, pedophile networks and other serious international crime including, most recently, cybercrime. The emergence of al-Qaeda and violent jihadist groups as a global phenomenon has created widespread public concern in many nations and a need for governments to reassure their publics over their management of the terrorist threat. Digital intelligence has proved invaluable in providing leads, such as identifying the contacts of terrorist facilitators, part of an intelligence chain that can allow the disruption of a terrorist plot[14] and as a tool after an attack to identify others in the conspiracy.[15]

For many nations, such intelligence work is reflected in a broadening of how national security is perceived in terms of anticipating threats to everyday life in addition to the traditional preoccupation with defence from external attack.[16] This shift has been described[17] as that from "the Secret State" to "the Protecting State," where it is the direct security of the public rather than that of the institutions of the state that is the focus of national security. Some relevant implications of these changes in demand include the following:

- secret intelligence becoming (for the democracies at least) a legitimate and avowed arm of government, regulated by legislation;

- a wider "customer"[18] base for secret intelligence than in the past, including local as well as national police forces, border and immigration authorities, revenue and customs, and domestic homeland security planners;

- a much higher proportion of effort[19] than hitherto going on analysis relating to terrorists and other individuals of intelligence interest to establish their identities, associations, activities and intentions, movements, and financing;

- erosion, from the point of view of the customer, of intelligence of the traditional distinctions between domestic and overseas spheres for intelligence collection since, for example, a terrorist plot may well have both domestic and external components, leads about which need to be brought together;[20]

- in both criminal and civil cases, the prosecution's use in court of evidence derived from intelligence and consequent issues over disclosure of sensitive operational details;

- the value of mutual sharing of intelligence-derived leads and tip-offs, and threat warnings with partners overseas to a much greater extent than in the past, both through police channels such as the International Criminal Police Organization and the European Police Office and between national intelligence agencies and counterterrorism analysis centres — this sharing now also includes the development of arrangements for supporting UN requirements for intelligence for their peacekeeping and peace enforcement missions;

- greater influence for the customers over intelligence collection priorities focused on intelligence reporting that could provide opportunities to take early action to protect the public or deployed armed forces, as against more traditional strategic intelligence analysis;

[13] Although there are many instances of states being behind proliferation of WMD, individuals have also been important, such as AQ Khan and his global commercial network of technology suppliers. See Corera (2006).

[14] The director general of the British Security Service has publicly given credit to the invaluable nature of such intelligence that frustrated a number of terrorist attacks in the United Kingdom in the latter half of 2014, but has emphasized the "jigsaw" nature of the intelligence work (Parker 2015).

[15] See www.theguardian.com/world/live/2015/jan/09/charlie-hebdo-manhunt-kouachi-terrorist-links-live-updates.

[16] The United States, India, the United Kingdom, France, Switzerland, the Philippines and Singapore, to take a range of examples, have brought together at the highest levels responsibility for policy on external national security and internal domestic or "homeland" security (including the response to civil emergencies) into a National Security Council.

[17] See, for example, Omand (2010).

[18] The term customer is used in this chapter to cover the varied recipients of intelligence reporting. The term does not imply the need for any financial relationship between customer and the supplier of intelligence.

[19] For example, on September 11, 2001, only about 1,300 Federal Bureau of Investigation (FBI) agents, or six percent of the FBI's total personnel, worked on counterterrorism. By 2003, that had risen to 16 percent. By 2003, over 70 percent of British Security Service effort was devoted to countering terrorism. See National Commission on Terrorist Attacks (n.d.) and Manningham-Buller (2003).

[20] A number of nations, including the United States, the United Kingdom, France and Germany, have created counterterrorism analysis centres where police and internal security and external communications intelligence analysts can work together to uncover terrorist plots, advise on threat warnings and alert states.

- especial interest in the identification (including biometrics) of individual suspects who are using the Internet under multiple aliases, and the geo-location in near-real time of individuals of counterterrorism interest; and

- the growth of interest in intelligence to support economic well-being, including anticipating key natural resource scarcities[21] and identifying corruption, fraud and detection of market rigging including by cyber means.

The growth in cyber threats, both malicious and criminally inspired, has made nations much more aware of the value of digital intelligence techniques to:

- help detect, classify and, where possible, attribute cyber attacks, including the theft of intellectual property;

- understand the nature of advanced persistent cyber threats (advanced since they involve exploiting vulnerabilities in software that firewalls will not detect, and persistent since the attacks will continue until there is a successful penetration) — such threats include the potential for disruptive cyber attacks on the critical national infrastructure and on systems essential for the effectiveness of military operations; and

- provide the means for designing and launching offensive cyber operations[22] to support military operations and for covert actions carried out in cyberspace.

The Resulting Digital Intelligence Environment

The coincidence of the modern digital communications and storage revolution and the post-September 11 demands for intelligence on suspects and their networks will be familiar to all modern intelligence agencies. It is less a question of how many terrorist attacks, criminal plots and cyber attacks have been stopped because of specific interception of terrorist intent in their communications and much more the unique contribution digital intelligence sources make to the intelligence jigsaw and the painstaking process of "discovery" of terrorist cells and involved individuals. This dynamic interaction between supply and demand forms the background to the allegations of Edward Snowden[23] about the advanced digital intelligence capabilities of the NSA and its many overseas partners.[24]

Two issues have often been conflated in the subsequent controversies over the scale and intrusiveness of digital intelligence activity both in relation to international human rights and in intelligence activity apparently directed at friendly states.[25] The first issue concerns what legal authority there should be for the state to compel (and subsidize) an Internet company to create and retain digital records of customer activity and furnish the authorities with data about the use of the service. An example would be the issue of a subpoena or warrant to an Internet Service Provider or Internet company for access to data in the Cloud or real-time transmission. The second issue concerns the ability of intelligence agencies to collect digital data without the knowledge or cooperation of the companies, in other words, as classic secret intelligence collection activities. An example would be an intelligence survey using cyber exploitation to place secretly, without the assistance of a third party, a harvesting tool on a device or network to identify the members of a child abuse network.

After the first round of publicity over the Snowden material, US President Barack Obama was forced to order an immediate "blue ribbon" inquiry into the conduct of the NSA and, subsequently, to make a major public statement and publish for the first time his directive to the NSA[26] to govern SIGINT collection. The President's Commission and the US Privacy and Civil Liberties Oversight Board both aired arguments over the potential unconstitutionality of certain domestic collection programs. The US Congress has continued to debate reforms in the relevant intelligence legislation, but the outcome is uncertain.

[21] An example is the group of rare earth minerals essential for electronic devices used in the defence, alternative energy and communications industries, and where 97 percent of world production is in China (Chapple 2012).

[22] A number of nations, including the United States and the United Kingdom, have admitted to seeking offensive cyber capabilities; others such as Russia, China and Iran have already implicitly demonstrated capabilities, either governmental or by so-called "patriotic hackers" based in those nations.

[23] An indexed guide to the material published as a result of Edward Snowden's actions can be found at www.lawfareblog.com/catalog-of-the-snowden-stored/#.UuBEdxDTk2w, and commentary at www.schneier.com/blog/archives/2014/01/catalog_of_snow.html.

[24] The long-standing Five Eyes partner agencies of the US NSA are the UK GCHQ, Canadian Communications Security Establishment, Australian Digital Signals Directorate and New Zealand Government Communications Security Bureau. In addition, Snowden has revealed networks of bilateral and multilateral digital intelligence relationships with countries such as the "SIGINT Seniors": the Five Eyes plus France, Germany, Sweden, Italy, Spain, Belgium, the Netherlands, Norway and Denmark, and others in Africa, South America and Asia, involving shared access to global communications and exchanges of technical information and techniques.

[25] Some care is needed in interpreting published material. The interception of the mobile telephone of Chancellor Angela Merkel of Germany was not denied, but the journalistic claims concerning the interception by NSA of large numbers of European telephone calls (for example, in France, Germany, Spain, Netherlands and Norway) turned out to be interception by the agencies of those nations themselves of calls overseas and shared with the United States. See Aid (2013).

[26] See The White House (2014).

In order to examine the implications of the Snowden allegations, the European Parliament is conducting its own inquiry into the alleged electronic mass surveillance of European citizens.[27] The United Kingdom is conducting several inquiries.[28] The German Bundestag has set up a special committee for broadly the same purpose. The German government has also announced that it will transfer its government e-services from the US carrier Verizon to the domestic provider, Deutsche Telekom, ostensibly for reasons of protecting the privacy of German citizens and fears of US intelligence access via US providers (Troianovski and Yadron 2014).[29] In 2014, the French government rapidly legislated to provide statutory legal authority for its ongoing interception activity under the *Loi de programmation militaire* adopted on December 10, 2013 by the French senate. This law enables the French secret services to intercept any electronic communication, under the direct authorization of the French prime minister or president. German legislation also allows electronic interception, but is much more restrictive.[30]

Whether the result of all this controversy and debate will be consistent, coherent and effective reform, or whether it will even be in the interests of the citizens concerned, much remains to be seen. The outcome of the different strands of investigation, inquiry and political debate following the Snowden affair may well be changes to tighten up the way many democratic nations regulate intrusive intelligence activity and legislate to protect personal data.[31] For some nations, learning about these advanced digital intelligence techniques will spur an effort to try to catch up, including increased monitoring of social media use by domestic publics. And, of course, there are major nations, such as Russia and China, that remain highly secretive about their national intelligence activity, and where it must be assumed that many of the techniques of intelligence access exposed by Edward Snowden are in regular use without the independent legal and parliamentary oversight mechanisms that are becoming common across democratic nations.

The Chinese government (along with a number of other governments) is reported as reappraising its reliance on major US Internet companies, concerns no doubt fuelled by the Snowden material.[32] And Western governments are, in parallel, examining their reliance on Chinese information technology suppliers as some of the methods of digital intelligence become more generally known, including the United States and Australia excluding the Chinese company Huawei from critical national infrastructure-related bids.[33] The US Internet and technology companies themselves are busy reassuring their customers that their data will be made invulnerable to all unauthorized access — including the intelligence agencies of their own government. Behind this stance by the US companies lies the commercial reality that the Snowden disclosure of the scale of NSA access to communications carried by them risked hurting their business. Companies want to be able to say that their citizenship or the placement of their servers should not become a competitive disadvantage because of customer fears that they may be more amenable to or compliant with legal mandates to furnish information.

Although approximately 40 percent of the world population already has access to the Internet, most of this is in the developed world. The expected future growth in business upon which these US companies will depend will be in China and elsewhere in Asia and South Asia, South America and Africa. For some countries in these regions, there is a long-standing suspicion of the dominance of US technology companies able to extract wealth, coupled with a natural wish on the part of these countries to see the development of indigenous capability. US Internet companies are also now, following Snowden, regarded by such states as having facilitated US espionage, and, in effect, able to impose US interpretations of human rights on their citizens since decisions relating to their own law enforcement needs are being taken by private US-owned companies under US law. At the same time, most intelligence and security agencies around the world are no doubt trying to work out how to close an apparent capability gap with the United States. Meanwhile, Western intelligence agencies and law enforcement complain that

[27] The evidence of Edward Snowden to the European Parliamentary inquiry can be found at www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

[28] A major review into interception is under way by the think tank, the Royal United Services Institute, at the request of the UK deputy prime minister. The UK government has also set up a statutory review to look at the capabilities and powers required by law enforcement and the security intelligence agencies, and the regulatory framework within which those capabilities and powers should be exercised. In the light of the Snowden material, the Intelligence and Security Committee of the UK Parliament has reported that the current powers of digital interception are essential, that the UK agencies operate at all times within human rights and national law, including applying the principles of proportionality and necessity, but that new consolidating legislation is now needed to provide much greater transparency for the citizen on how the law operates. Their report can be found at http://isc.independent.gov.uk/.

[29] In practice, intelligence penetration has little to do with the citizenship of the network provider or the location of the data. Rather, it turns on the technical ability of the intelligence agency to penetrate the target.

[30] See www.dw.de/germans-intercept-electronic-data-too-but-not-much/a-16909606.

[31] See, for example, the 2013 draft EU directive, "Proposal for a Directive of the European Parliament of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union," the draft EU regulation on data protection, at ec.europa.eu/justice/data-protection.

[32] See, for example, http://seekingalpha.com/article/2387365-chinese-restricting-of-apple-microsoft-and-symantec-are-harbingers-of-reduced-growth and http://politics.slashdot.org/story/13/06/25/140232/chinese-media-calls-for-boycott-of-cisco2014.

[33] See Intelligence and Security Committee (2013).

the publicity given to digital intelligence means they are no longer able to gather evidence as before (Hogan-Howe quoted in Whitehead 2014) and that risks to the public are rising.[34]

For intelligence and law enforcement to be able to identify communications of interest and, where authorized, to access the content of relevant communications themselves is in fact a harder technical challenge than the many internal NSA PowerPoint presentations stolen by Snowden might suggest. Capabilities identified in the Snowden material that are said to be used by the United States (and, it must be assumed, by other leading nations) include the following:

- Access in bulk to substantial quantities of Internet traffic (although still representing a very small proportion of the total). Bulk access can be achieved by intercepting terrestrial microwave links,[35] satellite links[36] and undersea cables.[37]

- Collection and storage of intercepted metadata.[38] Saved metadata can provide information concerning when and to whom phone calls are made or emails and texts are sent. It may also reveal the location of mobile devices.

- Computerized identification of traffic[39] likely to be of potential intelligence interest (as against the bulk of Internet traffic comprising machine-to-machine trading, streaming video films, pornography and so on) using deep packet inspection (DPI)[40] techniques or equivalent.

- Advanced "front end" tools to allow analysts to efficiently access and run advanced queries on intercepted data, in particular, in order to discover new leads in their investigations.[41]

- Cooperative access with the assistance of the companies concerned to commercial digital communications networks[42] and "over-the-top" applications.

- Computer network exploitation through which the networks used by targets are infiltrated digitally to extract and gather data,[43] or users' computers are spoofed into connecting into controlled servers (or base stations in the case of mobile telephones) in so-called "man in the middle" or "man on the side" attacks.

- Close-access attacks on the devices themselves and on servers[44] that are used by the target of an investigation by providing software or hardware implants that can facilitate network access to the machine, or by otherwise introducing malware.[45] So-called "watering hole" attacks use compromised websites to introduce cookies to enable users to be tracked and identified (a technique used, for example, against both child abuse and jihadist networks).

- Monitoring of social media use (such as Twitter, Facebook, Pinterest, Tumblr, Instagram, Orkut, Bebo, Qzone, Flickr and many others) with the application of computerized analytics including sentiment analysis (Omand, Bartlett and Miller 2012).

The mix of such methods exploited by nations obviously depends on ease of availability of access: for the United States, it appears from recent disclosures that access to

[34] A UK example can be seen in the comments by the Intelligence and Security Committee (2014).

[35] Both the United States and the Soviet Union developed geostationary SIGINT satellites during the Cold War in order to intercept spillover from microwave links deep inside each other's territory.

[36] For example, the Israeli capability. See http://mondediplo.com/2010/09/04israelbase.

[37] The GCHQ program TEMPORA is said to intercept bulk traffic on undersea fibre optic cables and buffer the data to allow warranted communications to be filtered out. The French Direction générale de la security extérieure (DGSE) is said to have an equivalent capability for trans-Mediterranean cables, operated in conjunction with the NSA (Follorou 2013).

[38] *The Guardian* revealed, from Snowden material, the alleged scope of the NSA's giant database, Marina, for retaining metadata. See Ball (2013).

[39] An example is the NSA XKEYSCORE program. See https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf.

[40] DPI is a form of filtering used to inspect data packets sent from one computer to another over a network. The effective use of DPI enables its users to track down, identify, categorize, reroute or stop packets with undesirable code or data. DPI is normally more effective than typical packet filtering, which inspects only the packet headers.

[41] The NSA program ICREACH is said to be able to handle upwards of five billion records every day, store them for a year, and make the database searchable by law enforcement and other US agencies and overseas partners (Gallagher 2014).

[42] According to the 2014 Vodafone law enforcement disclosure, 29 of its operating businesses around the world were required by local law to cooperate in such access either for communications data, content or both, with, for some countries, an absence of clear legal regulation and no independent oversight (Vodafone 2014). Le Monde has alleged there is a cooperative relationship between Orange and the French external service, DGSE (Follorou 2014).

[43] Widespread use of this approach is said to be responsible for large-scale theft of intellectual property from the United States and Western nations by the Chinese People's Liberation Army (Mandiant n.d.).

[44] See, for example, the allegations against both the NSA (https://edwardsnowden.com/2014/05/14/update-software-on-all-cisco-ons-nodes) and Huawai (www.technologyreview.com/news/429542/why-the-united-states-is-so-afraid-of-huawei/).

[45] Russian government hackers are suspected of creating a highly sophisticated malware program, code-named Uroburos, designed to steal files from nation states' digital infrastructure (Brewster 2014).

digital data via the dominant US Internet companies has been especially important; for the United Kingdom and France, for historical and geographical reasons, undersea cable access has featured; for Germany, satellite access; for China and Russia, digital computer network exploitation appears from the cyber-security press to have been highly productive in recent years; and for many smaller African and South East Asian nations, cooperative access to local commercial mobile communications networks is important. The ease of access to social media also provides for any nation that feels it justified, a ready source of information on the attitudes and sentiment of local populations that would require only limited investment in interception and digital technology.

Legal and Societal Constraints

The digital intelligence tools and methods outlined above provide powerful means for a state to meet its fundamental responsibility to protect its citizens, but also, if so minded, to acquire too much information about its citizens and to interfere with their liberties. The democracies have always, to greater or lesser extent and in a variety of different ways, tried to protect respect for the rights of their own citizens. 2015 is the eight hundredth anniversary of the Magna Carta, which in turn, influenced the drafters of the US Constitution, whose Fourth Amendment (1789) prohibits for US persons unreasonable searches and seizures, and requires any warrant to be judicially sanctioned and supported by probable cause. The UN Declaration of Human Rights[46] universalized this train of thought after World War II with the prohibition that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." All the members of the UN General Assembly subscribed to that declaration.

The universality of the right to respect for privacy means that it must apply to modern digital as well as more traditional means of communication. Four issues in particular arise here that are not fully resolved in international debate.

The first issue concerns what regulation should apply to the greatly increased amount of personal information that the individual discloses in the course of everyday life using the Internet, and, to a great extent, *must* disclose if the full value of the Internet to the individual is to be realized. Some of that information, such as credit card details, clearly must be protected. But other information, such as a person's physical address, is likely only to be sensitive in some contexts and, in many jurisdictions, must be publicly available for voting purposes. Although great efforts are made to anonymize large datasets, which may produce useful medical research findings or public opinion data, for some time expert opinion has been warning that the number of digitized data points relating to an individual (including tagged images) are so great that too often it would be possible to re-identify individuals (Tene and Polonetsky 2002).

The second issue concerns how an invasion of privacy of digital communications is defined. Is it when the computer of an intercepting agency accesses the relevant packets of data along with the rest of the streams of digital information on a fibre optic cable or other bearer? Or is it when a sentient being, the intelligence analyst, can actually see the resulting information about the communication of the target? Perhaps the most damaging loss of trust from the Snowden allegations has come from the common but unwarranted assumption that access in bulk to large volumes of digital communications (the "haystack") in order to find the communications of intelligence targets (the wanted "needles") is evidence of mass surveillance of the population, which it is not.

The distinction is between authorizing a computer to search through bulk data on the basis of some discriminating algorithm to pull out sought-for communications (and discard the rest) and authorizing an analyst to examine the final product of the material thus filtered and selected. It is the latter step that governs the extent of, and justification for, the intrusion into personal privacy. The computer filtering is, with the right discriminator, capable (in theory, of course, not in actual practice) of selecting out any sought-for communication. But that does not mean the population is under mass surveillance.[47] Provided the discriminator and selection program chosen and used by the accessing computer only selects for human examination the material that a warrant has authorized, and the warrant is legally justified, then the citizens' privacy rights are respected. Of course, if the selectors were set far too broadly and trawled in too much for sentient examination, then the exercise would fail to be proportionate (and would be unlawful, therefore, in most jurisdictions).

[46] Article 12 of the UN Declaration of Human Rights is available at www.un.org/en/documents/udhr/.

[47] This issue has recently been considered in respect of the Snowden allegations against the GCHQ by the statutory UK Interception Commissioner, who is a senior retired judge. He confirms in his annual report to Parliament for 2014 (available at www.iocco-uk.info/) that the GCHQ does have bulk access by computer to the Internet, but that is for the purpose of carefully targeted, highly discriminating selection of the communications of the targets where there are warrants authorizing interception with certificates attached, authorizing the targets whose communications are being sought. He has reported in the light of the Snowden allegations that everything the GCHQ does is properly authorized and legally properly justified, including under Article 8 of the European Human Rights convention regarding personal privacy. He confirmed categorically in his report that GCHQ does not conduct mass surveillance and that, furthermore, any such activity would be comprehensively unlawful. This judgement has been upheld by the UK courts. See UKIPTrib 13_77-H of December 5, 2014.

The third issue relates to the power of digital metadata (including revealing location, browsing history of Internet searches, and digital address, contact directories and diaries, and so on) to provide information about an individual said to be comparable in its degree of intrusion to accessing the content of communications themselves.[48] Traditionally, communications data on telephone calls was accessible in most jurisdictions on the authority of a senior police officer or investigating magistrate; access to the content of a call would require a higher level of judicial or equivalent warrant. One approach (taken by the United Kingdom in its interception legislation) is to stick to the traditional definition, and logically then to regard anything further possible from digital data (such as the browsing history) as content for which a warrant is needed.

The fourth issue is the question of extraterritoriality. Germany, for example, has put forward a number of proposals at the United Nations essentially seeking an obligation on states to respect the laws of the state where the subject of potential surveillance is located. The argument is that, at present, judgements about the necessity and proportionality of digital investigations that potentially invade their citizens' privacy are being made by judges and authorities in the United States (such as the Foreign Intelligence Surveillance Court) in accordance with US laws as opposed to German laws passed through a German democratic process. Paradoxically, for some non-democratic countries, there is an opposite concern that US privacy law overprotects US citizens and means that the US Internet companies do not have to disclose information about Internet use of their citizens that those states would want to monitor. This issue is, of course, linked to continuing and much wider arguments over the potential for there to be extraterritorial application of human rights law.

There is a separate argument about whether retention of unsorted data beyond a reasonable period, including buffering time taken to run a filtering program, constitutes mass surveillance given, the ease with which an individual's data could be retrieved (an analogy civil libertarians sometimes use is the prospect of the state installing a camera in every bedroom with the promise only to look at your camera if justified with a judicial warrant); the analogy for digital intelligence is much more akin to the ability authorities have in the most serious cases of getting a judicial warrant to install a listening device in the home of a suspect — potentially, therefore, any home. That is a serious invasion of a person's privacy, but it is not keeping the population or a substantial part of it under surveillance. So, when data is retained and held that potentially can allow privacy to be invaded, then controls over its access should be managed to the same standard as for any individual decision to conduct an act of intrusive surveillance. Just because the data is held in a digital database should not make the threshold for accessing it lower.

The caveat in the UN Human Rights Declaration that interference with privacy must not be "arbitrary" recognizes the steps a state may legitimately have to take in order to protect freedom and liberty, provided always that (in the words of Article 29), "In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society." Although the formulation predates the digital age, this need for balance within the basket of human rights, for example between the individual's right to safety and security and right to privacy, remains valid today.

Only a tiny minority that holds to the original "cyber punk" view of the Internet[49] would argue for an unqualified absolute right to digital privacy. The Snowden material, which publicized the apparent scale of US counterterrorist and other intelligence activity, has nevertheless provoked a vigorous global debate over how best to ensure respect for the right to the privacy of one's digital communications (and personal information accessible from Internet use) while meeting the state's obligation to uphold the law, protect the right to life and security for the citizen — for example, against terrorist attacks — and protect the right to own and enjoy property — for example, against the depredations of serious criminals.

An analogy can be drawn with the balancing act required to justify the use of violence by the armed forces. The "just war" approach seeks to reconcile seeming opposites: states have a duty to defend their citizens and justice — protecting the innocent and defending moral values sometimes requires willingness to use force and violence, but taking human life or seriously harming individuals is wrong. From this tradition has come the *jus ad bellum* challenge of having to justify the decision to enter a conflict and the *jus in bello* criteria for right conduct once engaged, including proportionality, necessity, right authority and discrimination (between legitimate targets and civilians deserving of protection) that are to be found in the Geneva Conventions and in customary international law. The approach has also been applied to suggest specific ethical

[48] For example, the view of cryptanalyst Bruce Schneier (2013) that "Metadata equals surveillance; it's that simple."

[49] The classic statement is that of John Perry Barlow's (1996) "Declaration of the Independence of Cyberspace": "Governments of the Industrial World….You are not welcome among us. You have no sovereignty where we gather….Cyberspace does not lie within your borders….You claim that there are problems among us that you need to solve. You use this as an excuse to invade our precincts….We are forming our own Social Contract. This governance will arise according to the conditions of our world not yours. Our world is different."

principles for secret intelligence activity (discussed further later in this chapter) (Omand 2006).

The European Court of Human Rights (ECtHR) in a number of notable cases[50] in the 1980s and 1990s gave judgments on claims that state authorities had violated the privacy rights[51] of European citizens by using unlawful methods of investigation including wiretapping and bugging of premises. In a series of judgements, the ECtHR established clear guidelines for the member states of the Council of Europe. These include the need for there not to be an unfettered discretion for executive action and for controls on the arbitrariness of that action. In essence, convention jurisprudence recognizes the need for states to defend themselves and to introduce measures in support of national security including intrusive methods of surveillance,[52] but insists that the impugned measures should have a basis in domestic law, which must be accessible to the person concerned who can foresee its consequences.[53] In its case law on secret measures of surveillance,[54] the court developed minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences that may give rise to an interception order (or warrant); a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed. Such safeguards are easily adapted to the digital world. In a case[55] relating to surveillance using a covertly placed tracking device of movements in a public places, on the other hand, the EctHR established the principle that for measures that interfered less with the private life of the person concerned, the conditions could be less strict.

There is an unresolved public policy issue for nations over how best to regulate intrusive surveillance by the authorities, drawing on arguments such as those of the ECtHR, at least for most democratic states. For example, from the point of view of the privacy interests of those individuals who are subject to investigative measures, it is difficult to draw a workable hierarchy of potential invasion of privacy through interception of digital communications data and content and other forms of highly intrusive intelligence such as the use of human agents or of bugging devices.[56] For instance, if an eavesdropping device is covertly installed in a target's home, it may record conversations between family members that are more intimate and personal than those that might be recorded if the target's telephone were to be intercepted (and this example becomes even clearer if, for instance, the telephone in question is used only by the target to contact his criminal associates).

The rule of law can be applied nationally to the world of intelligence, but there is no settled corpus of international law regulating secret intelligence activity itself, nor is there likely to be one given the universality of intelligence work (to which not all nations will admit) and the difficulties of arriving at international consensus on defining the practice (Yoo and Sulmasy 2007). All nations, on the other hand, make espionage against them a criminal offence. There is no positive obligation on a state to prevent or forestall another nation from intercepting the communications of its citizens,[57] nor is receiving the product of intelligence activity acquiescence in such activity. Nations will always do what they feel is necessary for national security.[58] Nevertheless, the world of secret intelligence need not be ethics-free any more than the world of warfare and

[50] Relevant ECtHR cases include *Malone v. UK* (1984) and *Hewitt and Harman v. UK* (1989). See echr-online.com/art-8-echr/introduction.

[51] Article 8 of the European Convention on Human Rights (ECHR) provides that "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (available at www.echr.coe.int/Documents/Convention_ENG.pdf).

[52] The relevant UK Court, the Investigative Powers Tribunal, has recently rejected legal challenges to the GCHQ and the Foreign Secretary by Liberty, Privacy International, the American Civil Liberties Union, Amnesty International and other civil liberties organizations following the Snowden allegations. In an important judgment, the court found that that there is no contravention by the GCHQ of ECHR Articles 8 (Privacy) and 10 (Freedom of Expression). See UKIPTrib 13_77-H, of December 5, 2014, at paragraph 161.

[53] The ECtHR did accept, however, that the requirement of foreseeability in the special context of secret controls of staff affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard. See *Leander v. Sweden* [1987] 9 EHRR 433 at paragraph 51.

[54] For example, *Malone v. UK* [1985] 7 EHRR 14, *Uzun v. Germany* [2011] 53 EHRR 24 and *Bykov v. Russia* 437.8/02 21 January 2009.

[55] *Uzun v. Germany* [2011] 53 EHRR 24.

[56] This argument by the UK government was accepted by the court examining claims of unlawful interception. See [2014] UKIPTrib 13_77-H, para 32 et seq.

[57] At least that would be an interpretation of the long-standing principle established by the ECtHR in *Bertrand Russell Peace Foundation v. UK* (1978) 14 D&R 117. In the words of the UK Court of Appeal, the ECHR contains no requirement that a signatory state should take up the complaints of any individual within its territory touching the acts of another sovereign state. See www.bailii.org/ew/cases/EWCA/Civ/2006/1279.html.

[58] The member states of the European Union have, for example, always withheld competence on matters of national security from the European Commission, seeing these as the prerogative of the nations themselves, meeting in the European Council of Ministers.

nations can agree voluntarily to abide by standards widely accepted as representing responsible state behaviour.

A Three-layer Model of Security and Intelligence Activity on the Internet

Edward Snowden's allegations highlight a major unresolved public policy issue. Like all such wicked public policy issues, there are several dimensions or layers to the problem. There are interactions — and conflicts — between the requirements of these layers that cannot be wished away and can only be managed by a holistic approach that recognizes that each layer has to be considered alongside the others. Optimize the policy instruments in only one of the dimensions and the result will be unexpected and unwelcome consequences in the others. The problem needs to be tackled as a whole. To examine this proposition, the following sections discuss the nature of intelligence and security activity on the Internet in terms of three layers:

- the everyday level of normal Internet activity and the threats society faces in using and getting the most out of cyberspace;
- the law enforcement level, trying to police at least the worst criminal excesses on the Internet; and
- the secret intelligence level, with agencies working to fulfill their national security mission but also capable of supporting law enforcement.

The Everyday Level of Internet Use

In the top layer is everyday activity on the Internet: communicating, sharing, entertaining and trading. Retaining confidence in the Internet and its financial systems and transactions is fundamental for global economic well-being. This was recognized by the Organisation for Economic Co-operation and Development in 2011 when it published a recommended set of principles for Internet policy making, including: promoting and protecting the global free flow of information; promoting the open, distributed and interconnected nature of the Internet; promoting investment and competition in high-speed networks and services; and promoting and enabling the cross-border delivery of services.[59]

The appropriate norms to be worked up here relate to:

- recognition of the primary importance of the Internet for economic and social progress and for economic development;
- multi-stakeholder principles being applied to the governance of the different aspects of the efficient functioning of the Internet; and
- net neutrality, sensibly interpreted to allow effective management of high latency services.

