CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 45 — DECEMBER 2016

Corporate Accountability for a Free and Open Internet

Rebecca MacKinnon, Nathalie Maréchal and Priya Kumar

CORPORATE ACCOUNTABILITY FOR A FREE AND OPEN INTERNET

Rebecca MacKinnon, Nathalie Maréchal and Priya Kumar

CIGI

CHATHAM HOUSE
The Royal Institute of
International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

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 conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

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

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

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

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

www.ourinternet.org

ABOUT THE AUTHORS

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.

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

EXECUTIVE SUMMARY

Private Internet intermediaries increasingly find themselves at odds with governments, with serious implications for human rights. While companies face tougher data protection and privacy laws in some jurisdictions, they also face growing legal requirements to comply with mass surveillance, weaken encryption and facilitate censorship in ways that contravene international human rights standards. In many countries, they face increasing legal liability for users' activities. Even where law does not compel companies to violate users' rights, companies generally lack sufficient market and regulatory incentives to protect the human rights of all of their users. The resulting global "governance gaps" require new types of cross-border institutions and mechanisms to strengthen companies' ability to respect users' rights and to hold firms accountable.

This paper first describes some innovative efforts that might serve as building blocks for such mechanisms and institutions. Next, it places these developments in the broader context of the evolving role of corporations in international governance and accountability systems beyond the information communications technology (ICT) sector. It then focuses on one particular accountability toolset: rankings and ratings, which, when combined with transparency and disclosure frameworks, can help to foster greater accountability as well as respect for international human rights standards. The final section focuses specifically on the Ranking Digital Rights (RDR) Corporate Accountability Index. The inaugural index, published in November 2015, ranked Internet and telecommunications companies on 31 indicators evaluating disclosed commitments, policies and practices affecting Internet users' freedom of expression and right to privacy. Key findings and initial impacts will be examined, concluding with a discussion of how such public benchmarking of companies, in concert with other initiatives and mechanisms, might foster greater corporate accountability for a free and open Internet.

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 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 paper 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, 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 paper'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 paper 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 paper) 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); in addition, 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,

[1] Millicom, Nokia, Orange, Telefónica, Telenor Group, TeliaSonera and Vodafone Group.

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, 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).

[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.

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, 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'

[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.

[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.

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 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

[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/).

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]

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.

[10] See the principles at http://ratesustainability.org/core/principles/.

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

[11] See https://lumendatabase.org.

[12] See https://business-humanrights.org/sites/default/files/documents/Kakao%20response.pdf.

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).

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.

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/.

[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.

[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.

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, September 1. wp.nyu.edu/howtoseetheworld/2015/09/01/auto-draft-78/.

Mosseri, Adam. 2016. "Building a Better Newsfeed for You." Facebook Newsroom, June 29. 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.* GCIC 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/

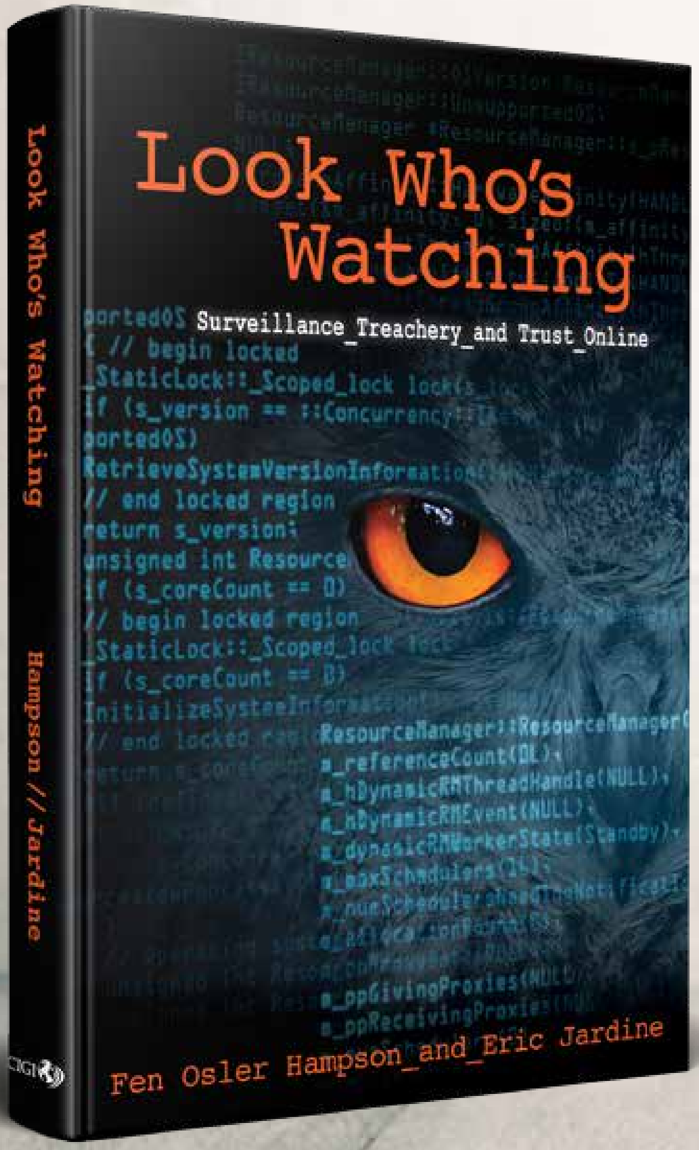
Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89.

