Progress and peril: the role of ICT companies in promoting and curtailing human rights

Priya Kumar[1], Revati Prasad[2] & Nathalie Maréchal[3]

Abstract

The 2030 Agenda for Sustainable Development highlights the centrality of information and communications technology (ICT) to 21st century development. Tools like e-learning, "smart infrastructure," service delivery databases, and mobile devices hold great potential to help meet the Sustainable Development Goals (SDGs) through partnerships between national governments and private companies. Any strategy for the use of ICTs to promote human rights and development must acknowledge that private entities develop most ICTs. Such companies help people access information, conduct business, and connect with others, but their role as gatekeepers also makes them choke points, particularly related to freedom of expression and privacy. Although ICT companies have taken steps to provide greater insight about how their actions affect human rights, far more transparency is needed hold these companies to account. If the SDGs are to "realize human rights for all," it is imperative that ICT for development (ICT4D) projects take steps to mitigate the risks that come from using ICTs. These technologies pose particular threats to privacy and freedom of expression, which jeopardizes people's ability to advocate for human rights more broadly without fear of reprisal. This article outlines the human rights risks of increased use of ICTs and offers a framework for private sector and government actors to mitigate them. While acknowledging the real and potential benefits of increased ICT use in advancing development and human rights, the article provides examples of threats to human rights that stem from the policies and practices of ICT companies. It concludes with specific recommendations for companies and guidance for governments that seek to influence the private sector in this regard. Notably, it calls for governments and donors to exercise due diligence in evaluating companies' commitment to human rights when choosing private sector partners for ICT4D projects.

Keywords**:** information and communications technology; human rights; freedom of expression; privacy; private sector.

1 College of Information Studies, University of Maryland.
2 Annenberg School for Communication, University of Pennsylvania.
3 Annenberg School for Communication and Journalism, University of Southern California.

I. Introduction

The 2030 Agenda for Sustainable Development sets forth an ambitious plan to profoundly improve the lives of people around the world. By including an explicit call to "realize the human rights of all", the Agenda foregrounds a rights-based approach to development. Each of the 17 Sustainable Development Goals (SDGs) corresponds to human rights enshrined in international law and treaties. For instance, Goal 2 (to end hunger) finds its human rights counterpart in the right to adequate food, and Goal 10 (to reduce inequality within and among countries, including promoting social, economic and political inclusion) draws upon the right to equality and non-discrimination and the right to participate in public affairs.[4]

The 2030 Agenda highlights the centrality of information and communications technology (ICT) to serve as a catalyst in enacting this vision of development. Goal 17 directly references ICT's ability to overcome the digital divide and spur knowledge economies. Other goals, including those aimed at education (Goal 4), gender balance (Goal 5) and "smart infrastructure" (Goal 9), also acknowledge ICTs, from mobile devices to e-learning, as powerful tools to help meet the SDGs. National governments will lead the implementation of the SDGs in partnership with private enterprise; indeed, the 2030 Agenda calls upon the private sector to support and amplify these efforts.

The 2030 Agenda employs an instrumental view of ICTs and the private sector; they are a means to the end of sustainable development. In this formulation, businesses drive economic growth, and ICTs are tools to accelerate and magnify reach and impact. The Agenda does consider the rights implications of the private sector in terms of labour and environmental impact, but it does not take into account how technology companies themselves can secure or subvert people's human rights, specifically the critical rights to freedom of expression and privacy. The exercise of these two rights is the cornerstone of civil society; lacking them, individuals cannot advocate for their human rights (or those of others) without fear of reprisal. While universal, these rights are not absolute; governments can and do balance these rights with other interests in accordance with international human rights law.[5] However, not all such limitations are compatible with human rights, and this article provides examples of cases where ICT companies unduly violate the rights to free expression, privacy, or both.