The principal threat to Internet confidence comes from the rapid increase in malware on the Internet designed, for the most part, for criminal gain. Cybercrime of all types is the most rapidly growing form of crime, driven by highly professional gangs largely based outside their target nations that use malware to make large criminal gains from fraud, as well as simply using cyberspace to conduct classic criminal activity at scale: stealing money, organizing narcotics, WMD and people smuggling, blackmail and extortion rackets. Some of this crime exploits the characteristics of software directly. Some could be characterized as simply traditional forms of crime (theft, for example) that can be perpetrated digitally at a much lower risk than old-fashioned analogues such as robbing banks. Some traditional illegal trading is made possible at scale by the existence of the dark Net component of the Internet (such as Silk Road and similar illegal marketplaces selling drugs and counterfeit items). The scale of Internet criminal enterprise itself spawns criminal marketplaces for false identities, credit card details and malware exploits that can be used for criminal purposes.

On the dark Net, beyond the indexing of Google, and accessible only with Tor or other anonymization software, jihadist beheading videos are circulated. Guns and weapons of all kinds, counterfeit goods, drugs, sex and slaves are sold. And this is where the cybercriminal can acquire the latest malware for their attacks.

An increasing number of nations are realizing the importance of consumer and business confidence in the Internet and are devoting considerable resources to improving cyber security, including through better education on the risks and counter-measures to be taken. Secure encryption and sound security protocols are needed for everyday communications to protect private communications and financial transactions and defeat global cybercriminals.

Alleged exploits of the NSA to get around hard encryption in pursuit of the external national security mission have raised doubts about whether software used for the everyday purposes of commerce and socializing has been weakened.[60] When flaws are detected in software systems (as they are all the time, given the staggering complexity of modern software and the interactions of applications, operating systems and communications) there is potential tension with (as inferred from some of the Snowden

[59] See www.oecd.org/internet/ieconomy/49258588.pdf.

[60] Tim Berners-Lee has criticized the NSA in those terms and has called for an Internet Magna Carta. Berners-Lee and the World Wide Web Consortium, a global community with a mission to lead the Web to its full potential, have launched a year of action for a campaign called the Web We Want, urging people to push for an Internet "bill of rights" for every country. See www.bdimedia.com/blog/happy-birthday-internet-web-founder-berners-lee-now-calls-magna-carta-protect-internet-users/.

material) the value to intelligence agencies of exploiting such flaws and exploits. Nevertheless, sound military reasoning would argue that a defence being breached is much more serious than losing the hypothetical value of a future tool. It would seem appropriate, therefore, to consider having norms here:

- To encourage the disclosure of software vulnerabilities in the interests of getting them fixed, and when it is a choice of keeping vulnerability for future covert use or disclosing it to bolster cyber defence, and it is a close call, the defence should always win.
- A nation under cyber attack should be able to call for, and expect, international support, and there needs to be the network of CERTS (Computer Emergency Response Teams) to provide it.
- Nations should sign up to the UN Human Rights Council Resolution 20/8 that the rights that apply in the offline world apply in cyberspace, too.
- Specifically, as the North Atlantic Treaty Organization (NATO) Tallinn Manual[61] states, international humanitarian law applies in cyberspace, too. So, the constraints of humanitarian law in warfare, the principle of discrimination to protect civilians, avoid collateral damage and so on, apply to cyber attacks.
- In the long term, it might even be possible to contemplate among the permanent five members of the United Nations Security Council (UNSC) an agreement that it is in each state's interest not to invite potentially fatal crisis instability by trying to plant cyber Trojan malware in key space and nuclear command and control systems.

Everyday Internet use is also the level at which data protection legislation, both national and international (for example, the new draft European Union Data Protection Regulation and Directive), kicks in to protect citizens' personal data from unlawful use. Such data protection is based on identifying and protecting personal data by insisting on the consent of the subject. Under the latest proposals, the subject would be given the "right to be forgotten" and thus the legal power to compel the deletion of personal data. Conflicts are already arising between jurisdictions with different interpretations of safeguarding and disclosing personal data, and erasing it. More international discussion is needed in order to establish agreement that to minimize conflicting and overlapping legal jurisdictions, national data protection legislation should be based on common principles such as sanctioning negligence in the safeguarding of personal data and misusing personal data for unlawful purposes.

The increasing dependence on the Internet for the routines of everyday life — and for the critical national infrastructure, such as power, telecommunications, transport and logistics, on which the normal life of the citizen depends — introduces new vulnerabilities into society. Even where systems are air-gapped from the Internet, such as the control systems for nuclear plants, the potential exists for breaches of security through the access required for visiting contractors or the staff of the facility themselves. The threat is from malicious hackers intent on disruption in support of their own causes or simply to prove a point, from criminals seeking gain through economic blackmail and from potentially hostile states.

Law Enforcement Activity on the Internet

Supporting the everyday level, therefore, is a layer of law enforcement activity by police, customs, immigration, child protection, civil contingencies and other authorities attempting to control the worst excesses of criminality, and to uphold the law and ensure the continuity of essential services. As earlier noted, the volume and nature of Internet communications and the claim asserted by some to an individual's right to anonymity in cyberspace[62] pose issues for law enforcement. Areas for norm construction for everyday activity might therefore include the need for an international norm that accepts Internet freedom of expression and personal privacy as fundamental rights as provided for in the UN Declaration (and national constitutions such as the US Constitution), but accepts explicitly that they are not absolute rights — they have to be qualified by other rights of the citizen such as the right to live in peace and to enjoy one's property. So, there is also no *absolute* right to anonymity on the Internet, but it is a part of the right to privacy that has to be respected and interference with it justified. Specifically, agreement that the Internet cannot be allowed to be a safe space for criminal activity by allowing absolute protection for personal communications.

The current work of law enforcement in attempting to police the top level of everyday Internet use has had some successes,[63] but in most states, law enforcement is falling further and further behind. Conventional non-cyber crime is decreasing in many nations as digital crime offers higher rewards at lower risk in terms of probability of detection and length of sentence if caught. The problems this poses for law enforcement include the following:

[61] The NATO Tallinn Manual was the outcome of a detailed expert study of international law applicable to cyberspace. See https://ccdcoe.org/tallinn-manual.html.

[62] A right to anonymity was never conceded by states in the world of three dimensions to apply to those committing crimes or harming society.

[63] Examples include the international cooperation led by the FBI that resulted in the taking down of the dark Web criminal sites Silk Road 1 and Silk Road 2, and the arrest of a number of suspects.

- As noted earlier, criminals of all types, including terrorists, use the same range of mobile devices and applications as everyone else, including the ability to disguise or strongly encrypt their communications and thus to hide criminal conspiracies.

- Traditional criminal investigation tools such as those derived from telephone billing information and wiretapping are increasingly ineffective as more communications switch to the Internet.

- There are insufficient numbers of suitably qualified cyber-trained officers capable of dealing with the volume of criminal activity on the Internet, including coping with a rising volume of cyber fraud, and of specialist officers capable of pursuing the most complex of cases to successful prosecution.

- The need to follow cyber attacks in near-real time, and the difficulties of attributing attacks that are bounced off servers located in different countries severely tests mechanisms of international law enforcement cooperation based on traditional models. The process for requests under Mutual Legal Assistance Treaties may not be the most appropriate mechanism for international cooperation required in the cyber age.

- It is in the nature of the Internet that victims and offenders are mostly no longer in proximity and a single offender can use the Internet to attack multiple victims across many police areas and national jurisdictions. Some of the most persistent and capable criminal groups are based in jurisdictions that do not or cannot respond fully to requests for assistance or to extradition requests/arrest warrants.

- Cyber criminals can buy exploits in dark markets as well as access to credit card and other personal details of potential victims, and do not need advanced hacker skills themselves.[64]

For these reasons, there needs to be active domestic law enforcement activity on the Internet, supporting everyday life, and trying to police the worst abuses of cyberspace. One of the biggest challenges is the absence of global agreement on dual criminality across a wide rage of cyber-related offences (including the nature of hate speech). The nature of the Internet is that for every nation there will be communications and websites that offend against domestic law (for example, by exhibiting images of child abuse, glorifying terrorism or expressing racial or other hate crime), following a set of norms that are widely recognized internationally:

- As is the practice within the European Union, there needs to be the widest possible international mutual legal recognition of certain clear classes of criminal offence that are cyber enabled, including child abuse (the double or dual criminality test that an act is, in law, a crime in all the jurisdictions involved), and cyber dependent, such as ransom-ware.

- The basic principles of necessity and proportionality, to be found in international and national human rights law, should be applied throughout law enforcement activity.

- The Internet companies responsible for maintaining global networks cannot be expected to take on the role of policing the Internet, but they can and should take steps to enable those who do have that legal responsibility to exercise it properly, provided that such steps are legally authorized. Steps should include retention of communications metadata, under appropriate safeguards and retention periods, and, if necessary, financed by national government.

- The close cooperation of Internet companies with law enforcement is essential both in their own interests to help manage cybercriminal attacks and in supporting criminal investigations that affect their customer confidence and profitability, and in the interests of corporate social responsibility, for example by removing illegal content.

- Cooperation with law enforcement should include prompt response to proper legal warrants for requests for information about subscribers and their use of the Internet and about threats to public safety and security.

Intelligence Activity in Cyberspace

To help overcome the problems of policing cyberspace, law enforcement in many nations is increasingly looking to national intelligence agencies for support. Some nations have specifically legislated to allow their national intelligence community to provide support for law enforcement[65] and the priority given to domestic counterterrorism has accentuated this trend. There are of course differences. Modern law enforcement has an intelligence function (for example, mapping crime hot spots to allow targeted policing). But most of the time, law enforcement is seeking evidence after the crime has been

[64] In September 2014, a report from Europol's European Cybercrime Centre, *Internet Organised Crime Threat Assessment*, revealed the diffusion of the business model in underground communities and highlighted that barriers to entry in cybercrime rings are being lowered even if criminal gangs have no specific technical skills. Criminals can rent a botnet of machines for their illegal activities, to infect thousands of machines worldwide. These malicious infrastructures are built with a few requirements that make them suitable for the criminals, including user-friendly command-and-control infrastructure and sophisticated evasion techniques.

[65] The EctHR has recognized the prevention and detection of serious crime as a legitimate purpose for intrusive intelligence activity along with national security and economic well-being.

committed that can be deployed as part of an open judicial process and whose legitimate derivation and meaning can be proved beyond reasonable doubt. Intelligence work is often described as probabilistic, as a jigsaw puzzle and as incomplete, fragmentary and sometimes wrong.[66] Digital intelligence can often generate leads for follow-up by conventional law enforcement methods designed to gather specific evidence, such as visual surveillance or the search of a premises.

The opportunity offered by mobile phone geo-location is an example of a digital technique that has been quickly taken up by police services, for example, to test alibis, eliminate suspects from an inquiry and help track down the perpetrators of multiple serious crimes. The power of keeping track, over a period of time, of the location of a mobile device (and what other mobile phones or devices might have been in the close vicinity of that device) is clearly of interest to the police, but is potentially very intrusive, as has been recognized by parliamentarians and civil liberties organizations. Nevertheless, for some jurisdictions, there are still constitutional concerns over the sharing of intelligence with conventional domestic police services and, in some cases, historical tensions due to past disputes over competence and territory. There is also a tension between the inevitably top-down federal nature of state intelligence activity and the local nature of policing in which "the police are the public and the public are the police," where the ability of the police to perform their duties is dependent upon public approval of police existence, actions, behaviour and the ability of the police to secure and maintain public respect.[67] One of the consequences of the Snowden affair is such questions are being increasingly posed in relation to national digital intelligence activity.

In general, national intelligence agencies have been ahead of police services in exploiting the more advanced digital information sources. For many, including the United States, the United Kingdom, Canada, Australia and New Zealand (the Five Eyes partnership that emerged from World War II) and the NATO nations, their SIGINT capabilities naturally developed into capability and cooperation in digital realms, and the same has been true for many other nations, including China, Russia, India, Japan, South Korea, Taiwan, Israel, Sweden and Finland. The Snowden material provides glimpses not only into US, Five Eyes and NATO digital intelligence but also into the capabilities that can be assumed of other nations.[68] In some cases, the claims of advanced techniques can be assumed to be spurring on others to follow suit.

An inevitable consequence of the purpose of secret intelligence being to obtain information that others are trying to hide is the essential part played by secrecy. The effectiveness of secret intelligence rests on sources and methods that must remain hidden, otherwise the targets know how to avoid detection. Oversight of intelligence activity cannot, therefore, be fully transparent and has to be by proxy: by senior judges and a limited number of parliamentarians who can, on society's behalf, be trusted to enter the "ring of secrecy" and give confidence that legal and ethical standards are being maintained.

Whatever view is taken of the legitimacy of Edward Snowden as a genuine whistleblower and of the proportionality of his actions,[69] his allegations have, in many respects, breached the necessary minimum secrecy that should surround details of intelligence sources and methods. It is important to recognize that the resulting damage to intelligence collection applies globally, not just to the agencies exposed by Snowden, from:[70]

- the scale of publicity sensitizing terrorists and criminal groups to the whole issue of digital intelligence, warning suspects of the need to be more secure and, for example, criminal networks to change their operating methods and equipment;

- highlighting/compromising specific types and methods of intelligence collection, and exposing gaps in coverage that provide signposts for criminal and hostile actors on how to reduce the probability of detection;

[66] "To supplement their knowledge in areas of concern where information is, for one reason or another, inadequate, governments turn to secret sources. Information acquired against the wishes and (generally) without the knowledge of its originators or possessors is processed by collation with other material, validation, analysis and assessment and finally disseminated as 'intelligence'" (Butler 2004).

[67] The second of the 1829 principles of law enforcement (upon the founding of Scotland Yard). See www.durham.police.uk/About-Us/Documents/Peels_Principles_Of_Law_Enforcement.pdf.

[68] In his speech at the Department of Justice on January 17, 2014, President Obama said, "We know that the intelligence services of other countries — including some who feign surprise over the Snowden disclosures — are constantly probing our government and private sector networks, and accelerating programs to listen to our conversations, and intercept our emails, and compromise our systems. We know that" (Obama 2014).

[69] Snowden has said his greatest concern was with what he saw as the unconstitutional nature of the NSA's bulk collection and storage program of the metadata of communications of US citizens, authorized under s.215 of the USA PATRIOT Act 2001. President Obama acknowledged the sensitivity of this program in his speech. The large volume of classified material (circa 170,000 documents) Snowden stole and passed to investigative journalists to expose went much wider than domestic surveillance, including US and NATO support to military operations. In addition, he passed on 58,000 top-secret documents taken from the British partner agency GCHQ. See www.headoflegal.com/2013/08/30/r-miranda-v-home-secretary-witness-statement-of-oliver-robbins/.

[70] See www.telegraph.co.uk/news/uknews/law-and-order/11300936/GCHQ-warns-serious-criminals-have-been-lost-in-wake-of-Edward-Snowden-leaks.html.

- accelerating the commercial information and communication technology sector's move to hard encryption on devices and software that cannot be overcome even with legal warrants (the response of the intelligence agencies is likely to be to try to get much closer to their targets, with consequential greater moral hazard of collateral intrusion);
- reduction in Internet company cooperation with law enforcement and government agencies as they seek to protect their commercial reputations for being able to secure their customers' data (and thus also prevent competitors deriving value from the content they are carrying); and
- the risk of overregulation due to fears of mass surveillance.

The main justification for all intelligence activity, including digital, remains national security, including support for the armed forces and for defensive alliances such as NATO and cooperative organizations such as the African Union. Where powerful digital intelligence tools exist, it is natural for law enforcement to seek support (or in some cases, such as social media, monitoring to acquire their own capability).

It is a proper use of national intelligence resources to support law enforcement, provided that the use of intrusive methods is legally regulated, as they would be if used by law enforcement itself.

As earlier noted, more often than not today a common feature of the demands placed on an intelligence community by the armed forces and law enforcement alike are for actionable intelligence about people — the terrorists, insurgents, cyber- and narco-criminal gangs, people traffickers and pedophile networks, cyber-vandals and hackers. For such targets, what is likely to be sought as of most value are their identities (a non-trivial issue given digital anonymity), associations, location, movements, financing and intentions. Often, large issues of public policy rest on the outcome of intelligence on dictators committing or threatening to carry out war crimes. For example, trying to establish whether there are Russian paramilitaries in Eastern Ukraine, on which UNSC and European Council sanctions decisions may rest. Or whether Islamic State of Iraq and the Levant jihadists in Iraq and Syria, responsible for the appalling executions of hostages, will bring their campaign to domestic streets in Europe, America and the Middle East. Of course, there are still demands from governments for intelligence on the activities of some traditional states, including friendly states where their intentions in specific areas engage vital national security interests[71] — but even in such cases the communications of interest are likely to be carried on virtual private networks on the Internet.

Not all intelligence requirements are, however, of equal importance or urgency. The limited budgets for intelligence activity at a time of general austerity in public expenditure (at least in most democratic nations) should force prioritization. Most of the top priorities will be obvious — in supporting the armed forces on operations and in providing leads for counterterrorist operations to protect the public, or where there are important diplomatic decisions to be taken, as with the negotiations with Iran over its nuclear enrichment program and over sanctions on Russia in relation to its actions in Ukraine. Intelligence agencies also have the task of providing strategic warning of new threats not yet on policy makers' radar, and leeway has to be allowed in authorizing intelligence collection operations accordingly, and in allowing intelligence relationships to be developed with other states.

Nations should make timely arrangements for sharing securely intelligence warnings on threats to the public, and, in relation to terrorism, should establish appropriate points of contact between national counterterrorism analysis centres or authorities.[72]

Most security and intelligence authorities see themselves as having a duty to seek and use information, including digital intelligence, to help manage threats to public and national security. Secret intelligence, because it involves overcoming the determined efforts of others, such as terrorists, to prevent it being acquired, inevitably involves running moral hazard such as collateral intrusion upon privacy of those such as family members who may be entirely innocent. Like law enforcement at the start of an investigation, it is also often necessary to examine a number of witnesses to a crime or associates of suspects in order to eliminate them from enquiries. The examination of those later shown to be innocent of wrongdoing is an inevitable consequence of investigative law enforcement. It should also be recognized that the powerful tools of digital intelligence are already being used in some repressive non-democratic countries for censorship and control of dissidents.

There are already, from the work of the EctHR and from academic legal scholarship, suggestions for internationally acceptable norms on how such activity is organized in order to reduce the risk of intelligence activity being

[71] Relevant here is President Obama's 2014 statement directing the US intelligence community not to monitor the communications of heads of state and government of close friends and allies, unless there is a compelling national security purpose. See The White House (2014).

[72] This suggested area for norm development follows the thrust of the UNSC Resolution 1373 adopted unanimously after the attacks of September 11, 2001.

abused. Taken together, and underpinned by domestic law, these form a new social contract in which, through democratic process, the public accepts the need for some infringement of privacy (within limits) in return for the government's commitment to keep the public secure:

- Intelligence agencies should be placed on a national legal footing with the organizations concerned having legal personalities.

- The purposes of secret intelligence should be restricted by law — for example, excluding its use for domestic political purposes and for commercial advantage.

- Investigative activity should be regulated by black letter law — there should not be secret law unavailable to the citizen.

- Highly intrusive methods should be authorized under a warranting system laid down by law.

- There should be independent oversight of intelligence activity, with sufficient access through some combination of judicial and parliamentary means, to ensure that the law is being applied and that the policies being followed are in accordance with democratic wishes. It would be best practice for governments to publish statistics on the scale of use of warranted digital intrusive methods.

- There should be the means for an independent court to assess claims of abuse of these powers, able to provide redress if proven, together with the authority to set matters right after mistakes have been made, for example, by having an individual removed from a watch-list or no-fly list.

There are also important principles of proportionality and necessity that should apply to legislation governing the intelligence agencies, so those authorizing intelligence activity, the regulators and overseers, and those inside the agencies all recognize the legal duty they have to satisfy themselves that the degree of intrusion or moral hazard likely to be occurred is in proportion to the harm to national security or public safety that is to be prevented or the benefit to be gained. Additionally, the operation must be necessary to help achieve the approved purpose, and must be one whose purpose could not reasonably be achieved in another way that did not have to involve secret intelligence. Not everything that technically can be done, should be done. Edward Snowden's allegations about the interception of the mobile telephone of Angela Merkel, the German chancellor, prompted President Obama to issue his own norm[73] on the interception of the communications of the leaders of friendly states: intelligence agencies should not, unless there is a compelling national security purpose, monitor the communications of heads of state and government of close friends and allies.

The analogy between the ethics that might responsibly apply to the activities of secret intelligence and those of the "just war" tradition underlying humanitarian law was referred to earlier. In brief, as applied to digital intelligence, appropriate norms might cover the following ground:

- **There must be sufficient sustainable cause.** There needs to be a check on any tendency for the secret world to expand into areas unjustified by the scale of potential harm to national interests, including public safety, so the purposes of intelligence should be limited by statute.[74]

- **All concerned must behave with integrity.** Integrity is needed throughout the whole system, from the reasons behind requirements, and the actions taken in the collection, through to the analysis, assessment and use of the resulting intelligence.

- **The methods to be used must be proportionate.** The likely impact and intrusion into privacy of the proposed intelligence collection operation, taking account of the methods to be used, must be in proportion to the harm that it is sought to prevent and the mechanisms for determining proportionality need to be tested through independent oversight.

- **There must be right authority.** There must be a sufficiently senior authorization of intrusive operations and accountability up a recognized chain of command to permit effective oversight. Right authority too has to be lawful and respectful of internationally accepted human rights.

- **There must be reasonable prospect of success.** Even if the purpose is valid and the methods to be used are proportionate to the issue, there needs to be discrimination and selectivity (no large-scale "fishing expeditions"[75]) with a hard-headed assessment of how to manage the risk of collateral intrusion on others.

[73] See Obama (2014).

[74] An example is the UK's Intelligence Services Act, which only permits the national intelligence agencies to act "(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or (c) in support of the prevention or detection of serious crime" (Government of the United Kingdom 1994).

[75] Law enforcement is used to having to show "probable cause" in relation to intrusive investigation of suspects. Such a criterion cannot simply be transferred over to secret intelligence, which is often seeking discovery of threats yet to crystalize and new threat actors yet to be identified. Nevertheless, "general warrants" remain unlawful both in the United States and the United Kingdom.

- **Necessity.** Recourse to the specific method of secret intelligence collection should be necessary for achieving the authorized mission and should certainly not be used if there are open sources that can provide the information being sought.

CONCLUSION

As a result of pressure from civil rights organizations following Snowden, governments are rightly re-examining processes and legal frameworks for intelligence activity and seeking to improve oversight mechanisms. No doubt the outcome of such inquiries will help the development of norms based on well-understood and tested principles that can help democratic societies regulate necessary digital intelligence activity in ways that respect the right to privacy and that help ensure that confidence is retained in the Internet.

The domestic legal framework of regulation and oversight within which intelligence activity has to be conducted will — and should — inevitably constrain the free interplay of demand for and potential supply of intelligence, not least derived from digital sources. That constraint also inevitably involves the public avowal of intelligence activity, and the according of legal status to the agencies that collect and analyze secret intelligence, as well as the provision of at least enough information outside the secret circles of agency activity to enable confidence in their activity to be justified publicly. It is not enough for the insiders to be confident that there are very effective safeguards. It is also essential for the democracies that digital intelligence is seen to be regulated effectively by applying safeguards that are recognized to give assurance of ethical behaviour, in accordance with modern views of human rights, including respect for personal privacy.

If — and it is a risk — nations are overzealous in response to Edward Snowden in constraining digital intelligence-gathering capability and data sharing, then the interests of national publics will be failed, since governments will not be able to manage the risks from terrorism, cybercrime and other criminality, nor will they have the intelligence on which sound policy decisions can be made. If, on the other hand, nations fail to exercise sufficient restraint on the use of the powerful digital tools in the hands of their intelligence agencies, and fail to be believed in doing so, then the resulting unease on the part of a vocal section of national publics and in such bodies as the European Parliament will destabilize the very intelligence communities whose work is essential in the collective interest to manage twenty-first-century risks.

Manifesting norms that law enforcement and security and intelligence agencies clearly abide by will go a long way to meet the challenge that intelligence agencies in the democracies must also be seen to behave consistently in ways that the public considers ethically sound.

WORKS CITED

Aid, Matthew M. 2013. "Greenwald's Interpretation of BOUNDLESSINFORMANT NSA Documents Is Oftentimes Wrong." November 24.

Ball, James. 2013. "NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show." *The Guardian*, September 30. www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

Brewster, Thomas. 2014. "Russians Suspected in 'Uroburos' Digital Espionage Attacks." TechWeek Europe, March 3. www.techweekeurope.co.uk/workspace/russian-intelligence-uroburos-malware-140494.

Butler, R. 2004. *Review of Intelligence on Weapons of Mass Destruction*. UK House of Commons, HC 898, July 14.

Chapple, Irene. 2013. "Why Minerals Dispute Threatens Electronics Industry." CNN, March 14.

Corera, G. 2006. *Shopping for Bombs*. New York: Oxford University Press.

Europol. 2014. *The Internet Organised Crime Threat Assessment*. Europol. September. www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta.

Follorou, Jacques. 2013. "Surveillance : la DGSE a transmis des données à la NSA américaine." *Le Monde*, October 30. www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html.

———. 2014. "Espionnage : comment Orange et les services secrets coopèrent." *Le Monde*, March 20. www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html.

Gallagher, Ryan. 2014. "The Surveillance Engine: How the NSA Built Its Own Secret Google." *The Intercept*, August 25. https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/.

Government of the United Kingdom. 1994. Intelligence Services Act. www.legislation.gov.uk/ukpga/1994/13/pdfs/ukpga_19940013_en.pdf.

Intelligence and Security Committee. 2013. *Foreign Involvement in the Critical National Infrastructure: The Implications for National Security*. June. www.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC-Report-Foreign-Investment-in-the-Critical-National-Infrastructure.pdf.

———. 2014. *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby*. HC 795, November 25.

Mandiant. n.d. "APT1: Exposing One of China's Cyber Espionage Units." http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Manningham-Buller, Eliza. 2003. "Transcript of the James Smart Lecture by the Director General of the Security Service, Eliza Manningham-Buller, City of London Policy Headquarters, 16 October 2003."

National Commission on Terrorist Attacks. n.d. *Law Enforcement, Counterterrorism and Intelligence Collection in the United States Prior to 9/11*. Staff Statement No. 9.

Obama, Barack. 2014. "Remarks by the President on Review of Signals Intelligence." Department of Justice, Washington, DC, January 17. www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

Omand, David. 2006. "Ethical Guidelines in Using Secret Intelligence for Public Security." *Cambridge Review of International Affairs* 19 (4): 613–28.

———. 2010. *Securing the State*. London: Hurst, and New York: Oxford University Press.

Omand, D., J. Barlett, and C. Miller. 2012. "Introducing Social Media Intelligence." *Intelligence and National Security* 27 (6): 803–23.

Parker, Andrew. 2015. "Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI) at Thames House, 8 January 2015." MI5 Security Service.

Schneier, Bruce. 2013. "Metadata Equals Surveillance." *Schneier on Security*, September 23. www.schneier.com/blog/archives/2013/09/metadata_equals.html.

Tene, O. and J. Polonetsky. 2002. "Privacy in the Age of Big Data." *Stanford Law Review* 64. www.stanfordlawreview.org/online/privacy-paradox/big-data.

The White House. 2014. "Presidential Policy Directive — Signals Intelligence Activities." Office of the Press Secretary. January 17. www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Troianovski, Anton and Danny Yadron. 2014. "German Government Ends Verizon Contract." *The Wall Street Journal*, June 26. www.wsj.com/articles/german-government-ends-verizon-contract-1403802226.

Vodafone. 2014. "Law Enforcement Disclosure Report." In *Sustainability Report*. www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html.

Whitehead, Tom. 2014. "Internet Is Becoming a 'Dark and Ungoverned Space,' Says Met Chief." *The Telegraph*, November 6. www.telegraph.co.uk/news/uknews/law-and-order/11214596/Internet-is-becoming-a-dark-and-ungoverned-space-says-Met-chief.html.

Yoo, J. and G. Sulmasy. 2007. UC Berkeley Public Law Research Paper No. 1030763. *Michigan Journal of International Law* 28.

ABOUT THE AUTHOR

Sir David Omand was the first UK security and intelligence coordinator from 2002 to 2005 as permanent secretary in the Cabinet Office. Previously, he was permanent secretary of the UK Home Office and director of Government Communications Headquarters (the UK signals intelligence and cyber-security agency). He has a degree in mathematics and theoretical physics and a master's in economics. He is a fellow of Corpus Christi College Cambridge and is senior independent director of Babcock International Group PLC. His book *Securing the State* is published by Hurst (United Kingdom) and Oxford University Press (United States).

CHAPTER SIX:
ETHICS IN THE INTERNET ENVIRONMENT

Rolf H. Weber

ETHICS AS AN ELEMENT OF THE INFORMATION SOCIETY

Notion of Ethics

The term "ethos" as used in Ancient Greece encompasses two different meanings — depending on which of the word's spelling variants one chose to use — namely, habit and custom, or character and morals. Consequently, ethos reflects guiding beliefs or ideals governing the community, such as — according to Aristotle — practical skills, wisdom, virtue, goodness and goodwill. As a result, ethos has the pursuit of a good life as its teleological goal.[1] In ancient times, ethics was linked to natural law, as in Sophocles' play *Antigone*. In clear opposition to King Creon, Antigone does not claim a personal (individual) human right; instead she refers to God's unwritten and unfailing laws. From this perspective, ethical behaviour is seen as a reflection of basic normative principles. The ensuing expectations naturally lead to presumptions about the desired actions and crystallize in a system of rules and institutions that underpin civil society.

In more modern times, ethos started to become an important notion for the legal philosophers of the seventeenth century.[2] Hobbes expressed the opinion that human identity is founded less in the collective social order than in an individual's autonomous rights to exercise his or her natural potential. According to Locke, the identity of an individual vested with self-sustaining attributes reflects natural freedom. Only Rousseau changed the discourse by advocating for a transformation from the natural man to the social man. In Kant's understanding, the moral dignity of the individual must be developed, since humanity is itself a dignity. In other words, for Kant, ethics refers to "right" or "wrong" conduct as part of the philosophy of human behaviour.

Ethics is about acting morally. From a general perspective, morals refer to the empirically valid "established conventions" of any social group. That is, the notion of ethics encompasses the "socially valid moral rights, duties and behavioural norms deriving from a culture-specific tradition" (Ulrich 2008, 31). Ethos therefore can then be seen as an individual's personal conviction, his or her "self-conception in regard to identity and legitimacy" (ibid.). Thus individuals have to justify the moral principles on which their lives are based (ibid.).

Ethics as an academic discipline evaluates normative claims from a transparent and unbiased perspective. Ethics thereby addresses principles or rules that state something about good human actions. Three types of ethics describe its applicable scope (Monteiro 2014). *Descriptive*, or *empirical*, ethics outlines the multiple appearances of practised morals and the customs of individuals, groups, institutions and cultures. *Normative* ethics examines existing attitudes toward morality and frames action-oriented norms. *Meta-ethics* critically scrutinizes ethical methods and extends them.

Objectives of Ethics

Ethics addresses the following concerns (Monteiro 2014): Ethical thinking should reflect the position of those affected by valid moral claims, familiarize them with the critical assessment of practical procedures and encourage attention to issues of social responsibility and moral competence. Ethics also fosters a long-term view of business relationships, that is, fidelity and fiduciary responsibility, as developed in Confucian thinking based on the concept of filial piety (Miles and Goo 2013).