CIGI PRESS

ADVANCING POLICY IDEAS AND DEBATE

cigionline.org

AVAILABLE NOW


Look Who's Watching
Surveillance_Treachery_and Trust_Online
Fen Osler Hampson_and_Eric Jardine
Look Who's Watching
Hampson // Jardine
CIGI

Look Who's Watching

Surveillance, Treachery and Trust Online

Fen Osler Hampson and Eric Jardine

Edward Snowden's revelations that the US National Security Agency and other government agencies are spying on Internet users and on other governments confirmed that the Internet is increasingly being used to gather intelligence and personal information. The proliferation of cybercrime, the sale of users' data without their knowledge and the surveillance of citizens through connected devices are all rapidly eroding the confidence users have in the Internet.

To meet the Internet's full potential, its users need to trust that the Internet works reliably while also being secure, private and safe. When trust in the Internet wanes, users begin to alter their online behaviour. A combination of illustrative anecdotal evidence and analysis of new survey data, *Look Who's Watching* clearly demonstrates why trust matters, how it is being eroded and how, with care and deliberate policy action, the essential glue of the Internet — trust — can be restored.

October 2016
978-1-928096-19-1 | hardcover
CDN $32 + shipping

> *The authors have produced a clear, timely and essential book about the importance of trust as an engine for the Internet. We must foster that trust if the global Internet is to continue to flourish.*
>
> — Michael Chertoff, Executive Chairman and Co-Founder, Chertoff Group, and former secretary of the US Department of Homeland Security

Centre for International Governance Innovation

CIGI Press books are distributed by McGill-Queen's University Press (mqup.ca) and can be found in better bookstores and through online book retailers.

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

Global Commission on Internet Governance

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

Global Commission on Internet Governance Paper Series

Global Commission on Internet Governance

The Regime Complex for Managing Global Cyber Activities

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Centre for International Governance Innovation
www.cigionline.org

CIGI PUBLICATIONS

ADVANCING POLICY IDEAS AND DEBATE

The Tor Dark Net
GCIG Paper Series No. 20
Gareth Owen and Nick Savage

The Dark Web Dilemma: Tor, Anonymity and Online Policing
GCIG Paper Series No. 21
Eric Jardine

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

Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity
GCIG Paper Series No. 23
Samantha Bradshaw

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

The Digital Trade Imbalance and Its Implications for Internet Governance
GCIG Paper Series No. 25
Susan Ariel Aaronson

A Pragmatic Approach to the Right to Be Forgotten
GCIG Paper Series No. 26
Kieron O'Hara, Nigel Shadbolt and Wendy Hall

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

Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation
GCIG Paper Series No. 28
Bertrand de La Chapelle and Paul Fehlinger

Patents and Internet Standards
GCIG Paper Series No. 29
Jorge L. Contreras

Tracing the Economic Impact of Regulations on the Free Flow of Data Localization
GCIG Paper Series No. 30
Matthias Bauer, Martina F. Ferracane and Erik van der Marel

Looking Back on the First Round of New gTLD Applications: Implications for the Future of Domain Name Regulation
GCIG Paper Series No. 31
Jacqueline D. Lipton

Governance of International Trade and the Internet: Existing and Evolving Regulatory Systems
GCIG Paper Series No. 32
Harsha Vardhana Singh, Ahmed Abdel-Latif and L. Lee Tuthill

Market-driven Challenges to Open Internet Standards
GCIG Paper Series No. 33
Patrik Fältström

How to Connect the Other Half: Evidence and Policy Insights from Household Surveys in Latin America
GCIG Paper Series No. 34
Hernán Galperin

A Framework for Understanding Internet Openness
GCIG Paper Series No. 35
Jeremy West

Internet Openness and Fragmentation: Toward Measuring the Economic Effects
GCIG Paper Series No. 36
Sarah Box

Why Are Two Networks Better than One? Toward a Theory of Optimal Fragmentation
GCIG Paper Series No. 37
Christopher S. Yoo

One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation
GCIG Paper Series No. 38
Laura DeNardis

Ethics in the Internet Environment
GCIG Paper Series No. 39
Rolf H. Weber

Standards, Patents and National Competitiveness
GCIG Paper Series No. 40
Michael Murphree and Dan Breznitz

Multi-stakeholderism: Anatomy of an Inchoate Global Institution
GCIG Paper Series No. 41
Mark Raymond and Laura DeNardis

Internet Intermediaries as Platforms for Expression and Innovation
GCIG Paper Series No. 42
Anupam Chander

Unlocking Affordable Access in Sub-Saharan Africa
GCIG Paper Series No. 43
Steve Song

Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study
GCIG Paper Series No. 44
Caroline Baylon and Albert Antwi-Boasiako

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

CIGI

Centre for International Governance Innovation
www.cigionline.org

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	Sara Moore
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
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