This article focuses on the intersection of the ICT sector and human rights. It begins by examining the critical role that policies and practices of ICT companies

4 A/RES/217 (III) A Articles 25, 2, 21.

5 A detailed legal analysis of the limitations of these rights falls beyond the scope of this article.

play in either advancing or hindering human rights, whether these policies and practices were developed of a company's own accord or in response to national laws. These companies have the greatest impact on the right to information and expression, as articulated in Article 19 of the Universal Declaration of Human Rights (UDHR), and on the right to privacy, as presented in Article 12. This article provides examples of how company actions can curtail, rather than respect, these rights. Because this action disproportionately affects vulnerable and marginalized populations, this article also addresses the UDHR's Article 2, the right to equality and non-discrimination, and Article 21, the right to participate in public affairs.

It then describes several norms-based frameworks to foster greater accountability among ICT companies to respect human rights. The rule of law is, of course, an essential component of human rights promotion, yet it is often insufficient. This is particularly true in the ICT sector, where technology and practice tend to move faster than the law. Moreover, smaller and less-developed countries often struggle to enforce laws that aim to regulate wealthy and powerful multinational corporations, and all too frequently laws directly compel ICT companies to violate or facilitate the violation of human rights.[6] The last section of this article offers recommendations for companies and for governments who seek to push companies to better respect their users' human rights. The conclusion connects these recommendations directly to the SDGs.

II. How ICT Companies Can Put Human Rights at Risk

In June 2016, the UN Human Rights Council recognized the global and open Internet as a driving force towards development and asserted that the "same rights that people have offline must also be protected online".[7] It acknowledged the importance of the Internet in meeting the SDGs and explicitly emphasized the need to protect freedom of expression and privacy rights in the march toward a more digitally connected world.

The council also highlighted the critical role of companies in ensuring that people can exercise these rights. Private-sector entities typically own and operate the infrastructure that enables digital communication. For-profit ICT companies, which include Internet service providers, search engines, social media sites, blogging platforms, and cloud computing services, exercise immense power over the global flow of information.

6 Rebecca MacKinnon and others, *Fostering freedom online: The role of Internet intermediaries* (Paris, France, UNESCO, 2014).

7 A/HRC/32/L.20, para. 1.

These Internet intermediaries, or "third-party platforms that mediate between digital content and the humans who contribute and access this content", serve as gatekeepers to the online world, and consequently can also act as choke points.[8] Heralded as "liberation technologies"[9] for their ability to open new spaces for expression and interaction, they can also serve as critical points of control where state actors can surveil or censor communication and suppress the rights of people across the globe.[10]

Despite their border-spanning character, ICT companies are often bound by the laws of the countries in which they operate.[11] For instance, Google blocks access to Nazi content in Germany and Austria pursuant to those countries' hate crime laws. However, companies may also contest the legality of government requests. Apple's resistance to decrypt an iPhone in response to a court order obtained by the US Federal Bureau of Investigation is only one such example.[12]

Internet intermediaries make public policy through decisions about what they do and do not permit on their platforms. For example, Facebook's community standards prohibit hate speech, but permit "humour, satire, or social commentary related to these topics".[13] Facebook establishes these rules and determines how to enforce them, and users have no mechanism to appeal if the company removes

8 Laura DeNardis, *The global war for Internet governance* (New Haven, Connecticut, Yale University Press, 2015), p. 154.

9 Jon Diamond, "Liberation technology", *Journal of Democracy,* vol. 21, No. 3 (2010); John Postill, "Freedom technologists and the new protest movements: A theory of protest formulas", *Convergence: The International Journal of Research into New Media Technologies,* vol. 20, No. 4 (2014) doi:10.1177/1354856514541350.

10 Ronald Deibert, *Black code: Inside the battle for cyberspace* (Toronto, Canada: McClelland & Stewart, 2013); Laura DeNardis, *The global war*, supra note 8; Rebecca MacKinnon, *Consent of the networked: The world-wide struggle for Internet freedom* (New York City, New York: Basic Books, 2012); Evgeny Morozov, *The net delusion: The dark side of Internet freedom* (New York City, Public Affairs, 2011).