The following fundamental ethical values are relevant to the development of the information society (Global Ethics Network for Applied Ethics 2013; Weber 2015a).

- **Justice/equity**: Every individual has an inalienable dignity and is entitled to equal rights; deep respect for each other cultivates justice; fair and equal access to information enables members of civil society to reach for bilateral understanding.
- **Freedom**: Human dignity calls for the development of various freedoms: in the Internet context, for example, the freedom of expression, of beliefs and of access to information. As a consequence, freedom, equality and responsibility must balance each other.
- **Care and compassion**: A capacity for empathy and respect leads to solidarity and reciprocal support.
- **Participation**: The right and ability to participate in societal life and in important decision-making processes are core values.
- **Sharing**: The sharing of information and knowledge in the Internet context enables and leads to sustainable relationships between human beings, and, as a result, strengthens communities.
- **Sustainability**: In the long term, sustainable projects are significant for the protection of a viable environment for all human beings.
- **Responsibility**: Assuming accountability for one's own actions is a core requirement in a societal setting. The level of responsibility must correspond to the levels of the individual's power, capacity and capability.

[1] See Weber (2015a, 100-101) for a general overview.

[2] See Indaimo (2015, 16–32) for more details.

These different ethical values are interlinked and can balance each other. In contrast to diverging human rights (for example, freedom of expression versus privacy), direct conflicts of interests hardly exist between the ethical values described above. Human rights can even be seen as formalized ethics (Global Ethics Network for Applied Ethics 2013).

Scope of Ethics in the Internet Environment

The realization of ethics depends on the opportunities and willingness to apply them in practical life. As the objectives of ethics clearly show, virtually no space in the information society lies outside of the behavioural rules that can guide moral actions. Since the ethical values are interlinked, their scope is almost unlimited.

Regarding the importance of practical circumstances, two case studies might help to identify the actual main challenges for ethical principles. The first case study examines the treatment of ethics in the many and diverse Internet governance declarations adopted during the past 10 years. The second study considers social network providers' compliance with ethical standards. Each study shows the practical challenges in implementing ethics principles and further suggests how some of the benefits of ethical behaviour can be achieved.

These two case studies have been deliberately chosen to address different societal fields. Internet governance is a global issue involving many stakeholders and requires the design of general rules for interconnected network infrastructures; that is, Internet governance plays at a macro level. In contrast, the relationships between social networks and their users are based on contracts, whatever their form; these relationships occur at the micro level. For such reasons, the two case studies attempt to approach ethics from different angles. Thereafter, the question of whether generally applicable notions of ethics can be developed is tackled.

ETHICS IN INTERNET GOVERNANCE

The role of ethics has come up in Internet governance discussions at various fora, but the issue has never been the main focus. The next section summarizes a detailed analysis (Weber 2015b) of the current state of the discussion, as published in a recent United Nations Educational, Scientific and Cultural Organization (UNESCO) report.[3]

Ethics as a Key Element in Internet Governance Declarations

More than 11,000 participants from 175 countries attended the first phase of the World Summit on the Information Society (WSIS) in Geneva in December 2003. At the end of the Summit, which was aimed at establishing the foundations for an information society, the "Declaration of Principles" (WSIS 2003a) and the "Plan of Action" (WSIS 2003b) were among the statements adopted that made ethics a subject of discussion.

The Geneva "Declaration of Principles" seeks to ensure that everyone can benefit from the opportunities of information and communication technology (ICT). It declares that addressing the ethical dimensions of the information society is a key principle for all stakeholders in building an inclusive information society (WSIS 2003a, number 19). The declaration exhorts the information society to respect peace and uphold fundamental values such as freedom, solidarity and shared responsibilities (ibid., number 56) and, by highlighting the importance of ethics for the information society, invites all actors to take appropriate actions and preventive measures (ibid., number 59). In this context, the document calls for the responsible use and treatment of information by the media in accordance with the highest ethical standards (ibid., number 55). Advocating an information society that is subject to universally held values, promotes the common good and prevents abusive reliance on ICT (WSIS 2003b, number 25), the "Geneva Plan of Action" invites all stakeholders to increase their awareness of the ethical dimensions of Internet use (ibid., number 25.c) and further encourages all relevant stakeholders to continue to research the ethical dimensions of ICT (ibid., number 25.d).

In May 2013, almost one decade later, the "Global Ethics Network for Applied Ethics" published its discussion paper "Ethics in the Information Society: The Nine 'P's," on ethical issues related to the Internet (Global Ethics Network for Applied Ethics 2013). The document calls for value-based decisions and actions in the development of information, communication and knowledge (ibid., preface). It discusses ethical values (ibid., 8), the ethics of information professions (ibid., 14) and the ethics of regulation and freedom (ibid., 24). The paper also advocates for an ethical dimension as a fundamental pillar of the information society post 2015 (ibid., 26) and calls for experts under the aegis of the international organizations concerned to further discuss the principles of an ethical information society. Private sector enterprises should take the initiative in introducing ethics into the information society (ibid., 27). All in all, the future governance of the Internet should be based upon ethical values (ibid., 27-28).

The "Riga Guidelines on Ethics in the Information Society," as agreed upon by the Riga Global Meeting of Experts on the Ethical Aspects of Information Society in October 2013 (UNESCO 2013), are meant to encourage debate on the ethical challenges of the information society (ibid., number 2), raise awareness of the ethical implications of the ICT use and development (ibid., number 4), and demand the support and participation of all interested stakeholders in the discussion of information ethics (ibid., number 5). The guidelines call on policy makers to be ready to give

[3] See also Weber (2015a, 96–100).

consideration to ethical principles (ibid., number 8) and to support policy makers' development of ethically informed frameworks and decision-making tools based on universal human rights and ethical principles (ibid., number 10).

UNESCO is considered the most important organization offering a constant review of ethics issues. Its document "UNESCO and the ethical dimensions of the information society" of September 14, 2012, addresses the organization's key role in developing ethical perspectives to enable social and human progress for the information society (UNESCO 2012, 7), its contribution to the international debate on the ethical dimensions of the information society (ibid., 8), ongoing global efforts in the field of ethical dimensions of the information society (ibid.), and proposals for possible ways UNESCO could address ethical dimensions of the information society (ibid., 9-10). Besides that, its "Reflection and Analysis by UNESCO on the Internet," adopted by UNESCO on April 18, 2011, also acknowledges ethical standards as being essential (UNESCO 2011).

General References to Ethics in Internet Governance Declarations

A number of declarations, guidelines and frameworks mention ethical issues in the context of other topics.

The "Tunis Agenda for the Information Society," adopted at the WSIS in November 2005, calls for the responsible use and treatment of information by the media in accordance with the highest ethical and professional standards (WSIS 2005, number 90).

The "Tshwane Declaration on Information Ethics in Africa" was adopted by the participants of the African Information Ethics Conference: Ethical Challenges in the Information Age, on February 7, 2007 (African Information Ethics 2007). The declaration considers ethics in the Internet as being a matter of critical reflection on moral values and practices with regard to the production, storage, distribution and access to knowledge. The declaration notes the necessity of ethical reflections on norms and values and points to the important role that information ethics should play in African education and policy in fostering social, cultural and economic development (ibid., preamble). According to the declaration, policies and practices regarding the generation, dissemination and utilization of information in and about Africa should be grounded in ethics based on universal human values, human rights and social justice.

The final recommendations of the European Conference on Ethics and Human Rights in the Information Society of September 2007 emphasize the need to proclaim universal ethical principles (UNESCO 2007, number 2), to monitor issues relating to ethics in knowledge societies (ibid., number 3), to translate principles into codes of ethics at all levels (ibid., number 4), and to encourage and develop ethics (ibid., number 6).

In 2013 the Working Party on Internet-mediated Research, under the auspices of the British Psychological Society (2013), published the *Ethics Guidelines for Internet-mediated Research.* The guidelines outline some key issues that researchers are advised to keep in mind when considering the implementation or evaluation of an Internet-mediated research study. They reinforce the main ethics principles as outlined in the British Psychological Society's (2010) *Code of Human Research Ethics,* namely, respect for the autonomy and dignity of persons, scientific value and social responsibility, as well as the maximizing of benefits and minimizing of harm to persons.

On May 12, 2014, the Council of the European Union published the *EU Human Rights Guidelines on Freedom of Expression Online and Offline* (Council of the European Union 2014), pointing to, among other things, the fact that an open society based on the rule of law needs an independent and pluralistic media environment offline and online for operating effectively. It further suggests that society needs to encourage the promotion of mechanisms such as media ethics codes within third countries (countries outside the European Union) to enhance media accountability (ibid., number 32.g).

Some additional declarations and guidelines mention ethical issues without elaborating on the specifics of the individual values.

The Internet Activities Board's "Ethics and the Internet" document of 1989 deals with ethics in general. Giving examples of unethical behaviour, the Internet Activities Board (1989, 2) characterizes as unethical and unacceptable any activity that purposely seeks to gain unauthorized access to the resources of the Internet, disrupts the intended use of the Internet, destroys the integrity of computer-based information and/or compromises users' privacy.

The "Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace," published by UNESCO in October 2003, states that ICT training should not be limited to the provision of technical competences but should also include awareness of ethical principles and values (UNESCO 2003, 19).

According to "The Seoul Declaration for the Future of the Internet Economy," adopted in June 2008 under the auspices of the Organisation for Economic Co-operation and Development (OECD), the secure and responsible use of the Internet should be promoted and international social and ethical norms are to be respected (OECD 2008).

Without addressing ethics in more detail, the "African Platform on Access to Information Declaration" of September 2011 calls on media to respect professional ethics and journalism standards (African Platform on Access to Information Campaign 2011, 8).

In February 2013, the WSIS+10 Conference issued a "Final Statement: Information and Knowledge For All," inviting all stakeholders to discuss the ethical challenges of emerging technologies and the information society (WSIS+10 2013, 3).

The Special Rapporteurs from the United Nations, the Organization for Security and Co-operation in Europe, the Organization of American States and the African Commission on Human and Peoples' Rights agreed on a "Joint Declaration on Universality and the Right on Freedom of Expression" in May 2014 that, without discussing ethical aspects in detail, recommends that media play a positive role in countering discrimination, stereotypes, prejudices and biases by adhering to the highest professional and ethical standards (Organization for Security and Cooperation in Europe 2014, number 2.c.).

Also without addressing ethics in detail, the "Bali Road Map," adopted at the Global Media Forum in Bali in August 2014, supports the promotion of respect for the highest professional and ethical standards in journalism (Global Media Forum 2014, number 1).

The "Nairobi Declaration on the Post 2015 Development Agenda" of November 2014, as agreed at the Global Forum for Media Development in Nairobi, highlights poor ethical values in some sectors of society, including governments, the private sector and the general public (Global Forum for Media Development 2014, observations). The declaration recommends that media regulatory bodies, media professional associations and unions and the media community in general ensure that the media around the world maintain ethical standards (ibid., recommendations).

Interim Assessment

This detailed analysis shows that the subject of ethics is addressed in many Internet governance declarations, guidelines and frameworks but that its treatment is rather disparate. In substance, the importance of ethics is not adequately reflected. For example, drawing on the general objectives of ethics, basic values such as justice and equity, participation and sustainability are not adequately taken into account. The key value of responsibility is also underestimated.

In a nutshell, much has been written, but the diverse quantity of review is lacking the substantive quality needed to result in adequate ethical standards in Internet governance. As a consequence, a more accurate assessment of the main ethical principles in the digital environment appears to be necessary.[4]

ETHICS IN SOCIAL NETWORKS

Online social networks such as Facebook, Google, Twitter and others have not only wide-ranging economic but also social and cultural impacts on the online world. Having enjoyed a vast increase in members and users during the past few years, online social networks have now recognized that compliance with ethical principles is a reputational issue. Acting in compliance with ethical principles improves the reputation of social networks, which in turn helps to gain users' trust and makes the service providers more attractive to potential customers. Of course, gaining and retaining more customers also enhances the networks' advertising revenues.

Therefore, at least rhetorically, social networks increasingly proclaim the ethical standards they follow as well as the corporate social responsibility (CSR) principles they observe. The public statements of social networks do not necessarily coincide with the reality, however. For that reason, it is worth examining the compliance by social networks with ethical principles in practice and at the micro level of ethics.

Contractual Relations: Theory and Reality

The public announcements of social networks that they comply with high ethical standards must be mirrored in reality; that is, the practical implementation of the standards must be subject to review. As an example, the activities of the microblogging site Twitter (twitter.com) and of other social networking sites are assessed here. These service providers offer users from all over the globe opportunities to share personal information and to participate in public discourse.

However, commercial imperatives, particularly the interests of the advertising industry, tend to direct user participation to an asymmetrical private regulation, mainly expressed in the social networks' terms of service — which do not necessarily take into account the interests of the users (for example, the avoidance of large-scale processing of personal data). These terms of service regulate the rights of the users, for example, regarding informational privacy and intellectual property, in a way that does not restrict the marketing activities of the social networks.[5] Such behaviour is problematic because these social networks are thus acting as quasi-governmental regulators (Busch 2013).[6]

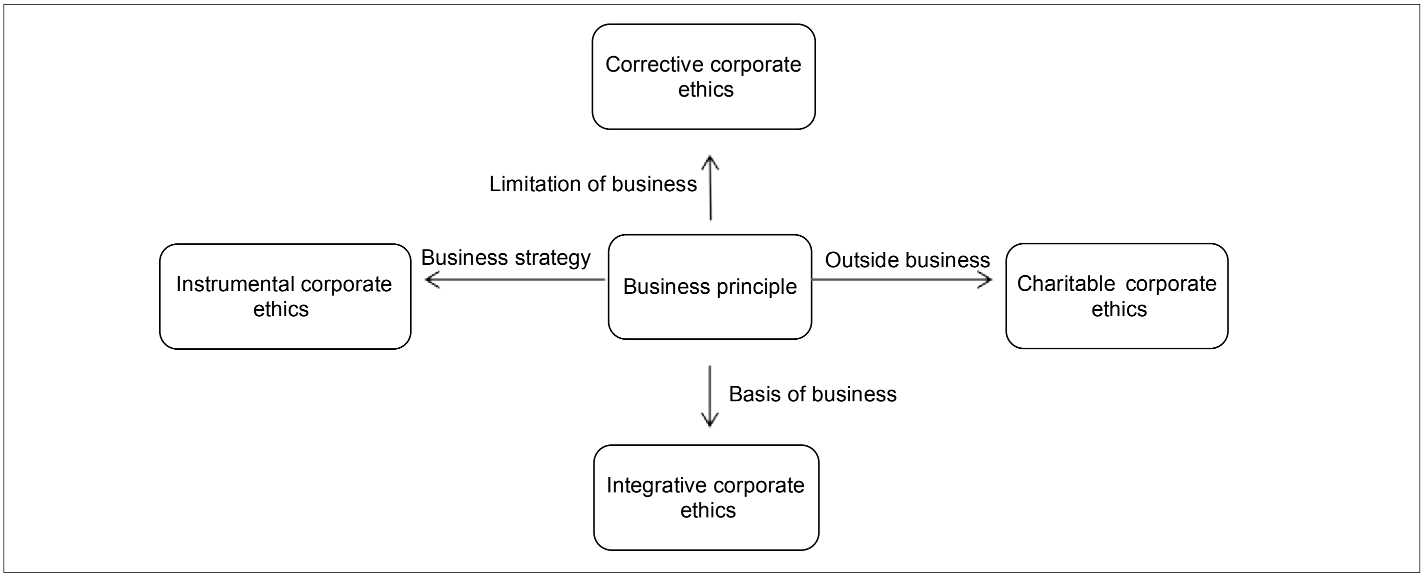
Ethics is often combined with the concept of CSR to be understood as the responsibility of commercial entities for their impact on society. Such frameworks encompass not only fundamental rights and additional societal elements, but also objectives of sustainability and overcoming the

[4] See "Lessons for Improving the Ethics Environment" below.

[5] For a general overview see Busch (2013, 56–87).

[6] For further details, see the section "Special Problem: Quasi-governmental Function of Social Networks" below.

Figure 1: Relations between Ethics and Business Principles


Corrective corporate ethics
Limitation of business
Business strategy
Instrumental corporate ethics
Business principle
Outside business
Charitable corporate ethics
Basis of business
Integrative corporate ethics

Source: Version of figure by Ulrich (2013, 399), adapted and reprinted with permission.

digital divide (Weber 2013). CSR requires a due diligence process that enables an enterprise to interact with all its stakeholders and with society at large, thereby identifying, preventing and mitigating possible adverse impacts from business operations (Weber 2012).

Twitter attracts Internet users and gains new members by offering participation in a "real-time information network" that supports free speech. The online social network is among others stating that they "believe that the open exchange of information can have a positive global impact."[7] These good intentions should be considered in light of the well-known adage that many successful business people take to heart: "The business of business is business" (Ulrich 2008). Some of the online social network's practices do not seem to coincide with the mentioned CSR principles and so they therefore appear to be ethically problematic. Twitter retains a wide-ranging licence over all content posted via its site and, furthermore, profits from collecting and using its customers' personal information for advertising purposes, a common practice of online social networks. These ethically debatable procedures can be observed in a thorough analysis of Twitter's "About Us" (Busch 2013).

It cannot be overlooked that Twitter and other social networks often seem to awaken an "instrumental CSR" ethos that fails to properly reflect the moral rights, responsibilities and strategic challenges that ICT companies face when interacting with stakeholders. In addition, the regulatory role played by social networks in the online environment makes it difficult to think critically about the actual implications of their role as quasi-regulators for notions of users' rights (ibid.). Simply stated, an important difference exists between the social networks' behaviour on paper and their behaviour in reality.

Corporate Ethics: Improving the Accountability Principle

The described contractual practices can be measured against various types of corporate ethics. In that regard, Peter Ulrich[8] differentiates between instrumental corporate ethics, charitable corporate ethics, corrective corporate ethics and integrative corporate ethics (Figure 1).

Busch, closely following Ulrich, defines the four types of business ethics slightly differently (Busch 2013, 59–62):

- **Functionalist business ethics** considers commercial ethics a mere function of the market mechanism; maximizing profits and increasing stakeholders' values are ethically sound in themselves (Busch 2013).

- **Instrumental business ethics** addresses ethics as a business tool for making profits in the long run (entrepreneurial success) (ibid.; Ulrich 2008). This more progressive approach is based on the idea that it might pay off later for companies to refrain from ethically questionable business decisions in building trust among its customers (Busch 2013). Without careful consideration of the moral point of view, the only motivators for this behaviour are the prospects for profits in return.

- **Charitable business ethics** aims at obtaining maximum profits as the primary moral duty of the business. The

[7] See https://about.twitter.com.

[8] For details of the aspects of corporate ethics, see Ulrich (2008, 376–442).

ethical element appears in the way a company spends its money (ibid.; Ulrich 2008). The more profit a company achieves, the more charitable projects it has to support. From a time perspective, this type of ethics is realized after the event has occurred (Ulrich 2008, 402).

- **Integrative business ethics** demands of companies that they involve ethical aspects in business decisions from the beginning (Busch 2013; Ulrich 2008). Ulrich (2008, 409) considers this approach a "permanent process of unconditional critical reflection and the shaping of sound normative foundations for entrepreneurial activity in the service of life."

A comparative analysis shows that Busch replaces Ulrich's term "corporate" with the term "business," which convincingly encompasses a broader definition in the economic environment. In addition, instead of following Ulrich's corrective ethics, which looks at the situative self-limitation of the entrepreneurial pursuit of profit, Busch applies a functionalist approach and goes back to the basics of business behaviour in a market-driven economy. In assessing social networks' policies, however, the slight deviations between the two models are not significant. But the weakness — no matter which definition of business ethics is used — consists of Twitter's partial non-compliance with basic ethical objectives such as justice and equity, care and compassion.

These ethical objectives are not met as a result of the economic rationality of Twitter's business practices. In particular, the elements of integrative ethics are not made fruitful in the practical environment. Normative tensions occur therefore, since the ethical behaviour is operationalized in instrumental ways. Twitter's role as a public, user-centric "platform" on the one hand and as a commercial service on the other should lead to a rights-based approach focusing on issues such as users' privacy and intellectual property rights.

However, as outlined, these rights are substantially restricted in Twitter's terms of service (Busch 2013). In particular, integrative business ethics are not applied as an important ethical discipline. In addition, accountability mechanisms should be substantially improved;[9] the lack of adequate accountability is a weakness in that non-compliance with the stated ethical principles does not have specific consequences. The lesson is that corporate ethics still leaves room for more ethical behaviour patterns.

Special Problem: Quasi-governmental Function of Social Networks

Social networks obviously play a role as gatekeepers and intermediaries. They are thereby positioned to apply censorship, both in a positive and in a negative manner. Since existing social networks, so far, have an almost state-like structural role, Rebecca MacKinnon (2012, 149) calls online social networks "sovereigns of cyberspace" and ironically refers to "Facebookistan" and "Googledom" when analyzing these companies' far-reaching power in the present online environment. Furthermore, social network platforms can determine what users are able to do or not do in their respective online territories. As a consequence, Facebook and Google are criticized as being an expression of a "new feudalism" (Busch 2013, 71).

ICT companies and social networks exercise a "quasi-governmental" function on two levels. The first level is in how their core business models (that is, how they make money) have a direct influence on their stakeholders. The second level is in the ways the business models interact indirectly with their stakeholders — for example, by way of technical or legal industry standards, or by shared and agreed-upon business practices within the industry (Busch 2013).

In view of these developments, MacKinnon proposes that online social networks such as Facebook should only be perceived as having implemented acknowledged and legitimate regulations as corporate actors *if* a number of elements are fulfilled. First of all, to be compatible with democracy and human rights, the online social networks' approach to governance must evolve (MacKinnon 2012). Having become the public squares of the Internet, online social networks need to realize and address the reality that they have become de facto political regulators whose legitimacy is constantly questioned and contested.[10] Further, to improve their decision-making processes and gain legitimacy, social networks should engage in unconditional dialogue with their stakeholders, ideally by taking on concrete roles and a "deliberative corporate policy" (Ulrich 2008, 418).

Given that Facebook, Google and other online social networks depend on the participation of their members, Internet users need to accept their own responsibility as well. To be respected online, they must actively speak out for their rights and create a more citizen-driven information environment (MacKinnon 2012). Accordingly, users need to stop behaving like passive customers and start acting like responsible netizens (citizens of the Internet) (ibid.). In addition, they need to hold companies running social networks accountable for their regulatory decisions (Weber 2009b; Busch 2013). In order to improve transparency, therefore, companies should regularly and systematically inform the public of how gathered information is monitored and under which premises the content gets removed or blocked (MacKinnon 2012). The more netizens actively

[9] For further details, see Weber (2009a, 152–67).

[10] According to MacKinnon (2012, 164), online social networks such as Google Plus or Facebook share a Hobbesian approach to governance by having a social contract with digital sovereigns: Internet users agree to give up some freedoms to the benefit of a sovereign in exchange for getting security and other services.

use their rights, the harder it is for governments and corporations to reduce their freedoms (ibid.).

Interim Assessment

Knowing the importance of acting in compliance with ethical principles, most online social networks at least pretend to agree with the concept of corporate social responsibility. However, some of their practices seem to be ethically problematic, as in, for instance, the common practice of profiting from collecting and using their customers' personal information for advertising purposes. In reality, the social networks do not live up to established ethical principles such as fairness or accountability. Only to a certain extent do they comply with corporate ethics.

In addition, since they are acting as quasi-governmental regulators, online social networks should be obliged to improve their legitimacy by engaging in unconditional dialogue with all concerned stakeholders. Such duty is owed because social networks are particularly expected to comply with behavioural rules since their position reflects an imbalance between them and their customers, deviating from the traditional equal and level understanding of partners in contractual relations.

LESSONS FOR IMPROVING THE ETHICS ENVIRONMENT

The two case studies examined here have shown that ethical issues are not completely neglected in the respective discussions but that practical compliance with theoretical principles does not meet the expectations of the involved stakeholders. To actually improve ethical thinking, the "ethics lite" approach must be overcome. The two chosen examples, representing the macro level and the micro level, respectively, could obviously be complemented by further case studies. Worthwhile research could also encompass ethical standards for technologists and international organizations, but those discussions exceed the scope of this chapter. Nevertheless, the two case studies conducted do allow reasonable lessons to be drawn for improving the ethics environment.

Enshrining a Fundamental Trust

Irrespective of its design, a technological system should inspire trust. From an ethical perspective, trust enhances cooperation and fosters reciprocal relations (Pettit 2008). As a consequence, improved ethics for emerging technologies are needed, and Internet applications should be designed in a way that they are considered trustworthy in the eyes of civil society. Therefore, in the Internet governance context, special attention should be paid to data security issues and accountability requirements.

Further, trust is also linked to "reliance." If an individual is relying on something or someone to display a trait or behaviour, then this individual is acting in a way that is shaped by a more or less confident belief in the other party having displayed it (Weber 2015a). Trust is particularly important in the context of cyber threats and cyber security. For example, the building of trust can be improved by better sharing of information or by introducing more appropriate norms of reliance.[11] But reliance and trust also play an important role in a contractual setting. Social networks that do not comply with expected behavioural values breed mistrust in the long run.

Trust should additionally be viewed through the lens of confidence. Any confidential interaction must establish a process of credential exchange. In the dynamic context of the Internet, where interactions are rapidly changing, trust relations must lead to the use of reputation systems, which can contribute to establishing reliability in the virtual world (for example, in social networks) (Pettit 2008). Building trust must also be more strongly addressed within the Internet Corporation for Assigned Names and Numbers (ICANN) regulatory framework. Many members of civil society do not have sufficient trust in institutional settings; they do not trust corporate bodies to adequately comply with public interest considerations.[12]

The other element critical to building trust, reliance and confidence is accountability — that is, the acknowledgment and assumption of responsibility for actions, decisions and policies within the scope of the designated role. Accountability consists of the obligation of a person to another, according to which the former must give account of, explain and justify his actions or decisions against criteria of the same kind, as well as take responsibility for any fault or damage (Weber 2009b). The strict implementation of an adequate accountability regime has a positive impact on trust. The importance of accountability has already been realized in the Internet governance framework. At the ICANN meeting of March 2016 in Marrakesh, the governments agreed to implement general ICANN accountability principles.

Realizing a Knowledge Society

Ethical considerations make it imperative that the information society is developed into a knowledge society. In this context, six aspects need to be considered (Global Ethics Network for Applied Ethics 2013, 12-13).[13]

- **Value-based approach**: Knowledge should be shared fairly, equally, freely, and for the benefit of caring, sustainable communities, thereby respecting the diversity of cultures, languages, religions and economic as well as political systems.

[11] For further details, see Bradshaw (2015, 11-12 and 14).

[12] See also Taylor (2015, 7–10).

[13] The following text is based on Weber (2015a, 105-106).

- **People-centred framework**: Technology should not be a goal in itself, but should serve individuals in their personal development.
- **Communities and identities-oriented solutions**: The Internet has a tendency to increase individualism, yet the needs and rights of individuals and of communities should be balanced, particularly since the flood of information leads to constant construction and reconstruction of identities.
- **Education-focused approach**: Information ethics calls for the responsible treatment of information. Education in critical media consumption, including the use of social media, can help stakeholders deal with information.
- **Gender-oriented design**: Somewhat neglected in previous Internet governance declarations (Weber 2015b), gender equality is an important dimension of an inclusive and people-centred society. Ensuring women's parity encompasses access to information, communication, knowledge and decision making.
- **Generation-sensitive framework**: Technological literacy helps to increase participation by all individuals in societal matters and particularly facilitates intergenerational exchange of knowledge.

The improvement of knowledge generation and sharing is mentioned in a good number of Internet governance declarations;[14] however, the substantive contents of these declarations remain relatively vague. The implementation of ethical guidelines as described above could make the framework for a knowledge society more concrete and the realization of the respective objectives more likely. Accordingly, more attention should be paid to issues such as education, multilingualism and cultural diversity (Weber 2015b). An emphasis on knowledge gained and shared can contribute to the ethical objectives of participation and mainly of sharing, leading to strengthened communities and sustainable relationships between human beings.

Avoiding a Digital and Access Divide

Ethical standards relate to social justice. Among the many different conceptions, social justice means fair distribution of benefits and burdens, as well as equal opportunities to take advantage of the technological advancements. In addition, social justice can contribute to social integrity and prevent social disparities (Weber 2015a).

A key issue is access to the virtual world. The ideal is avoiding disadvantages and unfairness in accessing knowledge, empowerment and other vital resources for individuals' well-being (ibid.). Virtual networks have become the public space for private communications and business transactions as well as for relations between governments and civil society. Exclusion from this space deprives concerned persons from participation in social and civic life.

The digital divide has been debated for more than 10 years. Beyond overcoming the digital divide, ethics also requires us to prevent the "access divide" to knowledge resources. This means reinforcing free and fair access to knowledge (also for developing countries), supporting open-access repositories (including training and support), developing regional hubs that index open-access repositories, and implementing open publishing initiatives including global visibility, accessibility and values (Global Ethics Network for Applied Ethics 2013). Even though there is evidence that levels of access to the Internet are growing in developed countries (Weber and Menoud 2008), a large part of humankind is still excluded from the Internet.

Overcoming the access divide can also be seen in the context of enhancing democracy and democratic institutions, providing the public with sufficient opportunities for effective public deliberation and participation in democratic processes. Equitable participation of all stakeholders from all regions of the world, while acknowledging the diversity of cultures, will also enable individuals to respond to the ethical challenges of the information society (UNESCO 2013, numbers 3 and 5). Since participation and sharing are key ethical objectives, greater attention to combatting the digital and access divide will improve the ethics environment.

Developing an Open Society

Recent technological developments and the growing involvement of civil society in cyberspace are perceived to be leading to the establishment and development of an open society (Weber 2014). In parallel, fundamental ethical values such as inalienable human dignity, basic freedoms, social responsibility and justice also have a global scope (as in McLuhan's vision of the global village, now possible in the electronic metropolis) and can promote public awareness of those principles (Weber 2015a).

The open society concept, as postulated by Karl Popper in 1945, strives to preserve individual freedom as well as the ideal of political-ideological pluralism (Popper 1945). The thinking is that openness and acceptance of other approaches to and solutions for problems would contribute to an environment that would allow the best alternative to establish itself (Weber and Weber 2009). An open society ideally offers space for individuals to access existing choices while reckoning their consequences and taking responsibility for the final outcome of their choices (Jarvie 1999).

[14] See "Ethics in Internet Governance" above.

An open society also depends on the existence of ethical standards to which members of civil society must comply. The resulting "guidelines" will mainly concern behavioural rules. For example, the ethical objectives of care and compassion are particularly addressed to civil society. So, in this context, civil society has to bear the ethical "burden." In the past, limited attention has been paid to the potential contribution of civil society to the realization of ethics; however, the compliance of civil society members with ethical objectives merits deeper consideration.

In the digital world, public fora allowing exchanges of opinions are available and enable the involvement of participants with different backgrounds and many and diverse ideas (Weber 2014). Given that new possibilities for participation may be developed and previous processes can be improved, a fair chance exists that cyberspace can serve as an apt tool for an open society (ibid.).

CONCLUSION

Although ethics played a certain role in recent years' Internet governance discussions, the subject has never gained substantive attention. A recently published UNESCO study supports this observation. Ethical issues are mentioned mostly in the context of other topics, and detailed discussion of the many facets of ethics is generally lacking. More effort should be invested in the practical realization of ethical principles in Internet governance frameworks.

In view of the growing importance of online social networks and their wide-ranging economic, social and cultural impacts, the public focus should increasingly concentrate on the ethical aspects of Twitter, Facebook, Google and others. Demanding immediate attention are the online social networks' common practice of monetizing customers' personal information for advertising purposes and their quasi-governmental functions.

Online social networks need to "live" ethical behaviour and corporate social responsibility by putting their virtuous-sounding marketing statements into practice. Matching their fine words with reality will improve their reputations and make them more attractive to potential customers. Besides that, further efforts are needed to enable developing countries' access to the Internet, since a large part of the world is still not able to participate online.

Ethics takes the form of behavioural directives stemming from values such as justice and equity, care and compassion, and responsibility. These values need not only formal attention in documents such as international guidelines and frameworks, but also concrete application in daily life. Ongoing discussions about the design and shape of the information society provide a suitable forum to enable a deeper understanding of ethical considerations.

WORKS CITED

African Information Ethics. 2007. "Tshwane Declaration on Information Ethics in Africa." February 7. www.africainfoethics.org/tshwanedeclaration.html.

African Platform on Access to Information Campaign. 2011. "African Platform on Access to Information Declaration." Pan African Conference on Access to Information, Cape Town, September 19. www.africanplatform.org/campaign/apai-declaration/.

Bradshaw, Samantha. 2015. *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity.* GCIG Paper Series No. 23. Waterloo, ON: CIGI. www.cigionline.org/publications/combatting-cyber-threats-csirts-and-fostering-international-cooperation-cybersecurity.

British Psychological Society. 2010. *Code of Human Research Ethics.* INF 180/04.2011. Leicester, UK: British Psychological Society. www.bps.org.uk/sites/default/files/documents/code_of_human_research_ethics.pdf.

———. 2013. *Ethics Guidelines for Internet-mediated Research.* INF206/1.203. Leicester, UK: British Psychological Society. www.bps.org.uk/system/files/Public%20files/inf206-guidelines-for-internet-mediated-research.pdf.

Busch, Thorsten. 2013. "Fair Information Technologies: The Corporate Social Responsibility of Online Social Networks as Public Regulators." Thesis, University of St. Gallen.

Council of the European Union. 2014. *EU Human Rights Guidelines on Freedom of Expression Online and Offline*. Foreign Affairs Council Meeting, Brussels, May 12. http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf.

Global Ethics Network for Applied Ethics. 2013. *Ethics and the Information Society: The Nine 'P's*. www.globethics.net/documents/4289936/14121854/InformationEthics_TextsSeries_04_WSIS_EN_text.pdf/8492ed8f-0818-4a18-8c3e-d1a61221f8ac.

Global Forum for Media Development. 2014. "Nairobi Declaration on the Post 2015 Agenda." November 14. http://gfmd.info/en/site/news/721/The-Nairobi-Declaration-on-the-Post-2015-Development-Agenda.htm.

Global Media Forum. 2014. "Bali Road Map: The Roles Of The Media In Realizing The Future We Want For All." August 28. http://gfmd.info/en/site/news/368/The-Global-Media-Forum-adopted-the-Bali-Roadmap-for-the-inclusion-of-media-in-the-post-2015-agenda.htm.

Indaimo, Joseph A. 2015. *The Self, Ethics and Human Rights*. New York, NY: Routledge.

Internet Activities Board. 1989. "Request for Comments 1087: Ethics and the Internet." January. https://tools.ietf.org/html/rfc1087.

Jarvie, Ian. 1999. "Popper's Ideal Types: Open and Closed, Abstract and Concrete Societies." In *Popper's Open Society after Fifty Years: The Continuing Relevance of Karl Popper*, edited by Ian C. Jarvie and Sandra Pralong, 71–82. London, UK: Routledge.

MacKinnon, Rebecca. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York, NY: Basic Books.

Miles, Lilian and Say H. Goo. 2013. "Corporate Governance in Asian Countries: Has Confucianism Anything to Offer?" *Business and Society Review* 118: 23–45.

Monteiro, A. Reis. 2014. *Ethics of Human Rights*. Cham, Switzerland: Springer.

OECD. 2008. "Seoul Declaration for the Future of the Internet Economy." June 17-18. www.oecd.org/sti/40839436.pdf.

Organization for Security and Cooperation in Europe. 2014. "Joint Declaration on Universality and the Right on Freedom of Expression." May 6. www.osce.org/fom/118298.

Pettit, Philip. 2008. "Trust, Reliance and the Internet." In *Information Technology and Moral Philosophy*, edited by Jeroen Van den Hoven and John Weckert, 161–74. Cambridge, UK: Cambridge University Press.

Popper, Karl. 1945. *The Open Society and Its Enemies.* London, UK: Routledge.

Taylor, Emily. 2015. *ICANN: Bridging the Trust Gap.* GCIG Paper Series No. 9. Waterloo, ON: CIGI. www.cigionline.org/sites/default/files/gcig_paper_no9.pdf.

Ulrich, Peter. 2008. *Integrative Economics: Foundations of a Civilised Market Economy.* New York, NY: Cambridge University Press.

UNESCO. 2003. "Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace." Paris, France: UNESCO, October 15. http://portal.unesco.org/en/ev.php-URL_ID=17717&URL_DO=DO_TOPIC&URL_SECTION=201.html.

———. 2007. "European conference on 'Ethics and human rights in the information society.' Final Recommendations." Strasbourg, September 13-14. http://portal.unesco.org/ci/en/files/26941/12121514093FinalRecommendations_en.pdf/FinalRecommendations_en.pdf.

———. 2011. "Reflection and Analysis by UNESCO on the Internet." 186EX/37. Paris, France: UNESCO, April 18. http://unesdoc.unesco.org/images/0019/001920/192096e.pdf.

———. 2012. "UNESCO and the ethical dimensions of the information society." In *Report by the Director General on the Follow-up to Decisions and Resolutions Adopted by the Executive Board and the General Conference at Their Previous Sessions.* 190 EX/5. Paris, France: UNESCO, September 14. http://unesdoc.unesco.org/images/0021/002173/217316e.pdf.

———. 2013. "Riga Guidelines on Ethics in the Information Society." Riga Global Meeting of Experts on the Ethical Aspects of Information Society, Riga, Latvia, October 16-17. www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/ifap/ifap_riga_guidelines_ethics_in_information_society_en.pdf.

Weber, Rolf H. 2009a. "Accountability in Internet Governance." *International Journal of Communications Law & Policy* 13: 152–67.

———. 2009b. *Shaping Internet Governance: Regulatory Challenges.* Zurich, Switzerland: Schulthess.

———. 2012. "Corporate Social Responsibility as New Challenges for the IT Industry." *Computer Law and Security Review* 28 (6): 634–40.

———. 2013. "Responsibilities of Business as New Topic in Internet Governance Debates." *Journal of Internet Law* 16 (11): 3–12.

———. 2014. *Realizing a New Global Cyberspace Framework: Normative Foundations and Guiding Principles.* Zurich, Switzerland: Schulthess.

———. 2015a. "Ethics as Pillar of Internet Governance." *Jahrbuch für Recht und Ethik* 23: 95–111.

———. 2015b. *Principles for governing the Internet: A comparative analysis*. Paris, France: UNESCO Series on Internet Freedom. http://unesdoc.unesco.org/images/0023/002344/234435e.pdf.

Weber, Rolf H. and Valerie Menoud. 2008. *The Information Society and the Digital Divide: Legal Strategies to Finance Global Access*. Zurich, Switzerland: Schulthess.

Weber, Rolf H. and Romana Weber. 2009. "Social Contract for the Internet Community? Historical and Philosophical Theories as Basis for the Inclusion of Civil Society in Internet Governance?" *SCRIPT-ed* 6 (1): 90–105.

WSIS. 2003a. "Declaration of Principles: Building the Information Society: a global challenge in the new Millennium." Document WSIS-03/GENEVA/DOC/4-E. Geneva, Switzerland: WSIS, December 12. www.itu.int/net/wsis/docs/geneva/official/dop.html.

———. 2003b. "Plan of Action." Document WSIS-03/GENEVA/DOC/5-E. Geneva, Switzerland: WSIS, December 12. www.itu.int/net/wsis/docs/geneva/official/poa.html.

———. 2005. "Tunis Agenda for the Information Society." Document WSIS-05/TUNIS/DOC/6(Rev. 1)-E. Geneva, Switzerland: WSIS, November 18. www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

WSIS+10. 2013. "Final Statement. Information and Knowledge For All: an expanded vision and a renewed commitment." Paris, France: WSIS+10, February 25–27. www.itu.int/net/wsis/review/inc/docs/2013.WSIS10_Final-Statement_EN.HD.pdf.

ABOUT THE AUTHOR

Rolf H. Weber is ordinary professor for civil, commercial and European law at the University of Zurich, Switzerland, and a visiting professor at the University of Hong Kong in China. His main fields of research are Internet and information technology law, international business law, media law, competition law and international finance law. He is a director of the European Law Institute and the Center for Information Technology, Society and Communication Law at the University of Zurich. From 2008 to 2015, Rolf was a member of the Steering Committee of the Global Internet Governance Academic Network and of the European Dialogue on Internet Governance. Since 2009, he has been a member of the High-level Panel of Advisers of the Global Alliance for Information and Communication Technologies and Development. He is an attorney-at-law, and his publication list is available at www.rwi.uzh.ch/lehreforschung/alphabetisch/weberr/person.html.

CHAPTER SEVEN:
THE PRIVATIZATION OF HUMAN RIGHTS: ILLUSIONS OF CONSENT, AUTOMATION AND NEUTRALITY

Emily Taylor

Business is collecting way more information than it should. We now have a stalker economy where customers become products.... Every time we — collectively — have had a choice between convenience and privacy/security, we've chosen convenience.

– Al Gore (2014)

INTRODUCTION

In the so-called "stalker" economy, as Al Gore (2014) has termed it, customers become products and business collects much more information than it should. He suggests that "we are rapidly approaching a gag point" at which consumers reject current norms and reassert their right to privacy. But in such a contested and controlled environment, what constitutes individual privacy, and how plausible would a reassertion of it be?

Many factors contribute to the current anxiety: the popularity of "free" services based on targeted advertising; decreasing technological costs and increasing capacity to process and store big data in novel ways; a tendency for surveillance to be enabled through "cosy, voluntary relationships" (Anderson 2015a) between governments and a handful of technical providers; the reach and power of a handful of (mostly US-based) companies with billions of users; and galloping technological innovation without a parallel track on ethics to guide decision makers — "not everything that technically can be done, should be done" (Omand 2015, 16).

There is a burgeoning field of scholarship encompassing the intersection of human rights with online life. It is not possible or desirable to attempt comprehensive coverage of this rich field in one short chapter. Beyond its scope are online state surveillance; the details of former National Security Agency (NSA) contractor Edward Snowden's revelations; the response of the technical community to alleged systematic weakening of encryption standards; the security risks arising from data breaches (such as the Sony hack, or the alleged targeting of Reuters by the Syrian army through a third-party advertiser). While the chapter briefly alludes to the tendencies of states to enlist the assistance of private companies in mass surveillance, or even copyright enforcement, this is not its primary focus.

The Snowden documents have sparked legal challenges in more than one country, many of which are still working their way through the system.[1] This chapter does not speculate on their likely outcomes.

CONTEXT

Human Rights: The Legal Matrix

The Universal Declaration of Human Rights (UDHR) was adopted in 1948 by the newly formed United Nations General Assembly, following "massive violations of fundamental rights immediately before and during World War II" (Gardbaum 2008, 750). The UDHR is founded on the concept that "the peace and security of mankind are dependent on mutual respect for the rights and freedoms of all" (Roosevelt 1948).

The UDHR was followed by, and provides the basis for, UN treaties and a patchwork of legally binding instruments and enforcement mechanisms at both the regional and the national level.[2] Recognition for fundamental rights is also enshrined in some national constitutions and domestic laws,[3] which broadly reflect the UDHR in form and substance. The UDHR has also influenced legal thinking and the harmonization of laws in Europe (Harris et al. 2014, 34).

Which Human Rights?

While this report focuses mainly on privacy and freedom of expression, all human rights are interdependent and indivisible (OHCHR n.d.). For example, poor privacy protection has an impact on freedom of expression, freedom of assembly and the peaceful enjoyment of property (Mendel et al. 2012). In *A Question of Trust: Report of the Investigatory Powers Review*, David Anderson (2015b, 25) uses the "catch-all word '*privacy*' as an imprecise but useful shorthand for such concepts." This chapter adopts the same approach.

While some rights — such as the right to life, not to be tortured, not to be held in slavery — are absolute, others are not; for example, states have a right of derogation from most human rights in times of public emergency. Other rights, such as privacy and freedom of expression, are subject to limitations. But the sources are clear that "any limitations of these rights should be exceptions to the norm, and be based on legitimate purposes. Likewise, limitations of any right need to be according to law, and be necessary and proportionate."[4]

[1] Note that the Court of Justice of the European Union judgment in *Schrems v Data Protection Commissioner* (6 October 2015) Case C-362/14 (http://curia.europa.eu/juris/documents.jsf?num=C-362/14) was issued after this chapter was written.

[2] For example, the International Covenant on Civil and Political Rights (Office of the United Nations High Commissioner for Human Rights [OHCHR] 1966). At the regional level, the European Convention on Human Rights (1950, 87 UNTS 103; ETS 5) has been described by David Harris et al. as having comparatively strong enforcement mechanisms through the European Court of Human Rights. Other mechanisms include the American Convention on Human Rights (1969, 1144 UNTS 123, in force 1978, 23 parties), and the African Charter on Human Rights and Peoples' Rights (1981, 1520 UNTS 143, ILM 59 (1981) in force 1986, 53 parties).

[3] For example, constitutions of Austria and Spain; the European Convention (which prevails over the national constitution in the Netherlands; the UK Human Rights Act 1998; Canadian Charter of Rights and Freedoms, Canada Act 1982.

[4] See OHCHR (1966, articles 4(1) and 4(2)).

Why Pay Attention to Private Companies?

States, not private actors, have legal obligations to respect, protect and fulfill human rights. That these obligations apply online, as well as offline, is well established — for example, in the influential Human Rights Committee's General Comment 34 (UN 2011b), resolutions of the Human Rights Council (UN 2012) and UN General Assembly,[5] and the NetMundial "Multistakeholder Statement" (NETmundial 2014). The reason for fixing states, rather than companies, with human rights obligations, is clear. The defining quality of a state is its "monopoly of the legitimate use of physical force within a given territory" (Weber 1946). Other than human rights standards, few checks and balances exist over the power of states to make or enforce laws in their territory. In contrast, companies (for the most part) have no coercive powers and are subject to national laws and regulations. This is why some human rights experts view a focus on private company actions as a distraction — the proper recourse, in their view, being for states to regulate or legislate to restrain market excesses.

Paying attention to private companies when evaluating risks to fundamental rights online is important for two reasons. First, both states and the private sector Internet platforms have shared interests in storing, processing and correlating big data, albeit for different reasons (security for the former; advertising revenues for the latter). At the same time, the market for web platforms is becoming more concentrated in the hands of a small number of companies. This alignment of powerful interests threatens an insidious erosion of fundamental rights and makes it unlikely that governments — who rely on private sector data and skills — would legislate or regulate to limit big data collection by Internet platform providers.

Second, the cross-border nature of the Internet makes it difficult to understand where responsibilities lie — with one state, many states, the private sector or a shifting combination of all of them? Moreover, the substantive issues are difficult — the scope of individuals' right to privacy; how to operate censorship of online content in an international, multicultural environment. It is tempting for states to park the issues in the "too difficult" pile and hope that someone else will take responsibility. There is evidence that the actions and inactions of states are placing private companies in the incongruous position of having to mediate users' fundamental rights.

Companies' Potential Impact — Offline and Online

Experience in the offline world demonstrates that real harms can occur to individuals through the actions of private companies. When Royal Dutch Shell exploited oil reserves in the Ogoniland, Nigeria, from the 1950s onwards "villagers lived with gas flares burning 24 hours a day (some for more than 30 years), and air pollution that produced acid rain and respiratory problems" (International Crisis Group 2008). Peaceful protests by villagers escalated into armed conflict and finally the execution of protesters, including Ken Saro Wiwa, in 1994. Eventually, Shell withdrew from Ogoniland (ibid.).

The Nigerian government did not actively "delegate" any rights to Shell and Shell did not actively assume any responsibility. The Ogoniland experience illustrates how large-scale human rights harms can arise through the passivity of states and their failure to take affirmative action.

In the virtual world, too, private company actions can have a direct impact on human lives. A classic example is the story of Beijing journalist Shi Tao. In 2004, he used his Yahoo email account, which had been set up under a pseudonym, to send an article to a pro-democracy website in New York. Yahoo complied with the Chinese authorities' request to reveal his identity. Shi Tao was arrested and sentenced to 10 years in prison. The Shi Tao case reveals how difficult it can be for multinationals to navigate between the legal requirements of host countries and accepted international standards: "It had taken two years of being pummelled by Congress, human rights groups, the media and shareholders before Yahoo finally shed its head-in-the-sand, lawyer-driven posture and actually took moral responsibility for what had happened" (MacKinnon 2012).

Guiding Principles on Business and Human Rights

Recognition of the impact that private actors, in particular multinationals, can have on human rights led to the development of guiding principles on business and human rights by the special representative of the UN Secretary-General on human rights and transnational corporations and other business enterprises, John Ruggie. The Ruggie Principles (UN 2011a) are a non-binding "protect, respect and remedy" framework for multinationals and were a breakthrough in a process that had been deadlocked for many years.

Despite endorsement by the UN Human Rights Council (in 2011), the Council of Europe (2014a) and adoption by Internet companies in "the Silicon Valley Standard" (Access n.d.), there is little evidence that the Ruggie Principles have had an impact on the culture or practices of "big tech." The Council of Europe's Commissioner on Human Rights observes that the Ruggie Principles do not deal with situations "where states make demands of companies that would lead companies into violations of international human rights law" and that "there is little

[5] For a good summary of UN resolutions recognizing human rights online, see Finnegan (n.d.).

other than moral rectitude or public relations pressure that can create incentives for online intermediaries to defend human rights" (Council of Europe 2014b).

Another example is the Global Network Initiative's work to advance human rights policies in information and communication technology companies; its membership includes Facebook, Google, LinkedIn and Yahoo (Global Network Initiative 2012).

BIG DATA AND PROFILING

Moore's law — after George E. Moore, the co-founder of Intel Corporation — states that computer capacity doubles approximately every two years.[6] With that increase naturally comes an exponential growth in data storage and a decrease in associated costs, as well as the hidden requirement, driven by business and national security concerns, to make sense of the information glut. The questions then arise: how is this done, who is doing it and with what justification?

The Internet has brought about a transformation in the quantity of digital data. Each day users send out 500 million tweets and upload 240 million photographs to Facebook; Google processes data that is "thousands of times the quantity of all printed material in the US Library of Congress" (Mayer-Schönberger and Cuker 2013, 8). While the quantity of non-digital data remains fairly static, digital data is doubling every three years. If all the digital data existing in 2013 were "placed on CD-ROMs and stacked up, they would stretch to the moon in five separate piles" (ibid., 9).

The Uses of Big Data

Big data — the ability to mine and make sense of enormous electronic files — is at the heart of the business models of today's Internet platforms. Big data allows the platforms to offer "free" services to users, financing their operations by enabling advertisers to target audiences with implausible precision. The author has personal experience of one small-scale example: a friend's start-up opera company in Oxford, England, was recently looking for soloists. Using Facebook's services, the company could specify that its advertisements be shown to conservatory-trained soprano and tenor soloists, aged between 25 and 30 years and based in the European Union. The advertising was cheap and the company was inundated with perfectly qualified candidates. The power of big data profiling is seen in the ability to match advertisers with potential targets with such precision.

On a much larger scale, big data can help improve public health by enabling authorities to respond to epidemics more rapidly. In much of the developed world, doctors are obliged to file with the authorities, within two weeks, every instance of a patient presenting with flu symptoms. Data mining of Google search queries relating to flu symptoms provides results that correlate almost perfectly with offline historic official data relating to flu epidemics, but with an important difference. Unlike the official data (which has at least a two-week lag), Google's data is available in real time.[7]

Big Data: Human Rights Risks

As ever, the technology has charged ahead of the policy analysis, with impacts already evident on privacy, freedom of expression and risks of discrimination. The corollary of the revolution in data analysis is that the same tools can be used for the purposes of repression.

The argument that "you have nothing to fear if you have nothing to hide" is enlisted by governments and companies to justify surveillance or big data processing. According to these reductive, "superficial incantations" (debunked by Solove 2007), privacy has only negative connotations, of protecting the scoundrel or the wrongdoer. Privacy is difficult to define, dependent on context, shifting and elusive, but it is a fundamental right, essential to individuals' autonomy, intimacy, dignity and ability to form an opinion.

Erosion of privacy by powerful actors (whether state or private) can cause insidious harm; as Evgeny Morozov (2013, 189) has said, "Given enough data and the right logarithms, all of us are bound to look suspicious." This idea echoes the famous epigram attributed to Cardinal Richelieu, "Qu'on me donne six lignes écrites de la main du plus honnête homme, j'y trouverai de quoi le faire pendre" (Only give me six lines written in the hand of the most honest man, and I will find something there to hang him by) (quoted in Stevenson 1964, 2259).

The human rights impact of compulsive data collection in an offline, paper-based context (although severe) is somewhat limited by the difficulty and cost of making any sense of it. For example, "by the early 1980s the Stasi[8] had about 85,000 regular employees and about a million and a half full- and part-time informers" (Clay Large 2001). Within a space of 40 years, the Stasi had amassed four miles of files, "more…than had been collected in the whole of Germany from the Middle Ages to the end of the Second World War" (Vaizey 2014).

Unlike the Stasi's unsiftable heaps of paper, digital data is searchable, indexed and correlated. It is usable, and used.

[6] See www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html.

[7] See www.google.org/flutrends/about/how.html.

[8] The Stasi (Ministerium für Staatssicherheit, abbrev.) was the state security service of the German Democratic Republic from 1950 to 1989.

Automated Tracking and Profiling

The ways in which private companies track online user behaviour, and their implications for privacy, are well explored in academic and industry literature (see, for example, Deibert 2013; MacKinnon 2012; Schneier 2015; Mayer-Schönberger and Cukier 2013). Cookies, social plug-ins and canvas fingerprinting are used throughout the Web. Their persistent popularity is partly due to the convenience they offer users. Session cookies allow browsers temporarily to store data entered into online forms before submission. Security cookies enable secure transactions upon which online banking and e-commerce depend. Social plug-ins enable users to share articles through Twitter, Facebook and other social networks. Single log-ins (for example, "Sign in with Facebook") enable users to interact with sites without creating hundreds of user profiles.

The trade-off for this convenience is "a shockingly extensive, robust, and profitable surveillance architecture" (Schneier 2015). Dozens of different companies' cookies are tracking users on popular sites; one site[9] installed 200 tracking cookies on a user's browser. DoubleClick (a Google company) enables targeted advertising to follow users as they browse. Single log-ins enable Facebook and other providers to track users — even those who are not logged into Facebook (ibid.).

Whereas the privacy implications of cookies have been well understood by policy makers for more than a decade, other tracking techniques might not be covered by the relevant legislation. Canvas fingerprinting and other tracking methods (such as evercookies and respawning) are widely used, even by the White House (Eckerslley and Opsahl 2014). These techniques uniquely identify users from their devices, are not transparent to users and are difficult to disable without significant loss of functionality.[10]

A whole industry of data intermediaries has emerged. Companies such as Datalogix and Acxiom collect consumer data "from numerous sources, largely without consumers' knowledge" (Federal Trade Commission 2014), sharing data with each other and creating profiles or categories of consumers, some of which make sensitive inferences about ethnicity, income levels or health-related conditions: "expectant parent," "diabetes interest," "cholesterol focus" (ibid.). Profiling and categorization can be beneficial for consumers: credit card fraud prevention relies on identifying breaks from a consumer's standard patterns of spending (Schneier 2015); targeted advertising has the potential to inform consumers about products or services they might enjoy. At the same time, profiling "can unwittingly lead to discrimination on grounds of race, gender, religion or nationality" (Council of Europe 2014b). It can also invade privacy: a father complained to the budget retailer Target that his teenage daughter had been sent coupons for baby products. It turned out that Target's "pregnancy prediction score" knew more than the girl's father did — his daughter was, indeed, pregnant (Duhigg 2012).

Data Anonymization: An Imperfect Form of Protection

So long as data is anonymized, what harms can arise to individuals? Unfortunately, it is straightforward to reverse anonymization, and metadata can be just as revealing as the underlying content, if not more so. Our relationships, what we do and correlations between different data sets provide the key to identify individuals from anonymized data. This fact has been demonstrated many times: when AOL released 20 million items of search data in 2006, researchers identified individuals by correlating different items in their search history, and, in 2008, 10 million movie rankings by 500,000 anonymized Netflix customers were de-anonymized by comparing rankings and time stamps with the public International Movie Database's rankings and time stamps (Schneier 2015). In an experiment carried out at Carnegie Mellon University in 2000, researchers were able to de-anonymize 1990 US census data for 87 percent of the population based on three data items: zip code, gender and date of birth (Sweeney 2000).

The scale of Internet data increases the fragility of anonymization as a protection. The artist Eric Fischer creates artwork based on publicly available data (Fischer 2010). He has produced world maps based on location data of 6.3 billion tweets (Fischer 2014). Fischer explains how he filters the data to eliminate duplicates: "Showing the same person tweeting many times within a few hundred feet also makes the map very splotchy, so I filter out those near-duplicates too" (ibid.). It makes for a much clearer map, but it is also a reminder that each data point can be traced back to an individual.

THE HUMAN RIGHTS RISKS OF BIG DATA COLLECTION

A Global Platform, with a Few Big Players

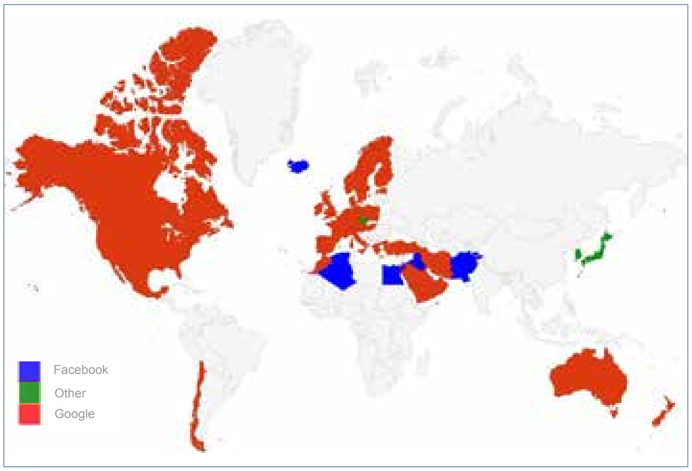
Competition between companies results in greater user choice and can provide a more diverse range of human rights protections. As markets become concentrated and people depend on a few essential platforms, the providers' rules have more impact on individuals' rights.

[9] Dictionary.com, 2010 (per Schneier 2015).

[10] For an explanation on how canvas fingerprinting works, see Acar et al. (2014); Mowery and Shacham (2012).

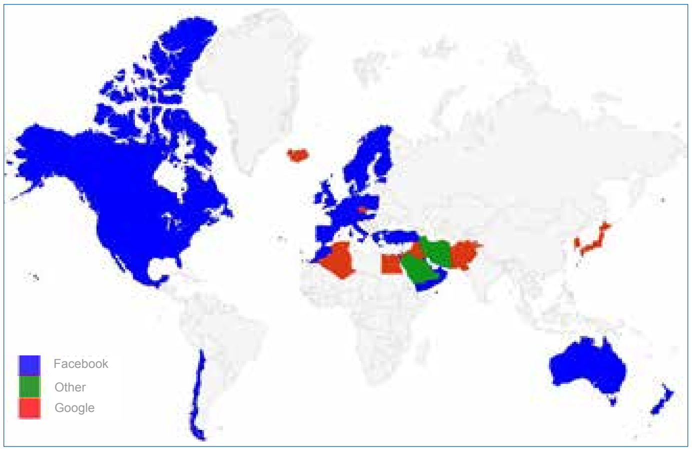
There might be a billion websites online[11] but the world's 2.9 billion Internet users spend their time on just a handful of platforms. For this study, the author undertook a comparison, based on Mark Graham and Stefano De Sabbata's "Age of Internet Empires" (2013), of the most popular sites across all 34 countries of the Organisation for Economic Co-operation and Development (OECD) and 17 countries from the Arab states and Central Asia.[12] The sample countries are geographically, economically and culturally diverse but the top websites in every country are the same[13] (see Figures 1, 2 and 3, and Table 1).

Figure 1: Most Popular Website by OECD Country and Arab States, 2015



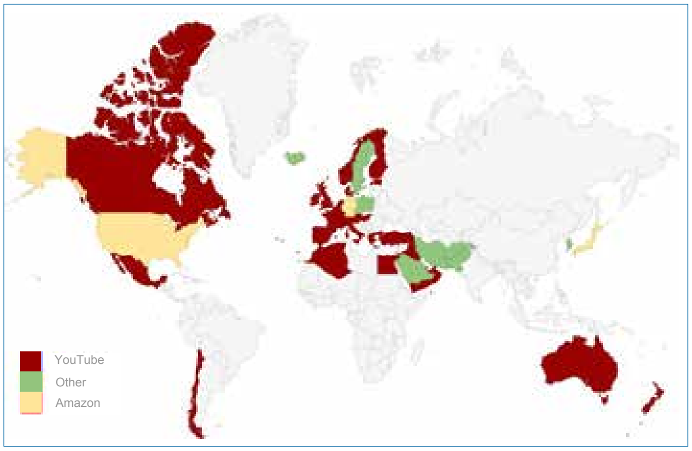
Source: Author; data from Alexa.com.

Figure 2: Second-most Popular Website by OECD Country and Arab States, 2015



Source: Author; data from Alexa.com.

Figure 3: Third-most Popular Website by OECD Country and Arab States, 2015



Source: Author; data from Alexa.com.

Table 1: Ranking of Top Sites Across OECD Countries, Arab States and Central Asia

	OECD	Arab States and Central Asia
Facebook.com	1	2
Google.com	2	1
YouTube.com	3	4
Google.local*	4	3
Wikipedia.org	5	7
Yahoo.com	6	5
Amazon (local)	7	–
Twitter.com	8	6

* "Google.local" means the local version of Google, for example, google.co.uk, google.ae, google.co.ma, google.dz. Across the Arab States and Central Asia sample, some countries also featured another country's local version of Google in their top 10 sites. Google sites occupy four of Algeria's top 10 sites: Google.dz (number 2), YouTube.com (number 3), google.com (number 4), google.fr (number 6) (see www.alexa.com/topsites/countries/DZ); google.com.sa is in Sudan's top 50 sites (number 22).

Source: Author. Ranking derived from mode score and number of instances in top 10, analyzing data from Alexa.com by country.

Google sites typically feature three times (google.com, google.local and YouTube) in the top 10 sites of every country sampled. The only exceptions are where particular countries have banned YouTube (Iran and Pakistan) or where there is no local service for Google (for example, Yemen and the United States, where google.com and YouTube.com feature but google.local does not). Other sites included in the 10 most popular sites across the entire sample are Wikipedia (42 countries), Yahoo.com (32 countries), Amazon (.com or .local, 26 countries), Twitter (20 countries).