11 Bertrand de La Chapelle and Paul Fehlinger, "Jurisdiction on the Internet: From legal arms race to transnational cooperation", *Global Commission on Internet Governance Paper Series*, No. 28 (Waterloo, Canada, Centre for International Governance Innovation and Chatham House, April 2016). Available from https://www.cigionline.org/publications/jurisdiction-internet-legal-arms-race-transnational-cooperation; Milton Mueller, *Networks and states: The plobal politics of Internet governance* (Boston, Massachusetts: The MIT Press, 2010).

12 Eric Lichtblau, "In Apple debate on digital privacy and the iPhone, questions still remain", *New York Times*, 28 March 2016. Available from http://www.nytimes.com/2016/03/29/us/politics/in-apple-debate-on-digital-privacy-and-the-iphone-questions-still-remain.html?_r=0.

13 Facebook defines hate speech as including, "content that directly attacks people based on their: race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, or gender identity, or serious disabilities or diseases". See Facebook, "Encouraging respectful behavior: Hate speech", 4 November 2016. Available from https://www.facebook.com/communitystandards/#.

their content.[14] Such "sovereigns of cyberspace" shape online discourse through their terms of service and privacy policies, to which users must agree.[15] As intermediaries, these companies facilitate the flow of information, knowledge, and personal data, which means that people increasingly depend on these companies as they exercise their human rights.

Moreover, the SDGs call for gender equality and implicitly acknowledge the need to reduce discrimination that can prevent marginalized populations from fully enjoying their rights.[16] While ICTs can support these goals, such efforts must confront the fact that discrimination and inequality occur online as well. Internet access remains gendered and inhibits women from being able to enjoy the many positive effects of the Internet.[17] Women who are online often experience the Web as an unsafe space, from women in Pakistan facing blackmail over doctored photos[18] to prominent feminist bloggers like Anita Sarkeesian and Jessica Valenti enduring hate speech and threats of violence.[19]

Internet intermediaries like Facebook and Twitter have become arbiters that must balance the expressive liberty of some users with the need to protect others from harm. These companies have faced criticism for their response to threats against women. One study on technology-related violence against women found that ICT companies hesitate to address the issue until it garners media attention, and that their responses fail to consider the experiences of non-Western women.[20] Vague definitions of terms such as "harassment" or "vulnerable individual" leave users wondering how policies apply in specific cultural contexts. For example, Facebook lacked mechanisms to evaluate hate speech in Urdu or Pashto, let

14 Facebook, "I believe my content was removed in error", 4 November 2016. Available from https://www.facebook.com/help/780814295267977.

15 Rebecca Mackinnon, *Consent of the networked*... supra note 10, p. 114.

16 A/RES/70/1.

17 International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization, *Doubling digital opportunities: Enhancing the inclusion of women & girls in the information society: A report by the Broadband Commission Working Group on Broadband and Gender* (Geneva, Switzerland, 2013). Available from http://www.broadbandcommission.org/documents/working-groups/bb-doubling-digital-2013.pdf.

18 Simon Parkin, "Pakistan's troll problem", *New Yorker*, 28 June 2016. Available from http://www.newyorker.com/tech/elements/pakistans-troll-problem.

19 Jessica Valenti, "Anita Sarkeesian interview: 'The word "Troll" feels too childish. This is abuse.'" *Guardian*, 29 August 2015. Available from https://www.theguardian.com/technology/2015/aug/29/anita-sarkeesian-gamergate-interview-jessica-valenti; Lyz Lenz, "Inside the psyche of a troll who threatens a child." *Daily Dot*, 3 August 2016. Available from http://www.dailydot.com/irl/jessica-valenti-online-threats/.