[11] According to Internet Live Stats, 957,208,000 websites, compared with 23,500 in 1995 (www.internetlivestats.com/total-number-of-websites/).

[12] Analysis took place in May and June 2015, using Alexa.com. Countries sampled: Afghanistan, Algeria, Bahrain, Egypt, Iraq, Islamic Republic of Iran, Jordan, Kuwait, Morocco, Oman, Pakistan, Palestine, Qatar, Saudi Arabia, Turkey, United Arab Emirates and Yemen.

[13] Median rankings across the 51 countries sampled.

This is not to say that the top websites are homogeneous across all the countries studied or that a YouTube user in the Republic of Korea will consume the same material as a user in Egypt or the United States. For example, 37 of the 50 most popular sites in Turkey are local and do not appear on any other country's top 50. The significance of the concentration at the top of the lists lies in the long tail typically experienced in Internet traffic, meaning that the top handful of sites account for the lion's share of traffic. When Google experienced a short outage in 2013, total web traffic dropped by 40 percent (Geere 2013). When Facebook was down for an hour in January 2015, "social traffic"[14] dropped by 80 percent (Ratomski 2015).

Standard Terms Analysis: The Illusion of Consent

The impact that large Internet platforms can have on individuals' fundamental rights is well recognized, forming part of the "Ranking Digital Rights" project,[15] the Electronic Frontier Foundation's (EFF's) annual "Who Has Your Back?" report (2015b), and Take Back the Tech's (2014) scorecard on social media and violence against women.

The concentration of web traffic within a handful of private for-profit platforms lends significance to the terms of service and privacy policies, which set out the rules of the road, expected standards of user behaviour and the rights of platform providers to access, edit, delete and share user data.

This study analyzed the standard terms of agreement of Google (including YouTube), Facebook, Yahoo, Twitter and Amazon. Table 2 highlights terms that have an impact on the user's fundamental rights of privacy and freedom of expression.

The terms give the providers unfettered rights to access, delete and edit user data, including location data, and to share user data with unspecified third parties (for example, advertisers). None of the providers have clear deletion policies for user data or metadata, with the limited exception of Twitter.[16]

Metadata is information about a communication, distinct from the content of a communication. Metadata tells you *about* the communication — for example, where a user was when a photo was taken, what telephone number was called and the duration of a call.[17] It is sometimes called communications data or user data.

Retention of user data is also a controversial area. The Court of Justice of the European Union recently ruled that the Directive requiring providers to keep communications data on all users was incompatible with fundamental rights and therefore void.[18] The Directive covered mandatory retention of data by communications providers, the data to be produced at the request of law enforcement. However, the Internet platforms are thought to keep user data for their own purposes. Apart from Twitter, which clearly states that it will delete logging data after 18 months, none of the other platforms' terms explain how long they keep data.[19] The human rights impact of data retention on the ability to create profiles, or to confirm a future suspicion, has rightly been highlighted as a human rights risk by commentators as diverse as Cardinal Richelieu and Evgeny Morozov.

Facebook (2015b) offers users the ability to download their data. It is all there: every wall post, every photograph (content with a public quality); the text, time and date of each and every long-forgotten private chat (content with a transient or private quality). There is no expiry date — the data comprises the user's activity ever since he or she joined the platform. The download tool, according to Austrian student Max Schrems, only gives a "fraction of the data Facebook stores about you" (Schrems n.d.)." When Schrems made a data subject access request to Facebook in 2011, he received a CD containing more than 1,200 pages of data.[20]

Each "like" is also recorded. Research shows that automated analysis of "likes" alone can "accurately predict a range of highly sensitive personal attributes…. The model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between

[14] "Social traffic" is web traffic flowing from a social network to another site. In 2014, an estimated 30 percent of total web traffic was "social traffic"; see Wong (2015).

[15] The Ranking Digital Rights project's "Corporate Accountability Index" was launched in November 2015 (after this chapter was written). The project's 31 indicators include analysis of terms of service as part of a broader focus on the many aspects of policies and practice that can impact human rights; see MacKinnon (2015).

[16] Twitter commits, in its Terms of Service (https://twitter.com/tos?lang=en) and its privacy policy (https://twitter.com/privacy?lang=en), to deleting one aspect of user data — log-data — within 18 months.

[17] For more about metadata, see Guardian US Interactive Team (2013).

[18] The *Digital Rights Ireland* case, C293/12 and C594/12, of April 2014. See, in particular, paragraph 65: "It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary." http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=179241.

[19] Major Internet platform providers were approached for interviews for this study. Apart from Google, none responded.

[20] See Robinson (2015). Schrems later went on to win a preliminary point referred to the Court of Justice of the European Union, resulting in a declaration that the US Safe Harbor Decision is invalid (http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf).

Table 2: Analysis of Websites' Standard Terms of Agreement

	Google	Facebook	Yahoo	Amazon	Twitter	YouTube
Unfettered right of provider to access user data	√	√	√	√	√	√
Access to private chat, emails	√	√	√	√	√	√
Access to location, GPS, IP address, Wi-Fi points and cell towers without further user consent	√	√	√		√	√
Right to delete any user data without notice		√	√	√	√	√
Right to modify any user data without notice	√	√	√	√	√	√
Right to share user data with law enforcement	√	√	√	√	√	√
Right to share user data with advertisers without user opt-out	√	√	√		√	√
No clearly stated deletion policy for user data and metadata	√	√	√	√		√
California law exclusive jurisdiction	√	√			√	√
No right for EU citizens to elect for home court	√	√	√		√	√
Unfettered right for provider to unilaterally change terms	√	√	√	√	√	√
Community standards include right to take down material that is not illegal in provider's home country	√	√	√	√	√	√

Note: GPS = Global Positioning System; IP = Internet Protocol
Source: Author.

Democrat and Republican in 85% of cases" (Kosinski, Stillwell and Graepel 2013). Other attributes that analysis can correctly predict include religious views, use of addictive substances and parental separation (ibid.), all from transient "likes." Facebook remembers what humans forget.[21]

Of particular concern is the intrusion into communications that — in other contexts — have a quality of privacy, for example, email communications, private chat or messaging (Figure 4). For example, Google's terms of service affect more than 425 million Gmail users,[22] and provide no restriction on its ability to scan email content, which potentially includes:

- Communications between journalists and sources. The Court of Justice of the European Union has held that only "an overriding requirement in the public interest" can justify lifting confidentiality protections for such communications.[23] In 2014, Microsoft admitted reading a third-party blogger's Hotmail emails to identify the source of a leak relating to Windows 8 (Hern 2014). The company was able to use its control of the email platform to identify a journalist's source, access which did not require judicial permission for the company.
- Communications protected by attorney-client privilege. In the recent Belhadj case,[24] the UK government conceded that its interception of privileged communications had been unlawful. If interception of such communications by a state on the grounds of national security could not be justified, what possible justification could a private company have for such intrusion?
- Communications between medical practitioners and patients, discussing sensitive medical data. The ability to scan such communications in bulk potentially places Google at a commercial advantage as it diversifies into other business streams, such as automobile insurance (Winkler 2015). After a public outcry, the UK government was forced to put on hold a scheme to sell National Health Service records to insurance companies; private platform provider terms already incorporate the user's consent to share or sell such data, without any feedback to the user on what information has been shared and with whom.

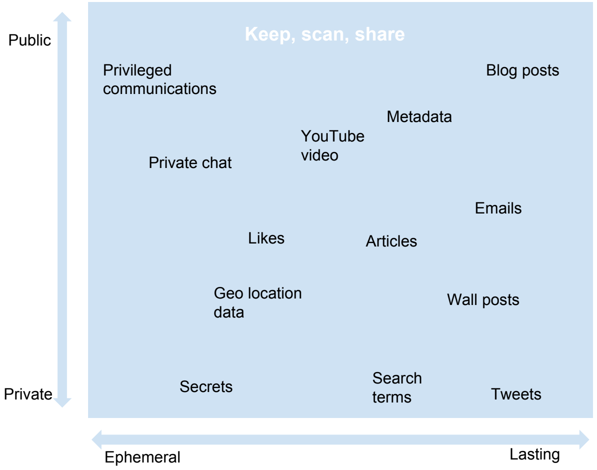
[21] For more on forgetting and remembering, see Mayer-Schönberger (2009).

[22] Yohana Desta's (2014) list of the 12 things dwarfed by Gmail's user base includes the population of the United States (318 million), Twitter users (214 million), Yahoo Mail users (273 million as of January 2014) and the number of household cats and dogs in the United States (83.3 million).

[23] *Goodwin v United Kingdom* [GC], no. 17488/90, paragraph 39, ECHR 1996-II.

[24] *Belhadj and others v Security Service and other,* IPT/13132-9/H, judgment of 29 April 2015. www.judiciary.gov.uk/judgments/investigatory-powers-tribunal-belhadj-and-others-v-security-service-and-others-judgment-and-determination/.

Figure 4: User Data on Proprietary Platforms Today



Source: Author.

Companies are not directly required to conform with international human rights standards but they are required to comply with national laws, which should be consistent with human rights conventions. There is clearly an implementation gap and a lack of guiding standards for today's leading Internet platforms. The standard terms — particularly those of the "free" platforms Google/YouTube, Facebook, Twitter and Yahoo — do not incorporate concepts such as necessity and proportionality, which moderate intrusions into rights of privacy under human rights law. There is little evidence of "reasonableness," a flexible safeguard that guides interpretation of consumer contract terms across the European Union according to unfair contract terms legislation.

A recent study (Van Alsenoy et al. 2015) on the legality of Facebook's terms cites concerns relating to data protection and unfair contract terms, which have a close nexus to human rights (privacy). The report describes updates to terms governing the provider's use of location data as "vague and broad." The report concluded that "there is no longer any mention of limiting the storage or use of location data to the time necessary to provide a service." Facebook has disputed the report's findings.

European consumer protection law limits or excludes certain contractual terms that might create "significant imbalances in the rights and obligations of consumers… and suppliers."[25] Examples relevant to human rights include terms "excluding or hindering the consumer's right to take legal action or exercise any other legal remedy,"[26] which invokes the human right to effective remedy through competent national tribunals (UN 1948, article 8). The standard terms of the popular websites — Google, Facebook, Twitter and Yahoo — contain exclusive law and jurisdiction clauses specifying California law and courts, with a few exceptions for EU citizens.[27] Only Amazon allows users to opt for their home court and laws.

Opting to resolve disputes exclusively in the supplier's home courts according to the supplier's national law provides a significant home field advantage to the supplier, not least by deterring consumers against bringing litigation in the first place (particularly where there are language barriers as well as geographic barriers). It takes an unusually determined and resilient individual, such as Max Schrems, to litigate against a multinational in a foreign jurisdiction.[28]

Amazon — and, to some extent, Twitter — present slightly more balanced terms. Amazon has different terms for various jurisdictions. Its terms in EU member states show awareness of not only privacy laws but also unfair contract terms legislation. So, Amazon customers have a right to elect their home jurisdiction for disputes, and Amazon gives its users a right to opt in to location data.[29] Twitter recently announced that it would automatically strip location metadata from uploaded photographs, and it also has a clear deletion policy for log-data (18 months), which the other providers do not.

[25] EU Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts OJ 1993 L95 p29, annex to Article 3(3) (j) and (q).

[26] Unfair Terms in Consumer Contracts OJ 1993, L95, Annex to Article 3(3)(q). For further discussion on this point, see Joined Cases C-240/98 to C-244/98 *Océano Grupo Editorial and Salvat Editores* [2000] ECR I4941, paragraph 24: "It follows that where a jurisdiction clause is included, without being individually negotiated, in a contract between a consumer and a seller or supplier within the meaning of the Directive and where it confers exclusive jurisdiction on a court in the territorial jurisdiction of which the seller or supplier has his principal place of business, it must be regarded as unfair within the meaning of Article 3 of the Directive in so far as it causes, contrary to the requirement of good faith, a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."

[27] Facebook refers EU citizens with a privacy dispute to the Irish data protection authority. EU citizens in dispute with Yahoo are referred to the laws and courts of Ireland.

[28] Despite the exclusive law and jurisdiction clause (15.1 of Facebook's terms of service), the data processor in the European Union is Facebook Ireland. Schrems brought his original complaint to the data protection authorities of Ireland. The case is being appealed to the Austrian Oberlandesgericht. See www.europe-v-facebook.org. The preliminary question was determined in October 2015 — see http://curia.europa.eu/juris/documents.jsf?num=C-362/14 — leading to the invalidation of the US Safe Harbor Decision.

[29] Studies related to organ donation (cited in Kahneman 2011) show the different effect of opt-in and opt-out. In countries operating an opt-out regime, the percentage of organ donors is 86 percent (in Sweden) and 100 percent (in Austria); in countries operating an opt-in regime, the percentage of organ donors is much lower: for example, four percent (in Denmark) and 12 percent (in Germany).

The UK's Independent Reviewer of Terrorism Legislation, David Anderson (2015a), said, in the context of government surveillance, "Each intrusive power must be shown to be necessary, clearly spelled out in law, limited in accordance with international human rights standards and subject to demanding and visible safeguards." Of course, it is governments' coercive powers that in part necessitate such safeguards. However, we have seen that highly sensitive information can be derived from users' interaction with popular platforms; we have seen that the platforms' standard terms provide few, if any "demanding and visible safeguards" governing use and retention of data. The reliance on — largely fictional — user consent provides an apparent legal justification for grossly intrusive powers. Processes for protecting individuals from harassment are opaque or non-existent, and the extent of data processing is loosely described by most (with the exception of Amazon). It is difficult to understand how the terms could be "in accordance with international human rights standards."

As Ronald Deibert (2013, para. 977) put it, "To repeat, the reason behind this data collection is advertising."

Alignment of State and Corporate Interests

States are attracted to big data honey pots, as the Snowden documents and the transparency reports by leading Internet companies make clear. The trend for governments seeking data from private sector networks is relentlessly upward: Facebook's first transparency report (January–June 2013) recorded 27,000 government requests for data relating to 39,000 user accounts from 71 countries. By December 2014 there had been a 28 percent increase in the number of user accounts affected, and a 22 percent increase in the number of states requesting data.[30]

The implications of states co-opting private company data for the purposes of counter-terrorism or surveillance is a substantial field of scholarship in itself. Their relevance to this study is the increasing reliance by states on private companies' skills — and data. The Snowden documents indicate that the US NSA and the UK's Government Communications Headquarters have paid "millions of dollars" to private companies, including popular Internet platforms and telephone companies, to cover the cost of compliance with requests for user data (MacAskill 2013; Ball, Harding and Garside 2013).

In *The Master Switch*, Tim Wu (2010, 298) predicted (pre-Snowden) that "should Facebook ever see a benefit in aligning itself with a government...clearly it could serve as one of the better spying tools ever created." Bruce Schneier (2015, 86) develops the thought (post-Snowden): "As long as these companies are already engaging in mass surveillance of their customers and users, it's easier for them to comply with government demands and share the wealth with the NSA. And as long as governments keep demanding access and refrain from legislating protections, it's easier to design systems to allow it. It's a powerful feedback loop: the business model supports the government effort, and the government effort justifies the business model."

The interdependence of private-sector business models with government surveillance poses a risk to the fundamental rights of individuals. Private sector actors become enmeshed within the law enforcement machinery, and the predictive powers of big data present democratic risks. Evgeny Morozov (2013, 189) says, "While Facebook might be more effective than the police in predicting crime, it cannot be allowed to take on these policing functions without also adhering to the same rules and regulations that spell out what the police can and cannot do in a democracy."

The risks arise through an imperceptible process of erosion as much as from any intent, as individuals become desensitized to sharing private things in public. This point leads to the question of how much individuals care about erosion of privacy. First, however, consider the ways in which the large web platforms have become drawn into moderating freedom of expression.

Platforms or Publishers?

Private platforms have a measure of choice in how they construct their standard contracts, but another key way in which popular providers have an impact on human rights has arisen almost by default. Despite sincere commitments to freedom of expression, and the legal incentives to maintain neutral intermediary status, popular web platform providers have become drawn into making decisions to remove or moderate content.

Google, Facebook and YouTube are perceived as platforms on which it is the users who generate content and communicate with one another. Unlike traditional publishers, the Internet providers do not screen content prior to publication. It would be futile to attempt traditional editorial control, such is the speed and scale at which new content is generated (300 hours of video are uploaded to YouTube every minute[31]). The providers are classified as intermediaries.

For more than a decade, concerns relating to images of child abuse and copyright infringement have provided the backdrop for ever-increasing liability of intermediaries

[30] See https://govtrequests.facebook.com/# for Facebook transparency reports.

[31] See www.youtube.com/yt/press/en-GB/statistics.html.

and the erosion of so-called "mere conduit" protections.[32] Private sector solutions, such as the Internet Watch Foundation in the United Kingdom and INHOPE, an international network of hotlines dealing with illegal content online, first established by Internet service providers, have been effective in combatting child abuse images. Another self-organized response is the EFF's Manila Principles (2015a), which set out guidance for laws and content restriction policies.

The difficulties of having private sector entities decide on complex issues such as the intersection between privacy and freedom of expression is illustrated with the example of Google's "Right to Be Forgotten" process.

Google and the Right to Be Forgotten

A Spanish individual brought a case against Google, complaining that news articles reporting on his historic (and resolved) financial difficulties remained at the top of Google search results on his name. The Court of Justice of the European Union[33] required Google to respect individuals' "right to be forgotten" by removing from search engine results links to historic web content. In response to the judgment, Google created a system to handle complaints.[34] To date, Google's system has handled more than 250,000 requests relating to 900,000 URLs (Williams 2015).

The systems, criteria and people involved in screening and making judgments to take down materials are not widely discussed. The quality of decisions under Google's Right to Be Forgotten process has been criticized. Even the privacy-orientated European Commission, after the process had been invoked to remove articles from the BBC business service, said that the ruling should not allow people to "Photoshop their lives" (quoted in Cooper 2014).

Part of the problem is that there is not enough information to determine how far Google's process fulfills basic rule of law requirements. The identity of those making the decisions is not revealed, nor are other due process considerations, such as whether decision-makers are subject to conflict-of-interest checks, which factors are taken into account and which are excluded in reaching decisions, and what rights of appeal exist for the parties. A small number of case studies are published, but reasoned decisions are not. An open letter to Google signed by 80 experts in technology and privacy law recently called for greater transparency in the process (Kiss 2015).

By contrast, ICANN's Uniform Domain-Name Dispute Resolution Policy (UDRP) has been in place since 1999 and has handled more than 40,000 cases — a single process to deal with domain disputes in any jurisdiction. It has provided a model for other domain name dispute mechanisms. Cases are filed online; there are written submissions, independent decision makers, published decisions; online materials offer guidance to practitioners and — in some variants of the UDRP, such as the .uk registry's (Nominet) Dispute Resolution Service and ICANN's Uniform Rapid Suspension process — the possibility of appeal. The UDRP and other domain name dispute mechanisms conform well to the rule of law.

It is true that the volume of content, and therefore of disputes, on the popular platforms is far greater than the volume of domain name disputes, but why should this be Google's problem to solve? Jonathan Zittrain (2014) responds, "If Google can process 70,000 requests, so can and should the data protection authorities." Zittrain reminds us that neither Google nor any other large platform provider has actively sought this work. They have had it thrust upon them by a mixture of inaction by states and ad hoc court decisions. But, having taken on the job, Google should be applying rule-of-law principles (open justice, conflict of interest, transparency, appeal). The example of the UDRP shows that a mixture of transparency, outsourcing decision making to others and automating the *process*, rather than the decision making, affords flexibility and allows dispute mechanisms to scale without sacrificing due process. According to Google, there are "no plans…to share individual decisions or aggregate them in a transparency-report-like format."[35]

CONTENT MODERATION: AN ILLUSION OF AUTOMATION

The popular web platforms, including Google, Facebook, Twitter and Yahoo, provide unprecedented opportunities for freedom of expression. Their intuitive tools have significantly lowered barriers to the publication of rich media — video, web pages and photographs — enabling individuals and small businesses to reach global audiences. Overwhelmingly, the impact on freedom of speech is positive. The US First Amendment ethos of the providers creates a permissive attitude toward all sorts of content.

But even in the most freewheeling environments, some types of content can cause real harm. Women who take a public position on social media are vulnerable to abuse — much of which is of a sexual or violent nature. In 2013, Caroline Criado Perez campaigned for the Bank of England to include at least one portrait of a celebrated woman on future bank notes. Perez suffered "life-changing

[32] "The burden of such policing is transferred to private intermediaries, such as search engines and social network platforms, through laws that widen liability for proscribed content from the original speaker to all intermediaries" (UN 2013).

[33] See *Google Spain v AEPD & Costeja-González* [2014] EUECJ C-131/12.

[34] Google's Right to be Forgotten form "Search removal request under data protection law in Europe," https://support.google.com/legal/contact/lr_eudpa?product=websearch.

[35] Google UK, email follow-up to interview for this chapter, March 31, 2015.

psychological effects from the abuse she received on Twitter," according to evidence given in the trial of two of the "trolls" (quoted in BBC News 2014).

These are not isolated incidents. One study concluded that 40 percent of Internet users have experienced online harassment, and that young women "experience certain types of harassment at disproportionately high levels," namely cyberstalking, online sexual harassment and physical threats (Duggan et al. 2014). Mary Beard (2014) places the phenomenon within the classical world's tradition of rhetorical speech and persuasion, in which "women who claim a public voice get treated as freakish androgynes." "Do those words matter?" she has asked. "Of course they do, because they underpin an idiom that acts to remove the authority, the force, even the humour from what women have to say" (ibid.).

All the large platform providers operate reactive notice-and-takedown systems. Users can flag "abuse" and content is then referred to human assessors for screening. It is difficult to obtain information about the number of complaints the providers handle or their processes. "Both Facebook and Twitter have in recent years grown more transparent about how they respond to government requests for content restriction….However...both companies are much more opaque about their internal decision-making processes around how and when their own rules are enforced" (MacKinnon et al. 2014, 152).

Sarah T. Roberts (2015) describes the tens of thousands of staff — often subcontracted through technical outsourcing companies such as Mechanical Turk or oDesk — who are removing abusive content, including hard core pornography and beheadings from users' newsfeeds: "Companies like Facebook and Twitter rely on an army of workers employed to soak up the worst of humanity in order to protect the rest of us. And there are legions of them…well over 100,000…about twice the total head count of Google and nearly 14 times that of Facebook."[36] According to Roberts, the workers "are really sophisticated. They are graduates of elite universities, providing a service so others don't have to."[37]

Facebook did not respond to requests for interviews for this chapter, but Google agreed to be interviewed and gave an indication of the challenges presented: "Our enforcement team, staffed around the world, reviews flagged videos 24 hours a day, 7 days a week. We review more than 100,000 flagged videos each day. In 2014, we removed 14 million videos from YouTube that violated our Community Guidelines."[38]

Arbitrating content issues involves complex value judgments, and — in an international context — requires sensitivity about cultural diversity and making difficult decisions about conflicts of law. Even cultures that are broadly aligned — such as the United States and Europe — still have marked differences in their approaches to controversial issues. For example:

- Reactions to the Right to Be Forgotten judgment on each side of the Atlantic have revealed differences in US and EU attitudes about privacy and freedom of expression: "In America the First Amendment's free-speech provision usually trumps privacy concerns" (*The Economist* 2014). Is the Right to Be Forgotten process a welcome redress for individuals who want to "grow and get beyond these incidents in their past" (Viktor Mayer-Schönberger, quoted in Toobin 2014) or a "terrible danger," only acceptable to "authoritarian dictators" (Wikipedia founder Jimmy Wales, quoted in Lomas 2014)?

- Determinations on copyright infringement can be complex and involve weighing whether any of the relevant exemptions apply (for example, fair use, limited terms, and the first sale doctrine),[39] yet Google complied with 97 percent of the requests it received between July and December 2011 to remove content that allegedly infringed copyright.[40] With such an implausibly high take-down rate, can one truly have confidence in the rigour of the assessment? There is simply not enough published information to be sure.

- Depictions of nudity seem more likely to offend sensibilities in the United States than in Europe. Following a campaign by "lactivists" (Burns 2007), Facebook's Community Standards now provide an express exception from its ban on nudity for pictures of breastfeeding[41]; Apple was criticized for "censoring" a "pixelated, low-res nudity — which is seen when you use a body scanning X-ray machine" in the app *Papers, Please* (Moore 2014).

- The EFF reports that "on Instagram, there have been several examples of larger women posing semi-clad,

[36] See also Chen (2014).

[37] Sarah T. Roberts, interview for this study, December 2014.

[38] Google UK, interview, March 31, 2015.

[39] For an exploration of copyright and the online environment, as well as the dangers of outsourcing evaluation of copyright infringement to machines, see Lessig (2006, 186 ff.).

[40] See www.google.com/transparencyreport/removals/copyright/faq/#compliance_rate. No data on compliance is provided beyond the six-month window July–December 2011.

[41] Within the section "Encouraging respectful behavior" on its Community Standards page, Facebook (2015a) states: "We also restrict some images of female breasts if they include the nipple, but we always allow photos of women actively engaged in breastfeeding." Other allowable nudity includes "showing breasts with post-mastectomy scarring...photographs of paintings, sculptures and other art." www.facebook.com/communitystandards/.

which have been taken down, or women with body hair, whereas pictures of thinner women are left up. Who is doing this? What is their demographic?"[42]

Human rights laws limit freedom of expression in certain situations, and companies are evolving self-regulatory processes to remove content that they feel would be covered by those limitations (or breach their acceptable-use policies). However, when cultural, political and legal differences become more pronounced, decisions on content moderation become more complex. For example:

- Scenes from war zones raise particular sensitivities. On the one hand, graphic depictions of individuals dying violently erode the individuals' inherent dignity (and rights to privacy) and can cause harm to vulnerable or young viewers. On the other hand, there is a clear public interest in sensitive reporting from war zones, subject to clear and consistent guidelines. Sarah T. Roberts interviews content moderators working for major web platforms, who contrast the handling of violent content from two separate conflict situations, Syria and Mexico:

  > The drug war that is going on in Mexico — a lot of the people who are on both sides were uploading videos of the war. Murders or hostages and interrogations. Stuff that we keep up for the war that is going on in Syria. The exact same content. I mean, it's for a different reason, but the content is the same. There are two sides, for all purposes it's the same content. But the argument they [the platform provider] gave me was that it wasn't newsworthy enough. The drug war….So it just feels like there is a double standard, and my understanding [from that] is that one person on the SecPol team is just passionate about the issues in the Middle East. (Quoted in Roberts 2015)

  The example illustrates a lack of consistency in approach.

- In Egypt, although homosexuality is not illegal, "homosexual acts in public are illegal and homosexuals have been convicted for breaching laws on public decency" (Gov.uk n.d.). Jillian York of the EFF recounts how a Cairo journalist allegedly colluded with police and reported on a gay men's club.[43] As a result, pictures were posted on a social network of identifiable people without their permission, in violation of the platform's terms. According to York, the pictures were a threat-to-life situation for the men tagged in the photographs: "Egyptian friends complained to the provider. The provider [based in Silicon Valley] did not take down the pictures even though it was in clear violation of their policy. It took a phone call from the EFF before the content was removed." Does this example illustrate a clash of cultures? Would an operative in the more permissive environment of California have an understanding of the different cultural norms applying to overt displays of homosexuality in Egypt? Should the process be so vulnerable to interventions by individuals or US organizations?

- Most people would welcome a decision by Twitter to remove videos of the beheading by the Islamic State of Iraq and al-Sham (ISIS) of the American journalist James Foley. Jay Kang (2014) of *The New Yorker* points out inconsistencies in Twitter policy decisions: "It's odd to think that a company that allows thousands of other gruesome videos, including other ISIS beheadings, would suddenly step in. Twitter, for example, allows creepshot accounts, in which men secretly take photos of women in public....Where, exactly is the enforcement line?" This decision on content moderation clearly would have been difficult for whoever had to make it. When such choices are made in private, without transparency, there is greater scope for inconsistency in approach, to the detriment of fundamental rights.

Making the right decision is difficult. In extreme cases, such as images of child abuse, the content is illegal in most jurisdictions — the content is appalling, but the decision to remove it is straightforward. For the most part, the line between what is acceptable and unacceptable is not so easy to draw; decisions are difficult and nuanced, and different cultures have varying levels of tolerance.

The Association for Progressive Communications criticizes Facebook, YouTube and Twitter for their "reluctance to engage directly with technology-related violence against women, until it becomes a public relations issue" (Nyst 2014). The reluctance in part stems from the awkward transition from being neutral platforms to being publishers, a transition that the platforms have not looked for and have yet to come to terms with. On the one hand, they risk adverse publicity or alienation of their user base if they fail to act; on the other, they might erode their legal protections as intermediaries (thereby threatening their business model) if they take responsibility for user-created content on their platforms. Conflicting statements highlight the duality: Twitter's former general counsel once described the company as "the free speech wing of the free speech party" (quoted in Ball 2014). More recently, according to a leaked internal memo, Twitter's then CEO Dick Costolo said, "We suck at dealing with abuse and trolls," and promised to "start kicking these people off right and left

[42] Jillian York, of EFF, interview for this study, December 2014.

[43] Ibid.

and making sure that when they issue their ridiculous attacks, nobody hears them" (Tiku and Newton 2015).

While there is a sense that "something should be done" by *somebody*, it is less clear *what* should be done, *by whom* and *according to what criteria*.

In the absence of *somebody* coming forward to moderate online content according to the public interest and rule of law, Internet platforms have had to step into the vacuum left by public authorities. Zittrain (2014) points up the "incongruity of having Google — or any private party, for that matter — as a decision maker about rights."

To whom will content moderators be accountable? What redress mechanisms will exist for those who believe the wrong decision has been made? Difficult decisions relating to content are not confined to the Internet. The British Board of Film Classification (BBFC) publishes guidelines, conducts research on changing social values and provides brief explanations for each film classification choice. "We have a simple approach. Listen to the public, and tell the public what we're doing," says the BBFC's President Patrick Swaffer.[44]

The Internet platform providers' lack of both transparency about their processes and public commitment to human rights standards other than freedom of speech help to perpetuate what Sarah T. Roberts terms a "collective hallucination that these things are done by a machine rather than people, perpetuating a myth of the Internet as a value-free information exchange with no costs."[45] There are few public discussions about the rules applied by providers or about their workers' conditions and the psychological impact on those workers of long-term exposure to harmful content.

THE ILLUSION OF NEUTRALITY AND THE NEED FOR ETHICS

On November 2, 2010, Congressional elections were held in the United States. Interested in discovering the extent to which voter behaviour is socially influenced, researchers, with Facebook's cooperation, selected 61 million US users at random and reviewed the effectiveness of different messages posted on their timelines. Some were shown a simple link to the local polling information. For others, a clickable "I voted" button was added to the link. For others, six small thumbnail pictures of friends were also added to the link and button. A control group was shown nothing at all. The result: turnout increased by 60,000 directly, and through social contagion, up to 280,000 voters. Voters were most likely to vote if they saw that their friends had done so (Bond et al. 2012).

In January 2012, in a week-long experiment, researchers, with Facebook's cooperation, exposed 690,000 randomly selected users to different types of emotional content. One group was exposed to friends' positive emotional content; the other to friends' negative emotional content. The experiment showed that emotions are contagious (Kramer, Guillory and Hancock 2014).

No information is given as to how the users in each experiment were selected, whether they gave consent and whether they were screened for vulnerabilities (for example, depression or suicidal thoughts). Offline psychological experiments are subject to stringent ethics, yet no information was provided in the Facebook studies as to how they satisfied ethical requirements.

The experiments highlight concerns about the power of large platform providers to influence human behaviour. The platforms are not as neutral as they seem. Content that users take for granted as being neutral — search results, friends' updates — are personalized. The algorithms of the leading providers are secret, so users do not understand why Facebook thinks a user prefers one friend over another. Search engines "restrict or modify search results for many…commercial and self-regulatory reasons, including user personalization and enforcement of companies' own rules about what content is acceptable to appear on their services" (MacKinnon et al. 2014, 11-12) but it is not clear how those decisions are made.

Of course, it is not good business to betray the trust of your users, and the companies — surprised by the backlash last time (see, for example, D'Onfro 2014) — might decide to do things differently in future. But the decision will be theirs alone. The experiments were pre-consented to in their terms and conditions.

Today's major providers have not only the platforms with which to experiment on their unwitting users but also privileged access to sensitive data. Some scholars have called for popular online service providers to be designated "information fiduciaries," thereby creating obligations — similar to those of lawyers or doctors — not to use the information entrusted to them for outside interests (Balkin 2014).

ANALYSIS: PUBLIC ATTITUDES ABOUT PRIVACY

What does the Internet-using public think about Internet providers' intrusion into their privacy or curtailment of their freedom of expression? Does the public care? Do people understand what is happening to their data? Even if they do know, and do care, what can they do about it,

[44] Patrick Swaffer, interview, January 6, 2015. The BBFC's vision statement is to "respond to and reflect changing social attitudes towards media content through proactive public consultations and research" (BBFC 2014) .

[45] Sarah T. Roberts, interview, December 18, 2014.

short of opting out of online life (and thereby much of offline life, too)?

Is Human Nature Changing?

One possibility is that the Internet has changed people, or at least their attitudes to what should be private or public. Noam Chomsky refers to "the exhibitionist character of the internet," noting that "younger people are less offended by this than the older generation" (quoted in Harvey 2013). While Chomsky is correct in saying that companies seem to be conspiring with young people — and not only young people — to parade their private lives in public, concluding that human nature has changed does not follow — at least not without reviewing some other possibilities.

It is more likely that the Internet platforms are not quite attuned to the subtleties of human interactions. Facebook's CEO Mark Zuckerberg (quoted in Kirkpatrick 2010, 199) stated, "You have one identity. The days of you having a different image for your work friends or co-workers...are probably coming to an end pretty quickly." Schneier (2015, chap. 10) takes Zuckerberg to task for his "remarkable naiveté": "We are not the same to everyone we know and meet. We act differently when we're with our families, our friends, our work colleagues and so on….It's not necessarily that we're lying, although sometimes we do; it's that we reveal different facets of ourselves to different people. This is something innately human. Privacy is what allows us to act appropriately in whatever setting we find ourselves."

It is also difficult for people to conceptualize that there is a dual audience for their Internet content: their friends on the one hand, the platform provider and those it chooses to share with on the other. "Viewing a YouTube video seems like a private action. Searching for medical information about a recently diagnosed condition in the privacy of one's living room seems like a private action" (DeNardis 2014). Sharing with one's friends within a social network feels like a social action with known recipients. The online platforms support this illusion, giving users an array of intuitive tools to control their privacy settings, even at the level of individual updates. So, users can choose whether their content goes to friends, friends-of-friends (on average 31,000 others[46]) or is public. Choices might depend on which facets of ourselves a particular post reveals. But certain choices are off limits. The standard terms analysis above shows how the world's most popular platform providers give themselves and third-party advertisers unfettered access to user content, including the ability to delete, edit and share that content with any third party. Individuals have no user tools or any chance to opt out to limit what the platform can do with their data.

Does the Public Trust Companies' Data Handling?

Survey evidence suggests that while there might be some tolerance, even support, for government gaining access to data in certain circumstances,[47] attitudes harden when it comes to private companies. "Public surveys have shown particularly low levels of trust in relation to phone companies and ISPs in dealing with data. A recent survey showed only between 4% and 7% had high levels of trust in such companies to use their data appropriately. They also show a general lack of confidence in the security of everyday channels, social media being viewed as the least secure" (as cited by Anderson 2015b, 34). A study of 23,000 Internet users from across the world for the Global Commission on Internet Governance indicates that 74 percent of users are concerned about companies monitoring online activities and then selling that information.[48] According to the Pew Research Center, 93 percent of adults say that being in control of *who* can get information about them is important; 90 percent say that controlling *what* information is collected about them is important (Madden and Rainie 2015).

So, either there is a gap between what people are saying in their survey responses and what they are doing online, or something else is at play.

Does the Public Understand the Deal?

It is known that few people read or have the legal training to understand privacy policies. One study estimates that "if all American Internet users were to annually read the online privacy policies word-for-word each time they visited a new site, the nation would spend about 54 billion hours reading privacy policies" (McDonald and Cranor 2008, 563). Ian Brown and Christopher T. Marsden (2013, 54) comment that "there is increasing evidence from behavioural economics that a 'consent' model has significant failings…. Privacy-related decisions are heavily context specific, dependent, for example on how much a user is thinking about privacy at the time, along with his or her trust in the other party and often-inaccurate assumptions about how data will be used."

[46] According to Keith Hampton et al. (2012): "At two degrees of separation (friends-of-friends), Facebook users in our sample can on average reach 159,569 other Facebook users. However, the relatively small number of users with very large friends lists, who also tended to have lists that are less interconnected, overstates the reach of the typical Facebook user. In our sample, the maximum reach was 7,821,772 other Facebook users. The median user (the middle user from our sample) can reach 31,170 people through their friends-of-friends."

[47] See, for example, TNS-BMRB Polling January 23–27, 2014: 71 percent of respondents "prioritise reducing the threat posed by terrorists and serious criminals even if this erodes people's right to privacy."

[48] "CIGI-Ipsos Global Survey on Internet Security and Trust." November 24, 2014. www.cigionline.org/internet-survey.

My Way or the Information Superhighway

It is evident that the standard terms of today's leading providers provide no mechanisms for users to opt out of having their data shared with third parties; nor are there paid alternatives (without advertising) for most services.

Google currently has more than 90 percent of the European search market. Facebook has 1.3 billion users. The existing all-or-nothing deal risks excluding people from what have become intrinsic parts of daily life.

Providers also exhibit a homogenous approach to data: communications that are private in nature seem to be handled in the same way as communications that are more public; information that, in offline life, humans are programmed to forget — such as the content of most chat conversations, or where we were at a particular date and time — is stored indefinitely, apparently in the same way as more permanent content, for example, YouTube videos.

CONCLUSIONS AND RECOMMENDATIONS

Human rights laws apply to states, not to private companies, reflecting the different realities for governments versus private entities. Governments can pass whatever legislation they wish, subject only to human rights standards. Meanwhile, private companies are subject to a plethora of laws. When a successful company starts to operate on a multinational basis, the regulatory and legal landscape becomes complex. Multinationals often have to contend with conflicting laws, regulations and norms across the international field of their operations.

However, multinationals can have an impact on human rights and the Ruggie Principles of "protect, respect and remedy" offer a framework to help companies understand and respond to their responsibilities. At the same time, states must be vigilant in monitoring the impact private actors have on human rights, redressing imbalances where necessary. While the impact of companies in the offline world can be direct and obvious, online companies' acts or omissions can also lead to direct harm. A more insidious harm is that the erosion of fundamental rights becomes normalized.

The early, open phase of the Internet's development has given way to a highly concentrated market for web content provision. Today's popular Internet platforms have lowered the barriers to freedom of expression and access to knowledge. Attitudes about sharing what used to be considered private might be changing. At the same time, the complexity of today's online data market and the unpredictable afterlife of our online communications when correlated with other big data sources make traditional consent models (which underpin the business models of the big platforms) ineffective. How can a provider frame terms that give consent for uses of data that have not yet been thought of, except by giving themselves the widest possible scope?

While people might be fairly relaxed about the reprocessing of data that is public in nature, such as tweets, blogs or YouTube videos, the picture is less clear with communications that appear private and transient — such as chat or location data. Nevertheless, these data are being scanned, processed and sold in just the same way.

States are seeking ways to reduce the cost and increase the effectiveness of surveillance by using online data — and states have to rely on the skills, resources and data of private companies. Commentators have noted the "powerful feedback loop" in which the ever-more intrusive data collection and processing by the private sector support the desire of governments to process such data for national security purposes. The current situation aligns the interests of two powerful actors: states and multinationals. This alignment poses democratic risks, as well as making regulatory interventions to limit such data collection unlikely.

What Needs to Happen?

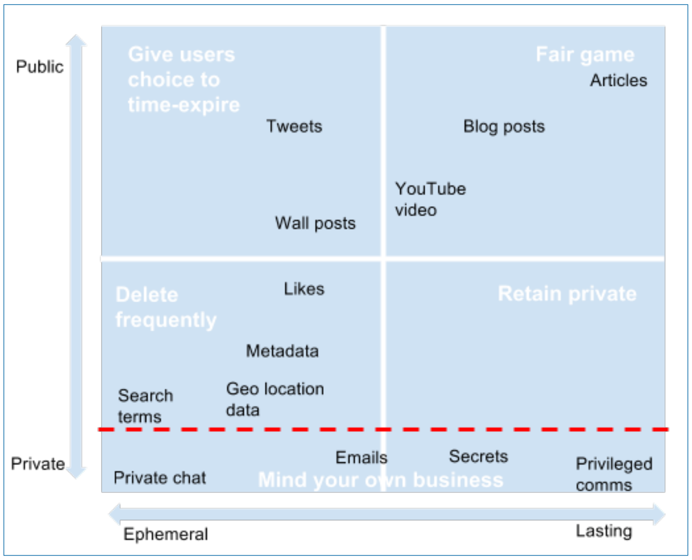
States need to review and, if necessary, reassert their human rights obligations in the online environment, rather than rely on ad hoc mediation of these rights by private companies.

Companies need to differentiate between private and public communications in their terms, and to limit their intrusion into private communications to what is necessary, proportionate and pursuant to a legitimate aim. Rather than treating all types of user data as homogenous (and fair game), policy makers need to recognize that not all data is created equal and that certain types of communications, such as legally privileged, intimate, confidential information and emails, need to be kept away from prying eyes — even of the platform providers. Meanwhile, other types of communications that are inherently ephemeral in nature should automatically expire and be deleted from the platform providers' systems (see Figure 5 for a possible model).

Particular care is required when dealing with data of young and vulnerable users. Google is piloting a service, YouTube Kids, in the United States, which limits advertising (della Cava 2014),[49] but it is not clear how far the tracking and mining of user behaviour and data are also limited.

[49] See "Advertising on YouTube Kids" about the restrictions on advertising: https://support.google.com/youtube/answer/6168681.

Figure 5: User Data on Proprietary Platforms — An Evolution?



Source: Author.

In the first instance, companies are best placed to make such distinctions through self-regulatory mechanisms, as these are likely to be more practical across national borders than a hodgepodge of national regulation. Platform providers might extend tools for users with which to make privacy choices such as expiry dates or preferences, which would also include limits of intrusion for the platform providers themselves.

There needs to be a collective effort for platform providers to arrive at deletion policies for data that is ephemeral in nature (such as chat messages) or which could give rise to human rights risks (such as historic location data).

Many users are not concerned about what happens to their data, or accept it as part of the bargain in using a free platform. Others do care, and they should be offered some alternative — such as a limited opt-out or an option of a paid subscription — other than exclusion from services that are now becoming embedded in daily life.

Recent judgments from the Court of Justice of the European Union reasserting fundamental rights in the online environment stand in stark contrast to the lack of leadership shown by states, which appear fearful of ensuring that powerful multinational platform providers are fulfilling the states' human rights obligations.

Other actors need to assist multinationals to arrive at realistic and robust processes for content moderation that comply with international human rights standards. Processes need to be more transparent; the decision makers and their freedom from conflicts of interest need to be clearly identified; and appeals mechanisms need to be introduced.

Pleading that the Internet is always different — digital exceptionalism — can be misleading. The scale of the Internet's data generation and management is enormous and the international nature of its services lends complexity. But these issues — and their potential solutions — are not unique to the digital world. An abundance of hard-learned lessons from other sectors, such as film classification, or even the extraction industries, could provide insight into the task of navigating the issues and responding to changing social attitudes. It should be possible to evolve independent monitoring bodies using the combined efforts of private, voluntary and state vehicles.[50] Most importantly, this work must be done transparently, effectively and responsibly.

Acknowledgements

I would like to thank the many people who have helped and guided me with this project: The team at CIGI, Eric Jardine, Samantha Bradshaw, Lynn Schellenberg and Fen Hampson, and at Chatham House, Caroline Baylon, Hannah Bryce and Patricia Lewis. Members of the Global Commission on Internet Governance, especially the incomparable Laura DeNardis, who provided invaluable input on early ideas for this chapter. Professor Ian Brown of the Oxford Internet Institute, for suggestions about sources and reading materials. Sarah Roberts of Western University, London, Canada, for background on content moderation practices and for generously sharing extracts from her research. Jillian York of EFF (always an inspiration), for real-life examples from the Middle East. Patrick Swaffer of the BBFC, for patiently explaining approaches to content moderation in the offline environment. Thanks also go to: Brittany Smith of Google, the only representative of the big online platforms who agreed to be interviewed (or even to answer emails from me). Rebecca MacKinnon, Jean-Jacques Sahel and many others who have helped me. Will Eaves, who gave editorial advice on early drafts, and my family — Lucien, Alice and Patrick — who put up with a very distracted wife and mother for too many months. Lastly, my thanks to the late Caspar Bowden, whose work I have long admired, who spoke with me at length for this project, and to whom this chapter is respectfully dedicated.

[50] For example, the BBFC is a private, non-profit company, its president appointed by the Secretary of State; CARA (Classification and Rating Administration), the US system for film classification, is voluntary; the Swedish Media Council has taken on a role originally done by the police.

WORKS CITED

Acar, Gunes, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan and Claudia Diz. 2014. “The Web Never Forgets: Persistent Tracking Mechanisms in the Wild.” Session at the 21st ACM Conference on Computer and Communications Security, Scottsdale, AZ, November 5.

Access. n.d. “Silicon Valley Standard.” https://s3.amazonaws.com/access.3cdn.net/d9369de5fc7d7dc661_k3m6i2tbd.pdf.

Alexa.com. 2015. “The Top 500 sites in each country or territory.” www.alexa.com/topsites/countries.

Anderson, David. 2015a. “Statement by the Independent Reviewer of Terrorism Legislation on Publication of the Report of the Investigatory Powers Review (‘A Question of Trust’).” Press release, June 11. https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/#more-2364.

———. 2015b. *A Question of Trust: Report of the Investigatory Powers Review*. H M Government, June 15. https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

Balkin, J. 2014. “Information Fiduciaries in the Digital Age.” *Balkanization* (blog), March 5. http://balkin.blogspot.co.uk/2014/03/information-fiduciaries-in-digital-age.html.

Ball, James. 2014. “Twitter: from free speech champion to selective censor?” *The Guardian*, August 21. www.theguardian.com/technology/2014/aug/21/twitter-free-speech-champion-selective-censor.

Ball, James, Luke Harding and Juliette Garside. 2013. “BT and Vodafone among telecoms companies passing details to GCHQ.” *The Guardian*, August 2. www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.

BBC News. 2014. “Two guilty over abusive tweets to Caroline Criado-Perez.” BBC.com, January 7. www.bbc.co.uk/news/uk-25641941.

BBFC. 2014. *BBFC Guidelines 2014 Research Report*. www.bbfc.co.uk/sites/default/files/attachments/2014%20Guidelines%20Research.pdf.

Beard, Mary. 2014. “The Public Voice of Women.” *London Review of Books* 36 (6): 11–14. www.lrb.co.uk/v36/n06/mary-beard/the-public-voice-of-women.

Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle and James H. Fowler. 2012. “A 61-million-person experiment in social influence and political mobilization.” *Nature* 489: 295–98. doi:10.1038/nature11421.

Brown, Ian and Christopher T. Marsden. 2013. *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge MA: MIT Press.

Burns, Matt. 2007. “Breast Isn’t Best on Facebook.” *TechCrunch*, September 7. http://techcrunch.com/2007/09/07/breast-isnt-best-on-facebook/.

Chen, Adrien. 2014. “The laborers who keep dick pics and beheadings out of your Facebook feed.” *Wired*, October 23. www.wired.com/2014/10/content-moderation/.

Clay Large, David. 2001. *Berlin: A Modern History*. London, England: Allen Lane.

Cooper, Paul. 2014. “Embarrassed EC: Right to be forgotten not a right to ‘Photoshop your life.’” IT Pro Portal, July 4. www.itproportal.com/2014/07/04/embarrassed-ec-says-right-be-forgotten-not-designed-photoshop-your-life-google-eu-robert-peston-bbc/#ixzz3uyQls6xv.

Council of Europe. 2014a. *Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users* (adopted by the Committee of Ministers on April 16, 2014, at the 1197th meeting of the Ministers’ Deputies). https://wcd.coe.int/ViewDoc.jsp?id=2184807.

———. 2014b. “The Rule of Law on the Internet and in the Wider Digital World.” Issue Paper by the Council of Europe Commissioner for Human Rights. www.coe.int/t/dghl/standardsetting/media/cdmsi/Rule_of_Law_Internet_Digital_World.pdf.

Deibert, Ronald. 2013. *Black Code: Inside the Battle for Cyberspace*. Toronto, ON: McClelland & Stewart.

della Cava, Marco. 2014. “Google to revamp its products with 12-and-younger focus.” *USA Today*, December 3. www.usatoday.com/story/tech/2014/12/03/google-products-revamped-for-under-13-crowd/19803447/.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Desta, Yohana. 2014. “12 Things Gmail’s User Base Dwarfs in Size.” Mashable.com, April 1. http://mashable.com/2014/04/01/gmail-user-base-size/.

D'Onfro, Jillian. 2014. "Facebook Apologizes for Its Huge Psychological Experiment on Users and Explains How It Will Do Future Research Differently." *Business Insider*, October 2. www.businessinsider.com/facebook-cto-mike-schroepfer-apologizes-for-facebook-experiment-2014-10?IR=T.

Duggan, Maeve, Lee Rainie, Aaron Smith, Cary Funk, Amanda Lenhart and Mary Madden. 2014. "Online Harassment." Pew Research Center, October. www.pewinternet.org/files/2014/10/PI_OnlineHarassment_102214_pdf1.pdf.

Duhigg, Charles. 2012. "How Companies Learn Your Secrets." *The New York Times Magazine*, February 16. www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=2&hp.

Eckersley, Peter and Kurt Opsahl. 2014. "White House Website Includes Unique Non-Cookie Tracker, Conflicts with Privacy Policy." EFF, July 22. www.eff.org/deeplinks/2014/07/white-house-website-includes-unique-non-cookie-tracker-despite-privacy-policy.

EFF. 2015a. "Manila Principles on Intermediary Liability: Best Practices Guidelines for Limited Intermediary Liability for Content to Promote Freedom of Expression and Innovation." Version 1.0, March 24. www.eff.org/files/2015/10/31/manila_principles_1.0.pdf.

———. 2015b. "Who Has Your Back? 2015: Protecting Your Data from Government Requests." www.eff.org/who-has-your-back-government-data-requests-2015#download.

Facebook. 2015a. Community Standards. www.facebook.com/communitystandards/.

———. 2015b. "Help Center. Manage Your Account: Downloading Your Info." www.facebook.com/help/131112897028467/.

Federal Trade Commission. 2014. *Data Brokers: A Call for Transparency*. May 2014. www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Finnegan, Shawna. n.d. "United Nations Resolutions Recognizing Human Rights Online." Association for Progressive Communication blog. www.apc.org/en/blog/united-nations-resolutions-recognising-human-rights.

Fischer, Eric. 2010. "Locals and Tourists." www.flickr.com/photos/walkingsf/sets/72157624209158632/with/4671589629/.

———. 2014. "Making the most detailed tweet map ever." Mapbox blog, December 3. www.mapbox.com/blog/twitter-map-every-tweet/.

Gardbaum, Stephen. 2008. "Human Rights as International Constitutional Rights." *European Journal of International Law* 19 (4): 749–68.

Geere, Duncan. 2013. "Google goes down for a few minutes, web traffic drops 40 percent." *Wired.co.uk*, August 17. www.wired.co.uk/news/archive/2013-08/17/googledip.

Global Network Initiative. 2012. "Participants." http://globalnetworkinitiative.org/participants/index.php?qt-gni_participants=1#qt-gni_participants.

Gore, Al. 2014. "A fireside chat with Al Gore," 2014 Southland Conference: Technology + Southern Culture, Nashville, TN, June 9–12.

Gov.uk. n.d. "Egypt Travel Advice." Updated November 18, 2015, still current at December 17, 2015. www.gov.uk/foreign-travel-advice/egypt/local-laws-and-customs.

Graham, Mark and Stefano De Sabbata. 2013. "Age of Internet Empires." Internet Geographies, Oxford Internet Institute. geography.ii.ox.ac.uk.

Guardian US Interactive Team. 2013. "A Guardian Guide to Your Metadata." *The Guardian*, June 12. www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000.

Hampton, Keith, Lauren Sessions Goulet, Cameron Marlow and Lee Rainie. 2012. "Why most Facebook users get more than they give." Pew Research Center, February 3. www.pewinternet.org/2012/02/03/why-most-facebook-users-get-more-than-they-give/.

Harris, David, Michael O'Boyle, Edward Bates and Carla Buckley, eds. 2014. *Law of the European Convention on Human Rights*. 3rd ed. Oxford, England: Oxford University Press.

Harvey, Fiona. 2013. "NSA surveillance is an attack on American citizens, says Noam Chomsky." *The Guardian*, June 19. www.theguardian.com/world/2013/jun/19/nsa-surveillance-attack-american-citizens-noam-chomsky.

Hern, Alex. 2014. "Former Microsoft employee arrested over Windows 8 leaks." *The Guardian*, March 20. www.theguardian.com/technology/2014/mar/20/former-microsoft-employee-arrested-over-windows-8-leaks?view=desktop.

International Crisis Group. 2008. "Nigeria: Ogoni Land after Shell." Crisis Group Africa Briefing No. 54. International Crisis Group, September 18. www.crisisgroup.org/~/media/Files/africa/west-africa/nigeria/B054%20Nigeria%20Ogoni%20Land%20after%20Shell.pdf.

Kahneman, Daniel. 2011. *Thinking Fast and Slow.* New York, NY: Farrar, Straus and Giroux.

Kang, Jay Caspian. 2014. "Should Twitter have taken down the James Foley video?" *The New Yorker*, August 21. www.newyorker.com/news/news-desk/twitter-taken-james-foley-video.

Kirkpatrick, David. 2010. *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. New York, NY: Simon and Schuster.

Kiss, Jemima. 2015. "Dear Google: open letter from 80 academics on the 'right to be forgotten.'" *The Guardian*, May 14. www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten.

Kosinski, Michal, David Stillwell and Thor Graepel. 2013. "Private traits and attributes are predictable from digital records of human behavior." *Proceedings of the National Academy of Sciences of the United States of America* 110 (15): 5802–5. www.pnas.org/content/110/15/5802.full.

Kramer, A. D. I., Jamie E. Guillory and Jeffrey T. Hancock. 2014. "Experimental evidence of massive-scale emotional contagion through social networks." *Proceedings of the National Academy of Sciences of the United States of America* 111 (29): 8788–90.

Lessig, Lawrence. 2006. *Code Version 2.0.* New York, NY: Perseus Books.

Lomas, Natasha. 2014. "Jimmy Wales Blasts Europe's 'Right to Be Forgotten' Ruling as a 'Terrible Danger.'" *TechCrunch*, June 7. http://techcrunch.com/2014/06/07/wales-on-right-to-be-forgotten/.

MacAskill, Ewen. 2013. "NSA paid millions to cover Prism compliance costs for tech companies." *The Guardian*, August 23. www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

MacKinnon, Rebecca. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom.* New York, NY: Basic Books.

———. 2015. "Corporate Accountability Index 2015." Ranking Digital Rights Project. https://rankingdigitalrights.org/project-documents/2015-indicators/.

MacKinnon, Rebecca, Elonnai Hickok, Allon Bar and Hae-in Lim. 2014. "Fostering Freedom Online: The Role of Internet Intermediaries." UNESCO Series on Internet Freedom. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

Madden, Mary and Lee Rainie. 2015. "Americans' Attitudes about Privacy, Security and Surveillance." Pew Research Center, May 20. www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Mayer-Schönberger, Viktor. 2009. *Delete: The Virtue of Forgetting in the Digital Age.* Princeton, NJ: Princeton University Press.

Mayer-Schönberger, Viktor and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London, England: John Murray.

McDonald, A. M. and L. F. Cranor. 2008."The Cost of Reading Privacy Policies." *Journal of Law and Policy* 43: 540–65.

Mendel, Toby, Andrew Puddephatt, Ben Wagner, Dixie Hawtin and Natalia Torres. 2012. *Global Survey on Internet Privacy and Freedom of Expression*. UNESCO Series on Internet Freedom. Paris, France: UNESCO. http://unesdoc.unesco.org/images/0021/002182/218273e.pdf.

Moore, Bo. 2014. "Apple's ridiculous censorship of the nudity in *Papers, Please*." *Wired*, December 12. www.wired.com/2014/12/papers-please-ios-censored/.

Morozov, Evgeny. 2013. *To Save Everything, Click Here.* New York, NY: Perseus Book Group.

Mowery, K. and H. Shacham. 2012. "Pixel Perfect: Fingerprinting Canvas in HTML5." Session at the Web 2.0 Security & Privacy 2012 Workshop, San Francisco, CA, May 24. www.w2spconf.com/2012/papers/w2sp12-final4.pdf.

NetMundial. 2014. "NetMundial Multstakeholder Statement." Netmunidal, April 24. netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Nyst, Carly. 2014. "End violence: Women's rights and safety online." Association for rogressive Communications, July. www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf.

OHCHR. 1966. International Covenant on Civil and Political Rights (1966, 999 UNTS 171). www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

———. n.d. "What are Human Rights." www.ohchr.org/en/issues/pages/whatarehumanrights.aspx.

Omand, David. 2015. *Understanding Digital Intelligence and the Norms That Might Govern It*. Global Commission on Internet Governance Paper Series No. 8. Waterloo, ON: CIGI. www.cigionline.org/publications/understanding-digital-intelligence-and-norms-might-govern-it.

Ratomski, Andrew. 2015. “Impact of Facebook Downtime on Global Traffic.” *GoSquared Engineering* (blog), January 27. https://blog.shareaholic.com/social-media-traffic-trends-01-2015/.

Roberts, Sarah T. 2015. “Behind the Screen: Digitally Laboring in Social Media’s Shadow World.” Unpublished manuscript, Western University, London, ON.

Robinson, Duncan. 2015. “Facebook wins latest case in class action privacy battle.” *Financial Times*, July 1. http://app.ft.com/cms/s/4914b45c-1fd1-11e5-aa5a-398b2169cf79.html?sectionid=topics/topics/Data_protection.

Roosevelt, Eleanor. 1948. “The Struggle for Human Rights.” Speech given at the Sorbonne, Paris. www.americanrhetoric.com/speeches/eleanorroosevelt.htm.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W. W. Norton & Co.

Schrems, Max. n.d. “Get your Data! Make an Access Request at Facebook!” *Europe versus Facebook* (blog). http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html.

Solove, Daniel. 2007. “‘I’ve got nothing to hide’ and other misunderstandings of privacy.” *San Diego Law Review* 44: 745.

Stevenson, Burton, ed. 1964. *The Home Book of Quotations, Classical and Modern*. 9th ed. New York, NY: Dodd, Mead.

Sweeney, Latanya. 2000. “Simple demographics often identify people uniquely.” Carnegie Mellon University. http://dataprivacylab.org/projects/identifiability/paper1.pdf.

Take Back the Tech. 2014. “Take Back the Tech’s! Report Card on Social Media and Violence Against Women.” www.takebackthetech.net/sites/default/files/2014-reportcard-en.pdf.

The Economist. 2014. “On being forgotten.” *The Economist*, May17.www.economist.com/news/leaders/21602219-right-be-forgotten-sounds-attractive-it-creates-more-problems-it-solves-being.

Tiku, Nitasha and Casey Newton. 2015. “Twitter CEO: ‘We suck at dealing with abuse.’” *The Verge*, February 4. www.theverge.com/2015/2/4/7982099/twitter-ceo-sent-memo-taking-personal-responsibility-for-the.

Toobin, Jeffrey. 2014. “The Solace of Oblivion.” *The New Yorker*, September 29. www.newyorker.com/magazine/2014/09/29/solace-oblivion.

UN. 1948. General Assembly resolution 217 A, *Universal Declaration of Human Rights,* A/RES/217 (111) (10 December 1948). www.un.org/en/universal-declaration-human-rights/.

———. 2011a. *Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie; Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework*, A/HRC/17/31. March 21. www.ohchr.org/Documents/Issues/Business/A-HRC-17-31_AEV.pdf.

———. 2011b. Human Rights Committee, 102nd Session General Comment No. 34, July. www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

———. 2012. General Assembly resolution 20.8, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/20.8 (16 July 2012). http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.

———. 2013. General Assembly. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank la Rue*, A/HRC/RES/23.40 (17 April 2013). www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Vaizey, Hester. 2014. *Born in the GDR: Living in the Shadow of the Wall.* Oxford, England: Oxford University Press.

Van Alsenoy, Brendan, Valerie Verdoodt, Rob Heyman, Jef Ausloos, Ellen Wauters and Güneş Acar. 2015. *From Social Media Service to Advertising Network: A Critical Analysis of Facebook’s Revised Policies and Terms*. Draft report for Belgian Privacy Commission, March 31. www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf.

Weber, Max. 1946. “Politics as a Vocation.” In *From Max Weber: Essays in Sociology*, edited by Hans H. Gerth and C. Wright Mills, 77–128. Oxford, England: Oxford University Press.

Williams, Rhiannon. 2015. “Telegraph stories affected by EU ‘right to be forgotten.’” *The Telegraph*, September 3. www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html.

Winkler, Rolfe. 2015. “Google Wants to Sell You Auto Insurance.” *Wall Street Journal* (blog), January 8. http://blogs.wsj.com/digits/2015/01/08/google-wants-to-sell-you-auto-insurance/.

Wong, Danny. 2015. "In Q4, Social Media Drove 31.2% of Overall Traffic to Sites [REPORT]." *Shareaholic Reports* (blog), January 26. https://blog.shareaholic.com/social-media-traffic-trends-01-2015/.

Wu, Tim. 2010. *The Master Switch: The Rise and Fall of Information Empires*. New York, NY: Knopf.

Zittrain, Jonathan. 2014. "Righting the right to be forgotten." *Future of the Internet* (blog), July 14. http://futureoftheinternet.org/2014/07/14/righting-the-right-to-be-forgotten/.