20 Carly Nyst, "Internet intermediaries and violence against women: Online executive summary and findings", *End Violence: Women's Rights and Safety Online* (Association for Progressive Communications, 2014). Available from http://www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf.

alone respond to it.[21] In a leaked staff memo, Twitter's CEO acknowledged the company's struggle to counter abuse and harassment on its platform.[22] Technologically mediated violence against women inhibits women's ability to speak freely, fully participate online, and engage socially and politically.

The digital space is also fraught for minorities such as the LGBT community. Online spaces can provide a platform for identity exploration and expression,[23] but DeNardis and Hackl show how these spaces can serve as "control points over LGBT speech, identity expression, and community formation".[24] They document instances where rules established in proprietary digital systems impact LGBT issues; for example, Nintendo's real-life simulation game Tomodachi Life did not allow same-sex relationships. Facebook's real name or "authentic identity" requirement has resulted in the termination of several drag queens' accounts, limiting these users' ability to navigate a multi-faceted identity and manage their professional and personal relationships online.[25]

While gaming or social media platforms can make technical and design decisions that limit LGBT users from expressing their identity, the data such platforms collect can also expose users to significant harm. For example, Egyptian activists raised concerns that police used the dating app Grindr to track down and arrest gay men on charges of debauchery and indecency. Grindr ultimately changed its default settings to hide the distance of users in countries such as Russia, Egypt, and Saudi Arabia, which have strong anti-LGBT laws.[26]

Beyond affecting marginalized populations, ICT companies can be conscripted to serve as blunt political weapons that undermine the political and civil rights of citizens *en masse*. During political turmoil, governments increasingly order ICT companies to block specific applications or shut down entire communications networks. The digital rights organization Access Now recorded at least 15

21 Simon Parkin, *Pakistan's troll...* supra note 18.

22 Charlie Warzel, "A honeypot for assholes': Inside Twitter's 10-year failure to stop harassment", *Buzzfeed*, 11 August 2016. Available from https://www.buzzfeed.com/charliewarzel/a-honey-pot-for-assholes-inside-twitters-10-year-failure-to-s?utm_term=.qgYzVJ4BL#.rrZWe6GEl.

23 Mary L. Gray, "Negotiating identities/queering desires: Coming out online and the remediation of the coming-out story", *Journal of Computer-Mediated Communication*, vol. 14, No. 4 (2009), doi:10.1111/j.1083-6101.2009.01485.x.

24 Laura DeNardis and Andrea M. Hackl, "Internet control points as LGBT rights mediation", *Information, Communication & Society*, vol. 19 No. 6 (2016), doi:10.1080/1369118X.2016.1153123, p. 753.

25 Jessa Lingel and Adam Golub. "In face on Facebook: Brooklyn's drag community and socio-technical practices of online communication", *Journal of Computer-Mediated Communication*, vol. 20, No. 5 (2015), doi:10.1111/jcc4.12125.

26 Laura DeNardis and Andrea Hackl, *Internet control...*supra note 24.

Internet shutdowns around the world in 2015, and it recorded 51 shutdowns in the first 10 months of 2016.[27] The UN Human Rights Council has condemned network shutdowns that violate international human rights law.[28]

While many shutdowns coincide with elections or political protests, governments have deployed the tactic for far more quotidian reasons. The Algerian government acknowledged that it blocked access to Facebook, Twitter, and other social media sites to prevent high school students from cheating during national exams,[29] and leaders in the Indian state of Jammu and Kashmir shut down Internet service before a local wrestling match.[30] Not only do such actions restrict citizens' ability to communicate and participate politically, as Goal 16.7 aims to ensure, but they also offer a cover of darkness for further human rights violations.