ABOUT THE AUTHOR

Emily Taylor is an Internet governance expert and an associate fellow of Chatham House. She has worked in the domain name industry since 1999. Emily is co-editor of the *Journal of Cyber Policy* (Taylor & Francis) and a member of the Global Commission on Internet Governance Research Advisory Network. Her research publications include the annual *World Report on Internationalised Domain Names* (lead author); various reports on Internet protocols for the UK regulator, Ofcom; a review of the policy development process of the Internet Corporation for Assigned Names and Numbers (ICANN); a study on the domain name system in the Middle East and adjoining countries (for ICANN) and a paper on IANA's (Internet Assigned Numbers Authority's) transition (for the Global Commission). She chaired the independent WHOIS Review Team for ICANN, and served on the United Nations Internet Governance Forum's Multistakeholder Advisory Group. For 10 years, she was at Nominet as director of legal and policy. She is a director of several Internet companies, including Oxford Information Labs, which specializes in data mining and statistical analysis.

CHAPTER EIGHT:
CORPORATE ACCOUNTABILITY FOR A FREE AND OPEN INTERNET

Rebecca MacKinnon, Nathalie Maréchal and Priya Kumar

ACRONYMS

EFF	Electronic Frontier Foundation
ESG	environmental, social and governance
GCIG	Global Commission on Internet Governance
GISR	Global Initiative for Sustainability Ratings
GNI	Global Network Initiative
HRIAs	human rights impact assessments
ICT	information and communications technology
IP	Internet Protocol
ISIS	Islamic State of Iraq and al-Sham
ISPs	Internet service providers
NSA	National Security Agency
OHCHR	Office of the High Commissioner for Human Rights
PII	personally identifiable information
RDR	Ranking Digital Rights
SASB	Sustainability Accounting Standards Board
ToS	terms of service

INTRODUCTION

As of July 2016, more than 3.4 billion people were estimated to have joined the global population of Internet users, a population with fastest one-year growth in India (a stunning 30 percent) followed by strong double-digit growth in an assortment of countries across Africa (Internet Live Stats 2016a; 2016b). Yet the world's newest users have less freedom to speak their minds, gain access to information or organize around civil, political and religious interests than those who first logged on to the Internet five years ago. Worse, according to Freedom House's *Freedom on the Net 2015* report, a growing number of governments are "censoring information of public interest and placing greater demands on the private sector to take down offending content" (Kelly et al. 2015).

In an ideal world — where existing global and national institutions could address human rights challenges in the Internet age — all of the world's nation-states would agree upon global frameworks grounded in human rights law for data protection, cyber security and management of cross-border law enforcement requests to restrict content or hand over user information. There would be clear and globally coordinated mechanisms to protect human rights while enabling states to meet their national security and economic obligations to their citizens. Such international frameworks, in addition to the laws and implementation practices of all participating governments, would have high levels of transparency and public accountability and would be fully consistent with international human rights standards, including the UN Office of the High Commissioner for Human Rights' (OHCHR) Guiding Principles on Business and Human Rights, under which states have a duty to protect human rights and companies have a responsibility to respect human rights (OHCHR 2011).

In the real world, governments, companies and a range of other non-state actors are pursuing short- and medium-term interests and agendas regarding how the Internet should be used and governed with whatever legal, regulatory, financial, political and technical tools happen to be available. The result: substantial "governance gaps" that either create a permissive environment for corporate violation of human rights (Ruggie 2008; 2013) or that cause information and communications technology (ICT) companies to be directly compelled by governments to violate the freedom of expression and privacy rights of their users (Kaye 2016).

As the revelations of former National Security Agency (NSA) contractor Edward Snowden and other recent policy developments in North America and Western Europe have shown, even governments that claim to champion the cause of global Internet freedom and openness have failed to be consistently transparent, accountable or respectful of international human rights norms in pursuing their interests. Fragmentation and "balkanization" of the Internet, whereby national borders are re-imposed upon globally interoperable digital networks (framed in another way by some governments as the assertion of states' right to "Internet sovereignty"), is a global trend that seems difficult to reverse in the absence of new mechanisms and processes for norm setting, problem solving, transparency and accountability (Drake, Cerf and Kleinwächter 2016; Mueller 2010).

Meanwhile, large multinational Internet platforms, which serve global constituencies of users and customers, increasingly find themselves at odds with governments — sometimes their home governments, sometimes other governments seeking to assert stronger sovereignty over how they manage information and data flows — with major implications for the rights and freedoms of people all over the world. At the same time, companies have insufficient (and sometimes negative) incentives to protect user information in the many countries where law either does not adequately compel them to do so or even compels them to violate privacy rights. Companies face growing legal and regulatory requirements around the world to comply with mass surveillance and to weaken encryption (DeNardis 2015; Schneier 2015). In many countries, Internet intermediaries also face growing legal liability for users' speech and activities (Frosio 2016). In addition, as Emily Taylor (2016) illustrated in her recent paper for the Global Commission on Internet Governance (GCIG) series, the privacy policies and terms and conditions of major global Internet platforms are by and large out of sync with human rights standards for freedom of expression and privacy. The execution of companies' private governance of users' activities is opaque and unaccountable.

If international legal and treaty frameworks cannot adequately protect human rights, then other types of governance and accountability mechanisms are urgently needed to provide incentives to owners and operators of Internet platforms and services to respect human rights. In response to this glaring governance gap, a number of initiatives and mechanisms have begun to emerge over the past decade.

This chapter first describes some of the key elements of a nascent yet innovative ecosystem of organizations and initiatives that could form the building blocks of a human-rights-compatible governance and accountability framework for Internet intermediaries, before examining how these developments fit within the broader context of the evolving role of corporations — beyond the ICT sector — in international governance and accountability systems. This examination focuses on rankings and ratings — one particular accountability toolset — which, when combined with transparency and disclosure frameworks, can help to foster greater accountability. For example, Ranking Digital Rights (RDR) published its inaugural Corporate Accountability Index in November 2015, ranking 16 global Internet and telecommunications companies on 31 indicators evaluating disclosed commitments, policies and practices affecting Internet users' freedom of expression and right to privacy. The chapter's final section considers the index's key findings and initial impacts, and discusses the potential for such public benchmarking of companies, along with other initiatives and mechanisms, to encourage greater corporate accountability for a free and open Internet.

INNOVATION IN GOVERNANCE AND ACCOUNTABILITY FOR INTERNET INTERMEDIARIES

Internet and telecommunications service operators, software producers and the manufacturers of device and networking equipment exert growing influence over the political and civil lives of people all over the world. They do so in a number of ways, including:

- compliance with laws, regulations and other government requirements;
- coordination of technical standards and resources with other public and private entities;
- product feature and design choices;
- software and hardware engineering (including security capabilities and features);
- corporate governance of employee actions;
- business priorities and practices;
- private policies governing how user information is handled; and
- private rules for what users can and cannot say or do.

As categorized by Laura DeNardis (2014), companies play a range of roles at all levels of Internet governance, from the basic layers of technical infrastructure and resource coordination that make global interconnection possible, to the layers of law and policy above them that determine rules for people's actions on the Internet and the mechanisms for policing such rules. This chapter focuses on efforts to establish greater accountability and transparency at one of six levels of Internet governance: "the policy role of information intermediaries" (ibid., 4).

Internet intermediaries are generally private entities that own and operate products and services that are channels for online communication. They mediate dissemination, exchange of and access to information on the Internet. In accordance with the UN *Guiding Principles on Business and Human Rights*, all companies — which necessarily includes all Internet intermediaries — share a responsibility to respect human rights (OHCHR 2011; European Commission 2013). A recent study commissioned by UNESCO (whose editor and co-author is also the lead author of this chapter) that examined the impact of Internet intermediaries on freedom of expression through in-depth case studies found that while the policy and legal environments of states are a major factor affecting companies' ability to respect human rights, companies in all jurisdictions nonetheless have control over a range of business practices and decisions that affect users' rights, including freedom of expression and privacy (MacKinnon et al. 2014).

One of the earliest efforts to build upon international human rights standards in defining the responsibilities of intermediaries for freedom of expression and privacy in the context of government demands for censorship and surveillance is the Global Network Initiative (GNI), a multi-stakeholder organization launched in 2008 with Google, Microsoft and Yahoo as founding corporate members. GNI member companies commit to uphold a set of core principles and implement them with guidance — often accompanied by honest critiques and tough questions — from other stakeholder groups: civil society, responsible investors and academics. Most important, company members are required to undergo regular independent assessments that enable the organization's multi-stakeholder governing board to verify whether they are satisfactorily implementing the principles (GNI 2015).

As of the fall of 2016, GNI's corporate membership has expanded from four to six companies (adding Facebook and LinkedIn); as well, seven European telecommunications companies[1] from the Telecommunications Industry Dialogue, a group that addresses freedom of expression and privacy in the sector, joined in early 2016 as observers, with the option to apply for full membership in early 2017 (GNI 2016a). While most of the material produced in company assessments reviewed by the GNI board is not published, methodical analysis of disclosed company policies and practices by the RDR Corporate Accountability Index (which will be discussed in greater detail in a later section) indicates that GNI member companies have made more systematic and verifiable efforts to institutionalize commitments, policies and practices related to government demands affecting users' freedom of expression and privacy than have most other Internet and telecommunications companies around the world (RDR 2015c).

GNI critics rightly point out that the organization was unable to prevent its corporate members from participating in PRISM and other US mass surveillance programs unveiled by whistle-blower Edward Snowden in 2013. Several factors explain this failure and underscore the reality that a multi-stakeholder non-regulatory corporate accountability mechanism has limited ability to expose, let alone prevent, abuse of power by a sufficiently well-resourced and determined government that is able to gain access to companies' core infrastructure through technical or legal means.

First, in several cases the companies did not wittingly share information with the NSA. For example, the NSA reportedly installed bugs on the cables connecting Google's data centres to one another, although Google's failure to encrypt this traffic was, in retrospect, negligent (Schneier 2015). Second, information silos within companies might also have kept those individuals involved with GNI processes in the dark about their employers' cooperation with the NSA. Third, the gag orders, particularly those associated with national security letters, prevented companies from bringing their concerns to GNI. National security letters are legally binding, confidential requests for information issued by US government agencies (notably the Federal Bureau of Investigation) in the context of national security investigations. Separately from GNI, Google, Microsoft and Yahoo have all successfully challenged the US government in court, but such legal battles tend to be protracted. GNI's limitations underscore the reality that efforts to strengthen corporate accountability will be most effective in strengthening the respect and protection of Internet users' rights only when they coexist with a broader ecosystem of efforts focused on legal reform.

Nevertheless, committing to implement the GNI principles, and to be assessed on that implementation, is an important step that companies can take toward accountability in respecting Internet users' rights in relation to policies and practices over which they do have operational control. In addition, GNI increasingly undertakes policy advocacy to push for legal and regulatory reforms that would maximize companies' ability to respect users' freedom of expression and privacy rights (GNI 2016c). Even so, GNI cannot actually stop governments from using the force of law — even sometimes physical force against employees — to compel Internet platforms and services to violate users' rights.

Nor does GNI membership prevent companies from infringing upon users' rights in a number of situations where government demands are not involved. As defined by the organization's multi-stakeholder board, which includes representatives from the companies themselves, GNI's implementation guidelines and assessment framework focus on company handling of government censorship, surveillance and data access demands affecting user freedom of expression and privacy. Issues related to terms of service (ToS) enforcement, commercial collection and use of user information, and the construction of privacy policies have thus far been out of scope for GNI.

Such scope limitations demonstrate another key weakness of multi-stakeholder accountability mechanisms: when the entities being held accountable play an equal role with other stakeholders in creating and governing the accountability mechanism, they will seek to define parameters with which they are comfortable as a condition of participation. This reality, combined with failures by all governments — to varying extents — to govern in a manner that fully meets the state's duty to protect human rights, highlights that if digital rights are to be respected and protected across the full range of threats, there is an urgent need for further innovation and efforts — not only in policy advocacy but in the creation of new types of governance mechanisms and tools.

One important GNI principle that has had widespread impact beyond its actual membership emphasizes the importance of corporate transparency about the handling of government requests (GNI 2012a). Google was the first company to release a "transparency report" in 2010. By early 2016, 61 Internet intermediaries had published at least one transparency report (Access Now 2016). Such reports disclose a range of information about actions companies have taken to restrict content or share user information, particularly in relation to government requests: when requests happen, how often they happen,

[1] Millicom, Nokia, Orange, Telefónica, Telenor Group, TeliaSonera and Vodafone Group.

how often companies comply and the company policies for handling them.[2]

Unfortunately, some of the longer-running transparency reports reveal a disturbing increase in government demands to restrict content and share user data.[3] Transparency, combined with implementation of best practices in handling government demands (for example, interpreting requests narrowly, so that one complies only with requests made in accordance with legal procedure and falling within scope of the law), has not deterred governments from making demands. Governments, for their part, are failing to match companies in transparency about the demands being made to companies. A report issued by a multi-stakeholder working group of the Freedom Online Coalition, an intergovernmental organization of governments committed to promoting a free and open global Internet, pointed to the general lack of government transparency about requests made to Internet intermediaries as a barrier to holding governments and companies accountable for respecting online rights (Freedom Online Coalition 2015). Governments and companies should independently disclose requests made and received, subject to an audit process, thus holding one another accountable. In cases where national law prohibits such disclosures, companies should, at a minimum, explain the kind of data being withheld and under what legal authority.

Given the limitations of transparency reporting, other types of accountability-enhancing efforts are needed to redefine when and under what circumstances it is acceptable for governments to make requests and how these requests should be made. Bertrand de La Chapelle and Paul Fehlinger have argued that in order to prevent the "uncontrolled reterritorialization of the Internet" (2016, 8) by governments seeking to impose their will on private intermediaries, new forms of transnational multi-stakeholder decision making and coordination, particularly around processes such as cross-border requests by law enforcement to companies, are urgently needed. They call on concerned stakeholders from government, the private sector, the technical community and civil society to work together to create a new system of "issue-based" multi-stakeholder "governance networks" (ibid., 10).

New multi-stakeholder bodies created to hash out solutions to specific problems, however, are unlikely to have the power and authority to prevent abuse of human rights or to hold abusers accountable unless they are accompanied by some kind of international court or arbitration body with international legitimacy to resolve disputes, pass judgments, impose appropriate penalties and ensure that victims receive appropriate remedy. Precedent suggests that this is unlikely, leaving would-be reformers with the softer tools of research and advocacy. Meanwhile, governments grow increasingly effective at censoring and surveilling people's online speech and activities via corporate intermediaries, restricting opportunities for such advocacy.

As a first step, Ronald Deibert (2016, 213) calls for greater corporate accountability and "a system for monitoring cyberspace rights and freedoms that is globally distributed and independent of governments and the private sector." Yochai Benkler (2016, 20), concerned about the "Internet that facilitates the accumulation of power by a relatively small set of influential state and nonstate actors," suggests "building an effective audit and accountability system into the Internet design to enable identification and accountability of abusive power" (ibid., 29).

GNI's voluntary assessment framework is the only systematic audit framework specifically concerned with Internet intermediaries' human rights responsibilities presently in existence.[4] Limited details of GNI company assessments are published, however, and only a handful of companies — all of them US-based Internet platforms — have thus far completed the voluntary process (GNI 2016b). GNI is a necessary part of the solution, but it alone is insufficient, given that it is unable to confront violations committed by non-member companies; nor does its scope address the full gamut of its members' human rights harms.

To fill these gaps, several other independent academic initiatives and organizations carry out in-depth research or collect and aggregate data about corporate practices and their human rights impacts, producing information that can potentially be used to hold companies and governments accountable. Examples include the University of Toronto's Citizen Lab, led by Ronald Deibert, which for more than a decade has supported a team of researchers who publish thorough and often highly technical investigations into practices — many of them often deliberately kept secret or obscure — by governments and companies that violate Internet users' rights. Harvard's Berkman Klein Center for Internet & Society produces a publicly accessible "Internet monitor" information platform that contains a variety of data about the shape and nature of the Internet,

[2] The advocacy organization Access Now maintains a directory of corporate transparency reports. In response to concerns that companies do not publish information in a way that is sufficiently consistent to enable clear comparisons, New America's Open Technology Institute and the Berkman Klein Center for Internet & Society have published a transparency reporting guide for US-based companies to use in disclosing government requests for user data (Budish, Woolery and Bankston 2016).

[3] For example, see the figures at www.google.com/transparencyreport/userdatarequests/?hl=en and at https://transparency.twitter.com/en/removal-requests.html.

[4] Note that the Berkman Klein Center for Internet & Society, which Benkler co-directs at Harvard, is a member of GNI's academic constituency and is represented on its governing board.

including information that reflects the actions and policies of governments and Internet intermediaries.[5]

Since 2011, the Electronic Frontier Foundation (EFF) has published an annual report called *Who Has Your Back?* that rates US-based companies on their policies and practices in response to US government demands. Over the project's lifetime, EFF staff have observed concerted efforts by some of the largest and most powerful US-based companies included in the yearly reports to improve their performance.[6] The EFF's success in creating a mechanism for benchmarking corporate respect for users' privacy and expression rights in the United States and in holding companies accountable for their policies and practices was among several factors that inspired the development of the global RDR Corporate Accountability Index.

CORPORATIONS, GLOBAL GOVERNANCE AND ACCOUNTABILITY BEYOND THE ICT SECTOR

ICT sector companies have played a prominent role in Internet governance organizations, mechanisms and processes over the past two decades. Companies in other sectors also play an expanding role in global governance. Multinational companies wield more power than many governments over not only digital information flows but also the global flow of goods, services and labour: one-third of world trade is between corporations, and another third is intra-firm, between subsidiaries of the same multinational enterprise (May 2015).

Increasingly since the end of the Cold War, governments have been forced to share many types of power — economic, financial, social, military, cultural and political — with non-state actors, including corporations and non-governmental organizations (Mathews 1997). Multi-stakeholder organizations have emerged to address "governance gaps" not only on Internet issues but also on concerns ranging from natural resources governance to human rights. Corporate accountability mechanisms — sometimes as a complement to regulatory weakness and sometimes in lieu of absent or problematic regulation — have emerged across various sectors to hold companies accountable for their impact on human rights, public health, environmental sustainability and many other areas of corporate responsibility.

Around the same time that the Internet Corporation for Assigned Names and Numbers was formed in 1998, with an innovative multi-stakeholder governance structure for managing the Internet's addressing system, other multi-stakeholder organizations addressing companies' human-rights-related governance challenges also began to emerge: the Fair Labor Association in 1999 (for the footwear and apparel manufacturing sector), followed by the Voluntary Principles on Security and Human Rights in 2000 (established to help extractive and energy companies maintain security and safety of their operations while respecting human rights). The Extractive Industries Transparency Initiative (which promotes greater public accountability in how countries manage their oil, gas and mineral resources) followed in 2002. GNI, for the ICT sector, came later, in 2008, borrowing and adapting elements from the previously established initiatives' governance and accountability structures.

The limitations of other sectors' multi-stakeholder accountability mechanisms in preventing abuse (or neglect) of human rights are similar to those GNI has faced. Private actors and voluntary initiatives can do much to prevent human rights harms within companies' operational control but they cannot make up for abject failures by public authorities to meet their duty to protect human rights. The Fair Labor Association, for example, while having done much to prevent human rights abuses in many corporate supply chains around the world, could not prevent the Bangladeshi government's failure to enforce labour and safety laws, which resulted in the disastrous 2013 Rana Plaza factory collapse that killed 1,138 people (Kasperkevic 2016).

Yet, while responsible and accountable governance remains a distant dream in many countries, efforts by non-state actors have done much to prevent the human rights situation around the world from being substantially worse than it might otherwise be — in particular in areas over which companies have at least some measure of operational control and an incentive to demonstrate respect for human rights. While investigations and advocacy campaigns by non-governmental organizations have helped to hold corporations publicly accountable for practices affecting the environment and human rights around the world (Pace and Courtney 2015), investors have also grown increasingly effective over the past two decades in using financial markets and sometimes even regulation as mechanisms for corporate accountability. By the beginning of 2014, US$21.4 trillion of investment assets were under professional management in Europe, the United States, Canada, Asia, Japan, Australasia and Africa. These assets were subject to some degree of screening for environmental, social and governance (ESG) factors, with more than half of European assets undergoing some type of ESG screen (Global Sustainable Investment Alliance 2015). The years 2015 and 2016 saw a record number of

[5] See https://thenetmonitor.org/.

[6] Through 2015, EFF's *Who Has Your Back?* report covered Internet intermediaries (Cardozo, Opsahl and Reitman 2015). Beginning in 2016 they switched their focus to "gig economy" and "sharing economy" services.

shareholder resolutions on non-financial issues ranging from climate change to human rights (Proxy Preview 2015; 2016). The presence of an investor constituency in GNI reflects emerging concern from responsible investors about companies' impact on freedom of expression and privacy.[7]

Building upon increased concern from shareholders and other stakeholders in companies' ESG performance, organizations such as the Global Reporting Initiative and the Sustainability Accounting Standards Board (SASB) now issue guidelines for how companies should report to investors about non-financial risks and impacts. Notably, the SASB has developed provisional non-financial reporting standards for the ICT sector, including information about practices affecting privacy, security and freedom of expression (SASB 2016).

The SASB's development process for corporate reporting standards comes at the same time as the US Securities Exchange Commission's undertaking of a public comment process on expanding requirements for corporate disclosure of non-financial information (US Securities Exchange Commission 2016; White 2016). Such expansion would follow in the footsteps of the European Union's 2014 directive, which required larger European companies to report non-financial and diversity information that is material to their business (European Union 2014). Member states must pass corresponding legislation by late 2016, with company reporting expected to start in 2017 (Gardiner and Lienin 2015). Consultations were undertaken in early 2016 regarding the scope of such reporting (European Commission 2016a). Meanwhile, investors are pushing for legal clarification that their fiduciary duty includes taking long-term factors, including non-financial ESG information, into account in decision making, which could lead to even greater weight being given to ESG factors by investors across Europe and beyond (Johnston and Morrow 2016).

The developments described above point to the increasing use of non-traditional governance mechanisms to "regulate" company practices, with financial markets an increasingly powerful vector with which to hold companies accountable for their impact on the environment and society. Companies have responded to the pressure: as of 2014, 93 percent of the world's 250 largest companies were publishing annual corporate responsibility reports, 60 percent of which were independently audited (Nelson 2014). The ability to reward companies for their environmental and social responsibility through investment markets has, in turn, increased the demand for data and metrics. One response has been the development of platforms such as CDP[8] (formerly known as the Carbon Disclosure Project, before it expanded to cover more areas), which works with companies to disclose information about their environmental impacts.

Another related response has been the proliferation of efforts to benchmark and rank companies on their policies, practices and impacts. The past decade has seen a proliferation of corporate ratings, rankings and indexes that aim to address global governance gaps on a range of issues including climate change, presence of conflict minerals in the supply chain, combatting corruption, sustainable food sourcing, access to medicines in developing countries, supply chain labour rights and human trafficking.[9] Academic research on the impact of sustainability rankings and ratings points to the various ways that they might affect company practices: providing a framework for companies to develop comprehensive strategies to improve; providing a platform through which companies can communicate their successes; and sparking efforts by employees who care about the environmental and social impact of their employer (Muli 2013). Industry surveys show that credible rankings and ratings enable companies to benchmark their own yearly progress as well as compare themselves to their peers (Sadowski 2012).

Rankings and ratings have also emerged over the past two decades as an accountability tool aimed at governments. Their efficacy in influencing government policy and practice in a manner that translates into improvement of people's lives on the ground is subject to much scholarly criticism and debate (Green 2001; Giannone 2010; Brooten 2013). They are found to be most successful when clearly tied to concrete economic or financial levers, such as development aid or international investment decisions (Cooley and Snyder 2015, 35). Scholars Alexander Cooley and Jack L. Snyder, editors of *Ranking the World*, have offered a list of recommendations to make these systems more effective. Suggestions include practising maximum transparency about the methodology, indicators and research process, as well as grounding the system on "best available empirically grounded knowledge" rather than "ideal-typical attributes" (ibid., 191).

For company-focused rankings, the non-profit GISR has developed a set of 12 principles to guide the development and assess the credibility — and therefore potential for impact — of a given ranking, rating or index. The principles include transparency, impartiality, inclusiveness (broad stakeholder engagement) and continuous improvement (through empirical research).[10]

[7] For a list of investor participants, see http://globalnetworkinitiative.org/participants/index.php?qt-gni_participants=4#qt-gni_participants.

[8] See www.cdp.net.

[9] The Global Initiative for Sustainability Ratings (GISR) has created a database of many of them (see http://ratesustainability.org/hub/index.php/search/).

[10] See the principles at http://ratesustainability.org/core/principles/.

RDR CORPORATE ACCOUNTABILITY INDEX

The RDR project drew upon GISR guidelines in designing a ranking that can hold companies accountable for respecting users' privacy and free expression by providing actionable data to stakeholders, including investors, human rights advocates, policy makers and companies themselves. After a lengthy process comprising stakeholder consultations, case study research, multiple methodology revisions and a pilot study, RDR published its inaugural Corporate Accountability Index in November 2015. The index ranked 16 global ICT companies on 31 indicators evaluating disclosed commitments, policies and practices related to digital rights.

The index's research methodology represented the culmination of three years of an iterative process of research, stakeholder consultations and exploratory studies. Notably, the case study research conducted in 2013 demonstrated the difficulty of empirically verifying actual practice and convinced the team to focus on companies' public disclosures. Indeed, researchers found that some company representatives, particularly but not exclusively those headquartered in less democratic or transitional states, either declined to be interviewed or provided answers that were at odds with other verified sources, and sometimes even threatened legal action. By emphasizing public disclosure of information related to users' rights, RDR (2016) puts the onus on companies to be transparent and accountable to their users directly and leaves room for others to verify companies' compliance with their own stated policies.

The 31 indicators used to evaluate companies align with recent recommendations for corporate practice issued by the GCIG, including that users "should know about and have some choice over the full range of ways in which their data will be deployed for commercial purposes"; terms of use should be clear and accessible and not subject to change without users' consent, and that "businesses should demonstrate accountability and provide redress in the case of a security breach or a breach of contract" (GCIG 2016, 42). The structure and content of the indicators also draw heavily from the UN *Guiding Principles on Business and Human Rights* and, more specifically, the GNI principles and implementation guidelines — as well as a range of emerging privacy standards, including the Organisation for Economic Co-operation and Development's privacy guidelines and the US Federal Trade Commission's fair information practice principles.

RDR was designed to pick up where GNI leaves off in several ways. Its scope is broader: it addresses commercial and private practices not related to government requests; and, unlike GNI, which only evaluates companies that choose to join the initiative, RDR selects companies for evaluation regardless of companies' willingness to engage with the project. Its process and results are more public and transparent: GNI company assessments are carried out under legal privilege and examine internal information that is not made public, whereas RDR examines information that companies publicly disclose and makes all of its raw research data publicly available. Yet the index also helps to reinforce and reveal the value of GNI's less public work by clearly exposing the differences between GNI member companies and non-GNI companies, in addition to exposing specific differences among GNI member companies.

The index found that across the board, companies need to improve disclosure of policies and practices that affect users' freedom of expression and privacy, as well as their commitments to these human rights. No company in the index provides users with sufficiently clear, comprehensive and accessible information about their practices that affect freedom of expression and privacy. These practices include companies' handling of user information, ToS enforcement and access to remedy for users whose rights have been violated. Detailed findings across all 31 indicators can be found in the index report and on the project website (RDR 2015a; 2015b). Below is a discussion of key findings that are of particular relevance to Internet governance gaps.

Corporate Governance

The "Commitment" section of the index (to be renamed "Governance" starting in 2017) looks for evidence that companies take their responsibility to respect human rights seriously by making a public commitment to free expression and privacy, with accountable oversight at the board, executive and management levels. Consistent with established corporate social responsibility standards, RDR expects companies to institutionalize their commitments by training employees on free expression and privacy issues, as well as maintaining whistle-blower programs that pertain to digital rights; to conduct human rights impact assessments (HRIAs) when entering new markets or launching new services; to engage with stakeholders, notably through membership in fora such as GNI and the Telecommunications Industry Dialogue, an industry organization also focused on freedom of expression and privacy; and to provide mechanisms for users to file grievances related to free expression and privacy as well as to offer appropriate remedy when violations occur.

It is notable that the seven companies earning more than 50 percent of total possible points in this section are all members of GNI or the Telecommunications Industry Dialogue.

User Information

Today's Internet users increasingly understand that their user information is the currency of the Internet (DeNardis

2015; Zuboff 2015) and that information initially exchanged for a given product or service may later be sold, combined with information from other sources, mined as part of "big data" calculations and acted upon in ways that are difficult to imagine, much less verify. Information collected by commercial entities can also end up in the hands of government agencies, whether pursuant to a legal process or not, as Edward Snowden's 2013 revelations made apparent. Governments might then use that information for legitimate law enforcement purposes but also to suppress social movements, harass political adversaries or otherwise violate human rights.

Part of the difficulty in governing user information is the ambiguity of the concept itself. Under US law, the existence of a privacy harm turns on whether the information in question is personal or personally identifiable information (PII), yet the law lacks a clear definition of PII, and information that often is not considered PII, such as an Internet Protocol (IP) address, can easily be linked to an identifiable person (Schwartz and Solove 2011). The European Union's General Data Protection Regulation takes a broader approach to personal data, defining it as "any information relating to an identified or identifiable natural person"; this can include "an identifier such as a name, an identification number, location data, an online identifier or...one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" that can be used to directly or indirectly link a piece of information to a person (European Union 2016, 33).

RDR's definition of "user information" is broader still: "Any data which is connected to an identifiable person, or may be connected to such a person by combining datasets or utilizing data-mining techniques" (RDR 2015a). This definition includes information that people actively provide (for example, name, content of messages), as well as information that companies automatically collect when people use a service (such as IP address, Global Positioning System coordinates). The rationale for this definition is that people need to know what happens to all information that could be used to build a profile or dossier about them.

The companies evaluated by the Corporate Accountability Index hew fairly closely to US legal and regulatory conceptions of personal information, which exclude information such as log data or cookie data. While every company provided at least some information about the type of user data it collected, the use of the broad term "personal information" to describe it collectively obscures, rather than clarifies, how companies handle the information they have on their users. Many companies appeared to leave open the option to collect a wide swath of extremely sensitive information, or included language that clearly indicated that their disclosures were not comprehensive.

ToS Enforcement

Users entrust companies with their personal information — however that is defined — in exchange for which companies provide access to the global public sphere. Companies then set certain limits on the types of speech that they will permit on their platforms, as outlined in their ToS. However, none of the companies evaluated in the Corporate Accountability Index disclosed any information about how these terms are enforced, beyond listing different types of speech or activities that are prohibited. Social media companies in particular have enormous latitude in determining the boundaries for permissible speech in the public sphere, somewhat akin to the discretionary powers of newspaper editors in earlier eras but with a much deeper reach into people's lives. Platforms such as Facebook, Twitter and YouTube are used for political speech but also for interpersonal interactions among families and communities in contexts as diverse as humanity itself. While ToS documents list the types of content that are not permitted (such as hate speech, so-called revenge porn and harassment), users have little to no insight into the mechanisms for enforcing these rules. Controversies regularly erupt around the uneven enforcement of rules about nudity, harassment and "real name" policies, among other topics. This lack of clarity can lead to chilling effects, and the reliance on flagging by other social media users allows reporting itself to become a tool for harassment.

The human rights implications are significant. The number and range of publicly reported incidents concerning Facebook are greater than for other platforms, although the harms caused by opaque and unaccountable ToS enforcement mechanisms are not limited to Facebook. For example, members of the global lesbian, gay, bisexual and transgender community rely on platforms such as Facebook to connect with one another, yet must use pseudonyms to stay safe. As Ethiopian activist HappyAddis explains, "People will go and attack you. Even other gay people, you don't trust them. How can you find out whether they're real gay people using their real account?" (Davidson 2015). HappyAddis's Facebook account was blocked in 2015 due to the company's "real identity" policy, which requires users to go by a name that matches their government-issued identification documents. Because Facebook only enforces this policy when an account is flagged by another user, it is often used as a tool to silence sexual minorities, activists and other vulnerable members of society. HappyAddis's account was eventually restored after his situation was profiled by the *Time Money* site (Davidson 2015).

Journalists also frequently fall afoul of the content moderation guidelines. In June 2016, the Facebook account of Radio France International reporter David Thomson (who covers issues related to terrorism) was blocked because of an Islamic State of Iraq and al-Sham (ISIS) flag in the background of an image posted in 2013. Social media companies have come under growing pressure from Western governments in 2015 and 2016 to eliminate content that glorifies ISIS, in particular efforts to use social media to radicalize and recruit new members (European Commission 2016b; Drozdiak 2016; Hughes 2016). However, Thomson's case is an example of the collateral damage caused by over-broad enforcement mechanisms, which were applied retroactively to Thomson's earlier content (Reporters Without Borders 2016).

Ordinary users speaking out in defence of human rights have likewise seen their content subject to removal. Images depicting victims of war and violence, such as Syrian artist Khaled Barakeh's photographs of body bags containing the remains of drowned refugees, are routinely taken down despite their newsworthiness. As one Facebook user commented, "with [this] reasoning, CBS and Walter Cronkite should have never reported on the Vietnam War the way they did" (Mirzoeff 2015). Indeed, in the twentieth century the depiction of war and violence was the subject of intense debate, but this debate was conducted within the context of a highly evolved code of journalistic ethics and editorial responsibility. Considering the repercussions on advertising revenue or other business interests was understood to be in violation of that code (Kovach and Rosenstiel 2014; McChesney 2013). In contrast, Facebook's June 2016 changes to the Newsfeed algorithm, which prioritizes "friends and family" content, would seem to represent a rejection of the duties to inform and educate — not only entertain — central to earlier notions of media's role in society (Mosseri 2016).

Yet, some of the world's most powerful Internet companies have thus far resisted calls for greater transparency with respect to content moderation and ToS enforcement. Several companies told RDR's researchers in private communications that publishing data about the volume and type of content removed in the course of enforcing ToS (for example, against hate speech, harassment, incitement to violence, sexually explicit content and so on) would not, in their view, help promote freedom of expression. Some argued that too much transparency about such enforcement would enable criminals and people seeking to harm other users to more effectively "game" the system, while others argued that private enforcement also includes fighting spam, about which it supposedly would not be meaningful to provide insight.

At the same time, civil society groups in a range of countries have raised concerns that companies enforce their ToS in a manner that is opaque and often viewed as unfair to certain groups. Such problems indicate that for companies to maintain or establish legitimacy as conduits for expression, they must also offer greater transparency and accountability in relation to how they police users' content and activities.

Without clear disclosure from companies, the public is left to draw conclusions about ToS enforcement based on anecdotal evidence and conjecture. While both algorithms and human reviewers are used by companies, it seems that enforcement largely relies on flagging by individual users and, reportedly, certain categories of "superflaggers" whose reports might be prioritized (Crawford and Gillespie 2014). Even then, much activity that would seem like a clear case of harassment is deemed to meet community standards. Rules without fair enforcement tend to devolve to the law of the jungle, where the strong flourish at the expense of the weak. Jillian C. York (2016) of the EFF and OnlineCensorship.org argues that the reliance on user flagging feeds a culture of snitching that serves to reflect and reinforce existing power imbalances. Moreover, companies' ability to moderate content fairly and consistently differs drastically according to the language and cultural context involved, so that content that is expressed in languages spoken by fewer users or less machine-readable is at a disadvantage.

Content moderation also has a labour rights dimension: who performs this work, and under what conditions? While companies themselves are quite opaque about their practices, several journalistic outlets have looked into these questions in recent years. According to the reports, US Internet giants outsource much of this labour to specialized firms that employ young workers in the developing world, notably in the Philippines, for as little as US$300 per month. Workers in these digital-age sweatshops often sustain a form of post-traumatic stress disorder due to repeated exposure to vile content, and are required to sign strict non-disclosure agreements. For US-based content moderators, the pay is much higher, but the working conditions are just as draining. Lacking full-time employee status, these workers are not included in companies' corporate disclosures, despite representing up to half of the social media sector's workforce (Chen 2014; Roberts 2016).

Multi-stakeholder and civil society initiatives to date have focused on the user dimension of content moderation, but this related governance gap is also worthy of attention, particularly as the selection and working conditions of the moderators have a direct impact on the free expression rights of users. For digital media consultant Joi Podgorny, this governance gap shows the task of content moderation to be an "afterthought" within the ICT industry. As she told The Verge's Catherine Buni and Soraya Chemali (2016), "moderation and related work remains a relatively low-wage, low-status sector, often managed and staffed by women, which stands apart from the higher-status, higher-paid, more powerful sectors of engineering and finance, which are overwhelmingly male." Company founders and developers are rarely exposed to the most toxic content and might even resist understanding the practice of moderation, viewing the issue instead as an ironclad binary of free speech and censorship (ibid.). This frame inhibits the kinds of nuanced debate necessary for developing a transparent approach to content moderation that respects and promotes human rights.

Given the complexity of the problem, pressure from researchers and civil society alone might be insufficient to force companies to substantially change their practices. At the same time, resolving the human rights issues surrounding content moderation through regulatory intervention is likely to be elusive, given that governments, facing public pressure to address violent extremism, are turning to solutions that push companies in a direction that is less rather than more accountable to international human rights standards on freedom of expression (Jeppesen and Llansó 2016). Nonetheless, a clearer understanding of the problem is the first step toward innovation in governance, to be followed by the articulation of concrete steps that companies should take toward improved accountability.

Grievance and Remedy

Grievance and remedy constitute a third area ripe for substantial improvement. The Corporate Accountability Index found very little disclosure related to grievance and remedy, even though this is an important component of the UN *Guiding Principles*. This finding may be partially due to the difficulty for users to determine whether a problem is a digital rights issue, a technical malfunction, human error or something else. Nevertheless, the index results highlight how performance differs substantially from commitment and ideals. GNI has stated its intention "to implement a standard for freedom of expression and privacy in the ICT sector that is consistent with the UN's Protect, Respect, and Remedy framework" (GNI 2012b). The Telecommunications Industry Dialogue, in its principles, has identified implementation of grievance mechanisms as an aspiration (Telecommunications Industry Dialogue 2013).

However, unlike other indicators in the "Commitment" category, membership in GNI or the Telecommunications Industry Dialogue was not a predictor of performance on the indicator, which focused on grievance and remedy mechanisms that clearly include complaints related to freedom of expression and privacy. The fact that few companies provided disclosure that aligned with expectations for business and human rights highlights an important opportunity for dialogue between industry and other stakeholders about what these practices should look like. Much of the disclosure suggests that, despite their principled commitments, companies have not conceptualized how to incorporate grievance and remedy into their established communication mechanisms.

Without access to meaningful channels for users to report violations of their rights and to obtain remedy, it is difficult to hold corporate or government actors appropriately accountable when people's rights to freedom of expression are violated in the digital realm. Unfortunately, remedy mechanisms in the ICT sector in relation to freedom of expression and privacy are underdeveloped and largely ineffective. The companies that received the highest scores for remedy mechanisms in the index were Bharti Airtel and Kakao — based, respectively, in India and South Korea. Regulation appears to play a positive role: both of these countries have laws that require grievance and remedy mechanisms.

Impact of the Regulatory Environment

The 2015 Corporate Accountability Index research reveals a number of instances in which laws and regulations in a range of countries make it more difficult for companies to perform well on certain indicators within the "Freedom of Expression" section of the index, and *all* of the ranked companies face some legal and policy hindrances in the "Privacy" section of the index. Some companies face more domestic political, legal and regulatory obstacles to respecting users' rights than others, because some countries' political and legal frameworks are less compatible with international human rights standards. There are also legal and regulatory obstacles that inhibit corporate transparency on the ways in which laws, policies and government actions affect users in practice. Laws in many countries forbid companies from disclosing national-security-related government requests to share user information or restrict or remove content.

Jurisdictional analysis conducted by country experts for the Corporate Accountability Index revealed a number of ways that governments limit or explicitly forbid companies from informing users about demands they receive from governments and other third parties to restrict or remove speech in the digital environment. Such disincentives are an obstacle to basic levels of transparency necessary to hold governments and private actors accountable for protecting and respecting human rights generally, and freedom of expression specifically.

Governments that make direct requests to companies to restrict or remove content generally do not publish data about the volume and nature of requests being made, thus hindering public accountability about demands being placed upon companies to restrict speech. A number of governments prohibit companies from reporting on government requests, to varying extents. Examples drawn from the index report include:

- In China, laws pertaining to state secrets and national security prevent companies from publishing information about government requests to remove or restrict online speech.
- In South Korea, while it is possible to report data about government and private requests to restrict

content, the law prevents companies or other third parties from publishing copies of restriction or removal requests, even when the requests originate from non-governmental sources. This law makes it impossible in Korea to have an online repository of take-down requests similar to the Lumen database (formerly known as "Chilling Effects"), a public service project operated by US-based lawyers.[11]

- In India, the law prevents companies from disclosing information about specific government requests for content restriction or removal. However, it does not prevent aggregate disclosure.

In addition, RDR researchers identified a number of instances where ambiguity about the scope of laws and regulations creates uncertainty among companies about the extent to which they may be transparent about requests to restrict speech without falling afoul of the law. Examples include:

- In South Africa, it is unclear whether it would be legal for companies to report aggregate data about government content restriction requests. While companies in South Africa are banned from reporting on government requests for user information, it is unclear whether Internet service providers (ISPs) or mobile operators could be affected by the National Keypoints Act of 1980, which gives the government the ability to censor information ab out infrastructures considered crucial to national security. This act could potentially prevent a company from disclosing information about requests related to content or account restriction.

- In Malaysia, ISPs are subject to licensing requirements, rules and regulations, not all of which are published or made available to the public. The Malaysian Official Secrets Act of 1972 may prevent companies from disclosing some information about government requests, although according to local legal experts, it would be unrealistic to conclude that this law affects every restriction request that companies receive.

- In the United Kingdom, more than one law could potentially prevent an ISP or mobile data service from disclosing specific requests to restrict content or access to a service. However, even if some UK laws limit companies from being fully transparent, companies could nonetheless publish more aggregate data related to all the requests they receive that they are legally able to publish (based on UK law as it stood in 2015). Different companies have taken different positions on whether they can publish the number of copyright-related blocking orders they receive (Vodafone does not publish this data while Virgin, TalkTalk and Sky do). Moreover, on the basis that information about terrorist-related sites that have been blocked upon request of the Counter Terrorism Internet Referral Unit has been announced in Parliament, it seems there is no barrier to companies also disclosing such information.

Company Responses

We are already seeing indications that RDR's strategy of coupling public benchmarking with company-oriented insider advocacy is effective. In response to a letter from the advocacy group Access Now about the company's results in the index — which showed greater emphasis on privacy than freedom of expression — a senior executive of Kakao wrote that the company will "soon start to institutionalize our commitments to users' freedom of expression at the same level of our commitments to privacy" and that other improvements were being planned such as "clearer control options for collection of user information and more details of the company's collection of user information."[12] In its public response to Access Now's letter about Microsoft's results, the company stated: "We already have work underway to address some of Access Now's primary recommendations, particularly around further enhancing our human rights grievance and remedy mechanisms."[13] While AT&T was found to carry out no assessments on the human rights impacts of its US operations, a company executive wrote to Access Now that AT&T is conducting HRIAs on its newly acquired Mexican wireless operations.[14]

RDR's results also helped to highlight shortcomings in a manner that added extra evidence and data to existing advocacy efforts by a range of stakeholders. For example, shortly after research was completed for the 2015 index, Microsoft substantially expanded its transparency reporting to include content restriction, which had previously been absent from transparency reports that included only government requests for user information. WhatsApp and Instagram (both owned by Facebook) have, respectively, implemented end-to-end encryption and announced the roll-out of two-step authentication, two recommendations from the 2015 index. Likewise, Facebook's Messenger now offers optional encryption for messages between two mobile applications (encrypting messages sent from a web browser is more technically difficult, although far from impossible). After RDR's 2015 index highlighted the lack of company disclosure about ToS enforcement, Twitter's February 2016 update of its transparency report included some data on it (Kessel 2016).

[11] See https://lumendatabase.org.

[12] See https://business-humanrights.org/sites/default/files/documents/Kakao%20response.pdf.

[13] See https://business-humanrights.org/sites/default/files/documents/Microsoft-Response-to-Access-Now-June-1-2016-letter.pdf.

[14] See https://business-humanrights.org/sites/default/files/Letter%20to%20Access%20on%20RDR.pdf.

Some of the ranked companies state publicly that they are using the index as an internal tool. For example, in its response to Access Now's recommendations for how the company can improve its performance in future iterations of the index, Google stated: "Since the report was issued, we have used the findings to guide internal discussions about how our practices and communications to the public can evolve."[15] Moreover, anecdotal indications are that companies beyond the 16 ranked in 2015 are using the index to benchmark and improve upon their own performance.[16]

The full extent to which companies have responded to the inaugural RDR Corporate Accountability Index will not be known until the project completes its second rankings cycle and releases its second index in early 2017, when the full range of changes can be examined and compared.

CONCLUSION

Existing global governance structures developed in the analog age are failing to address a range of global governance gaps, which, due to their cross-jurisdictional nature on a globally interconnected Internet, are even more difficult to address than analog governance gaps that persist due to governance failures by nation-states. At the same time, the Internet has enabled the rise of a new global force sometimes called "the Fifth Estate," an ecology of "networked individuals" who use the Internet and related technologies to hold governments and other institutions accountable (Dutton 2009, 3). Governance of the decentralized, globally networked Internet that powers this Fifth Estate requires an approach that is equally decentralized, distributed and networked (Maréchal 2015).

The RDR project generates data that can be used by investors, advocates, policy makers and companies to identify and address governance gaps affecting freedom of expression and privacy on the Internet. RDR's effectiveness will depend on the extent to which its data and underlying standards are used by an ecosystem of stakeholders to hold companies and governments accountable for respecting and protecting Internet users' rights. Importantly, it does not aim to be comprehensive, given that it only assesses company disclosure, inviting other researchers to build on this starting point to verify company claims with empirical testing. Rather, it aims to be one of many inputs that might eventually form a globally distributed system of monitoring, audit and accountability as called for by Deibert, Benkler and others. Such a decentralized system of research and verification in turn might inform the establishment of new, distributed, multi-stakeholder governance mechanisms and processes needed to address (if not fully eliminate) existing governance gaps and to hold the individuals, institutions and companies that shape the Internet accountable to the public interest.

[15] See https://business-humanrights.org/sites/default/files/documents/GoogleLettertoAccessNow.pdf.

[16] Representatives from several companies that were not part of the ranking have told RDR project staff that they have begun to use the indicators in internal assessments of policies and practices related to digital rights. Representatives of several investment firms have also told staff in private conversations that they have contacted companies about their performance in the index.

WORKS CITED

Access Now. 2016. "Transparency Reporting Index." February 18. www.accessnow.org/transparency-reporting-index/.

Benkler, Yochai. 2016. "Degrees of Freedom, Dimensions of Power." *Daedalus* 145 (1): 18–32.

Brooten, Lisa. 2013. "The Problem with Human Rights Discourse and 'Freedom' Indicators: The Case of Burma/Myanmar Media." *International Journal of Communication* 7: 681–700.

Budish, Ryan, Liz Woolery and Kevin Bankston. 2016. *The Transparency Reporting Toolkit: Survey & Best Practice Memos for Reporting on US Government Requests for User information.* New America, March 31. www.newamerica.org/oti/policy-papers/the-transparency-reporting-toolkit/.

Buni, Catherine and Soraya Chemali. 2016. "The Secret Rules of the Internet: The Murky History of Moderation, and How It's Shaping the Future of Free Speech." *The Verge*, April 13. www.theverge.com/2016/4/13/11387934/internet-moderator-history-youtube-facebook-reddit-censorship-free-speech.

Cardozo, Nate, Kurt Opsahl and Rainey Reitman. 2015. *Who Has Your Back? Which Companies Help Protect Your Data from the Government? The Electronic Frontier Foundation's Fifth Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data*. EFF, June 17. www.eff.org/files/2015/06/18/who_has_your_back_2015_protecting_your_data_from_government_requests_20150618.pdf.

Chen, Adrian. 2014. "The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed." *Wired*, October 23. www.wired.com/2014/10/content-moderation/.

Cooley, Alexander and Jack L. Snyder, eds. 2015. *Ranking the World: Grading States as a Tool of Global Governance.* Cambridge, UK: Cambridge University Press.

Crawford, Kate and Tarleton Gillespie. 2014. "What Is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint." *New Media & Society* 18 (3): 410–28.

Davidson, Jacob. 2015. "Ethiopian LGBT Activist Banned by Facebook Under Real Name Policy." *Money*, July 11. time.com/money/3954390/ethiopian-lgbt-activist-banned-facebook-real-name/.

Deibert, Ronald. 2016. "Cyberspace under Siege." In *Authoritarianism Goes Global: The Challenge to Democracy*, edited by Larry Jay Diamond, Marc F. Plattner and Christopher Walker, 198–215. Baltimore, MD: Johns Hopkins University Press.

de La Chapelle, Bertrand and Paul Fehlinger. 2016. *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation.* GCIG Paper Series No. 28. Waterloo, ON: CIGI. www.cigionline.org/sites/default/files/gcig_no28_web.pdf.

DeNardis, Laura. 2014. *Internet Points of Control as Global Governance.* GCIG Paper Series No. 2. Waterloo, ON: CIGI. www.cigionline.org/sites/default/files/no2_3.pdf.

———. 2015. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Drake, William J., Vinton G. Cerf and Wolfgang Kleinwächter. 2016. "Internet Fragmentation: An Overview." Future of the Internet Initiative White Paper, January. Geneva, Switzerland: World Economic Forum. www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Drozdiak, Natalia. 2016. "U.S. Tech Firms Agree to EU Code of Conduct on Terror and Hate Content." *The Wall Street Journal*, May 31. www.wsj.com/articles/u-s-tech-companies-sign-up-to-eu-code-of-conduct-on-terror-1464689959.

Dutton, William H. 2009. "The Fifth Estate Emerging through the Network of Networks." *Prometheus* 27 (1): 1–15.

European Commission. 2013. *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*. ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf.

———. 2016a. "European Commission consults on non-binding guidelines on disclosure of non-financial information by certain large companies." European Commission press release, January 15. europa.eu/rapid/midday-express-15-01-2016.htm?locale=en#5.

———. 2016b. "European Commission and IT Companies announce Code of Conduct on illegal online hate speech." European Commission press release, May 31. europa.eu/rapid/press-release_IP-16-1937_en.htm.

European Union. 2014. *Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups (Text with EEA relevance)*. Document 32014L0095. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0095.

———. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Document 32016R0679. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG.

Freedom Online Coalition. 2015. *Working Group Three: Privacy and Transparency Online Report*. London, UK: Global Partners Digital. freedomonlinecoalition.com/wp-content/uploads/2015/10/FOC-WG3-Privacy-and-Transparency-Online-Report-November-2015.pdf.

Frosio, Giancarlo F. 2016. "Digital piracy debunked: a short note on digital threats and intermediary liability." *Internet Policy Review* 5 (1). doi:10.14763/2016.1.400.

Gardiner, Matthew and Stephan Lienin. 2015. "Impact of the EU directive on Non-Financial Reporting." *Environmental Leader*, August 6. www.environmentalleader.com/2015/08/06/impact-of-the-eu-directive-on-non-financial-reporting/.

GCIG. 2016. *One Internet: Final Report of the Global Commission on Internet Governance.* Waterloo, ON: CIGI. www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf.

Giannone, Diego. 2010. "Political and ideological aspects in the measurement of democracy: the Freedom House case." *Democratization* 17 (1): 68–97.

Global Sustainable Investment Alliance. 2015. *Global Sustainable Investment Review 2014*. February. www.gsi-alliance.org/wp-content/uploads/2015/02/GSIA_Review_download.pdf.

GNI. 2012a. "Global Network Initiative Principles on Freedom of Expression and Privacy." http://globalnetworkinitiative.org/principles/index.php#22.

———. 2012b. "GNI's submission to the UN Working Group on Business and Human Rights." www.globalnetworkinitiative.org/newsandevents/GNI_s_Submission_to_the_UN_Working_Group_on_Business_and_Human_Rights.php.

———. 2015. "Governance Charter." Revised. GNI, February. globalnetworkinitiative.org/sites/default/files/GNI%20Governance%20Charter%20-%202015.pdf.

———. 2016a. "The Global Network Initiative and the Telecommunications Industry Dialogue join forces to advance freedom of expression and privacy." GNI press release, February 1. www.globalnetworkinitiative.org/news/global-network-initiative-and-telecommunications-industry-dialogue-join-forces-advance-freedom.

———. 2016b. "The Global Network Initiative Releases Public Report on the 2015/16 Independent Assessments of Facebook, Google, LinkedIn, Microsoft, and Yahoo." GNI press release, July 7. globalnetworkinitiative.org/news/global-network-initiative-releases-public-report-201516-independent-assessments-facebook-google.

———. 2016c. "Global Network Initiative and Telecommunications Industry Dialogue Joint Statement on Network and Service Shutdowns." GNI press release, July 12. globalnetworkinitiative.org/news/global-network-initiative-and-telecommunications-industry-dialogue-joint-statement-network-and.

Green, Maria. 2001. "What We Talk About When We Talk About Indicators: Current Approaches to Human Rights Measurement." *Human Rights Quarterly* 23 (4): 1062–97.

Hughes, Owen. 2016. "Twitter, Facebook and YouTube sign EU code of conduct to help combat online hate speech." *The International Business Times*, June 1. www.ibtimes.co.uk/twitter-facebook-youtube-sign-eu-code-conduct-help-combat-online-hate-speech-1563163.

Internet Live Stats. 2016a. "Internet Users." www.internetlivestats.com/internet-users/.

———. 2016b. "Internet Users by Country (2016)." www.internetlivestats.com/internet-users-by-country/.

Jeppesen, Jens-Henrik and Emma J. Llansó. 2016. "Letter to European Commission on Code of Conduct for 'Illegal' Hate Speech Online." Center for Democracy & Technology, June 3. cdt.org/insight/letter-to-european-commissioner-on-code-of-conduct-for-illegal-hate-speech-online/.

Johnston, Andrew and Paige Morrow. 2016. "Fiduciary Duties of European Institutional Investors: Legal Analysis and Policy Recommendations." www.purposeofcorporation.org/fiduciary-duties.pdf.

Kasperkevic, Jana. 2016. "Rana Plaza collapse: workplace dangers persist three years later, reports find." *The Guardian*, May 31. www.theguardian.com/business/2016/may/31/rana-plaza-bangladesh-collapse-fashion-working-conditions.

Kaye, David. 2016. *Freedom of expression and the private sector in the digital age. Report of the Special Rapporteur on freedom of expression to the Human Rights Council*. A/HRC/32/38. www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Privatesectorinthedigitalage.aspx.

Kelly, Sanja, Madeline Earp, Laura Reed, Adrian Shahbaz and Mai Truong. 2015. *Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy.* October. Washington, DC: Freedom House. https://freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf.

Kessel, Jeremy. 2016. "Providing more #transparency into legal requests to remove content." *Twitter Blog*, February 19. blog.twitter.com/2016/providing-more-transparency-into-legal-requests-to-remove-content.

Kovach, Bill and Tom Rosenstiel. 2014. *The Elements of Journalism: What Newspeople Should Know and the Public Should Expect.* 3rd ed. New York, NY: Three Rivers Press.

MacKinnon, Rebecca, Elonnai Hickok, Allon Bar and Hae-in Lim. 2014. *Fostering Freedom Online: The Role of Internet Intermediaries.* UNESCO Series on Internet Freedom. Paris, France: United Nations Educational, Scientific and Cultural Organization. unesdoc.unesco.org/images/0023/002311/231162e.pdf.

Maréchal, Nathalie. 2015. "Ranking Digital Rights: Human Rights, the Internet and the Fifth Estate." *International Journal of Communication* 9: 3440–49.

Mathews, Jessica T. 1997. "Power Shift." *Foreign Affairs* 76 (1): 50–66.

May, Christopher. 2015. "Who's in charge? Corporations as institutions of global governance." *Palgrave Communications* 1 (December): 15042. doi:0.1057/palcomms.2015.42.

McChesney, Robert Waterman. 2013. *Digital Disconnect: How Capitalism Is Turning the Internet against Democracy.* New York, NY: The New Press.

Mirzoeff, Nicholas D. 2015. "Facebook Censors Refugee Photographs." *How to See the World* (blog), September 1. https://wp.nyu.edu/howtoseetheworld/2015/09/01/auto-draft-78/.

Mosseri, Adam. 2016. "Building a Better Newsfeed for You." Facebook Newsroom, June 29. https://newsroom.fb.com/news/2016/06/building-a-better-news-feed-for-you/.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Boston, MA: The MIT Press.

Muli, Sharon. 2013. "Sustainability Rankings: Impacts on Corporate Sustainability." University of Pennsylvania Scholarly Commons. repository.upenn.edu/cgi/viewcontent.cgi?article=1053&context=mes_capstones.

Nelson, Jane. 2014. "Corporate Social Responsibility: Emerging good practice for a new era." OECD Observer No 299, Q2 2014. http://oecdobserver.org/news/fullstory.php/aid/4369/Corporate_Social_Responsibility:_Emerging_good_practice_for_a_new_era.html.

OHCHR. 2011. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect Respect and Remedy" Framework*. New York, NY: United Nations. www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

Pace, Barnaby and Oliver Courtney. 2015. "Briefing: Shell and Eni's Misadventures in Nigeria." Global Witness, November 17. www.globalwitness.org/en/campaigns/oil-gas-and-mining/shell-and-enis-misadventures-nigeria/.

Proxy Preview. 2015. "Record Number of Social and Environmental Shareholder Resolutions Filed in 2015." Proxy Preview press release, March 5. www.proxypreview.org/wp-content/uploads/2015/03/release-record-number-of-social-and-environmental-shareholder-resolutions-filed-in-2015.pdf.

———. 2016. "Record Number of Climate and Corporate Political Spending Resolutions Dominate 2016 Shareholder Votes." Proxy Preview press release, March 8. www.proxypreview.org/wp-content/uploads/2016/03/proxy_preview_release_record_number_climate_corporate_political_spending_resolutions_dominate_2016_shareholder_votes_20160308.pdf.

RDR. 2015a. *2015 Corporate Accountability Index*. Washington, DC: RDR. https://rankingdigitalrights.org/index2015/assets/static/download/RDRindex2015report.pdf.

———. 2015b. "Corporate Accountability Index." https://rankingdigitalrights.org/index2015/.

———. 2015c. "Corporate Accountability Index: All Indicators — Commitment." https://rankingdigitalrights.org/index2015/categories/commitment/.

———. 2016. "Methodology Development." Last updated September 14. https://rankingdigitalrights.org/methodology-development/.

Reporters Without Borders. 2016. "RSF deplores suspension of French journalist's Facebook account." Reporters Without Borders News, June 23. rsf.org/en/news/rsf-deplores-suspension-french-journalists-facebook-account.

Roberts, Sarah T. 2016. "Commercial Content Moderation: Digital Laborers' Dirty Work." Western Libraries Media Studies Publications 12. London, ON: Western University. ir.lib.uwo.ca/commpub/12/.

Ruggie, John Gerard. 2008. *Statement on Human Rights and Transnational Corporations and Other Business Enterprises to the 63rd Session of the General Assembly, Third Committee.* October 27. United Nations, New York. www.hks.harvard.edu/news-events/news/testimonies/john-ruggie-testimony-oct.

———. 2013. *Just Business: Multinational Corporations and Human Rights.* 1st ed. Amnesty International Global Ethics Series. New York, NY: W. W. Norton.

Sadowski, Michael. 2012. *Rate the Raters: Phase Five.* London, UK: SustainAbility. www.sustainability.com/library/rate-the-raters-phase-five.

SASB. 2016. "Technology & Communications Standards Download." www.sasb.org/standards/download/techcomm/.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* New York, NY: W. W. Norton.

Schwartz, Paul M. and Daniel J. Solove. 2011. "The PII Problem: Privacy and a New Concept of Personally Identifiable Information." *New York University Law Review* 86: 1814–94.

Taylor, Emily. 2016. *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality.* GCIG Paper Series No. 24. Waterloo, ON: CIGI. www.cigionline.org/publications/privatization-human-rights-illusions-consent-automation-and-neutrality.

Telecommunications Industry Dialogue. 2013. "Telecommunications Industry Dialogue on Freedom of Expression and Privacy: Principles." Version 1, March 6. www.telecomindustrydialogue.org/wp-content/uploads/Telecoms_Industry_Dialogue_Principles_Version_1_-_ENGLISH.pdf.

US Securities Exchange Commission. 2016. *Business and Financial Disclosure Required by Regulation S-K.* www.sec.gov/rules/concept/2016/33-10064.pdf.

White, Mary Jo. 2016. "Focusing the Lens of Disclosure to Set the Path Forward on Board Diversity, Non-GAAP, and Sustainability." Keynote address, International Corporate Governance Network Annual Conference, San Francisco, June 27. www.sec.gov/news/speech/chair-white-icgn-speech.html.

York, Jillian C. 2016. "Facebook and Twitter are getting rich by building a culture of snitching." *Quartz*, July 14. qz.com/731347/facebook-and-twitter-are-getting-rich-by-building-a-culture-of-snitching/

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89.

ABOUT THE AUTHORS

Rebecca MacKinnon is director of the Ranking Digital Rights project at New America and author of *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, 2012). She is also a founding member of the Global Network Initiative and a co-founder of Global Voices.

Nathalie Maréchal is a Ph.D. candidate at the University of Southern California's Annenberg School for Communication and Journalism and a Ranking Digital Rights senior fellow.

Priya Kumar was a research analyst with Ranking Digital Rights until August 2016 and is now a Ph.D. student at the University of Maryland's College of Information Studies.

ABOUT CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan qui formule des points de vue objectifs dont la portée est notamment mondiale. Nos recherches, nos avis et l'opinion publique ont des effets réels sur le monde d'aujourd'hui en apportant autant de la clarté qu'une réflexion novatrice dans l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

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 Finance	Shelley Boettger
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
Chief Operating Officer and General Counsel	Aaron Shull
Director of Communications and Digital Media	Spencer Tripp

Publications

Publisher	Carol Bonnett
Senior Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Sharon McCartney
Publications Editor	Lynn Schellenberg
Graphic Designer	Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.

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