Governments often adopt a more targeted approach to restricting speech online by blocking and removing online content. States can request ICT companies to remove content to comply with laws against defamation, blasphemy, pornography, or state secrets. Such requests can also silence political opposition. Restrictive intermediary liability laws that hold ICT companies liable for their users' online activities, such as those in China, incentivize companies to proactively monitor and remove content on their platforms. One study of Weibo, China's most popular microblogging service found approximately 16 percent of all messages was deleted.[31]

These "arbiters of online expressive liberty"[32] can censor content when governments compel them; they can also remove or block content that violates their own policies. Users whose actions do not align with the policies of such dominant ICT companies as Google, Apple, or Facebook have few, if any alternatives. For example, Google and Apple hold a duopoly over mobile operating systems and the app stores through which most mobile users download software. Most Google Android users install applications through the Google Play Store, and Apple iOS users must go through Apple's App Store. Each company retains discretionary control over the third-party apps available

27 AccessNow, "#KeepItOn", 28 November 2016. Available from https://www.accessnow.org/keepiton/.

28 A/HRC/32/L.20, para. 10.

29 Patrick Markey, "Algeria blocks Facebook, Twitter to stop exam cheats: State media", *Reuters*, 19 June 2016. Available from http://www.reuters.com/article/us-algeria-media-idUSKCN0Z50JX.

30 Peerzada Ashiq, "Jammu goes offline ahead of controversial wrestling event", *Hindu*, 22 June 2016. Available from http://www.thehindu.com/news/national/other-states/jammu-goes-of-fline-ahead-of-controversial-wrestling-event/article8756852.ece.

31 David Bamman, Brendan O'Connor and Noah Smith, "Censorship and deletion practices in Chinese social media", *First Monday*, vol. 17, No. 3 (2012), dx.doi.org/10.5210/fm.v17i3.3943.

32 Laura DeNardis, *The global war*... supra note 8, p.157.

in its app store. Companies may decide to block an app for various reasons, for example, because it promotes violence or bigotry, or because it espouses unpopular speech.[33] While Google and Apple publicly state what is and is not permitted in the app store, neither publishes any information about how they evaluate apps or enforce their policies.

ICT companies hold a wealth of user information, and their policies regarding the management of such information directly affects users' rights. Many ICT companies generate revenue by collecting and aggregating information about their users and sharing it with advertisers. Such collection and sharing of data occurs under the auspices of online advertising, but it also facilitates government surveillance on and offline. For instance, people in India must provide official identification to use a cybercafé, and cybercafé operators must retain this information for a year.[34] These identification mechanisms put users' privacy at risk, and this loss of anonymity can impact their freedom of expression. Indeed, awareness of surveillance has demonstrable chilling effects on speech.[35]

While privacy laws seek to mitigate the harm of such data collection, they often struggle to keep up with technology. Many laws hinge on the notion that if one can obscure or remove personal identifying information (PII), "there is no privacy harm."[36] Yet the proliferation of user information online means that seemingly innocuous data points can be aggregated and analysed in a way that identifies individual users, suggesting that laws focused on the removal of PII are ill-equipped to protect people's privacy.[37]

III. How to Hold ICT Companies Accountable

Over the past decade, several accountability frameworks grounded in human rights norms and principles have arisen to address these concerns. While corporate social responsibility (CSR) emphasizes self-regulation among companies, the corporate accountability movement "implies both a measure of answerability (providing an account for measures undertaken) and enforceability (punishment

33 Ibidem.

34 Ibidem.

35 Elizabeth Stoycheff, "Under surveillance: Facebook online spiral of silence effects in the wake of NSA Internet monitoring", *Journalism and Mass Communication Quarterly,* vol. 93, No. 2 (2016).

36 Paul M. Schwartz and Daniel J. Solove, "The PII problem: Privacy and a new concept of personally identifiable information", *New York University Law Review*, vol. 86, (2011), p. 1816.

37 Paul Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA Law Review*, vol. 57, (2010).

or sanctions for poor performance or illegal conduct)".[38] Entities of the UN have acknowledged that businesses face obligations related to human rights. Efforts like the Global Network Initiative and Ranking Digital Rights apply these obligations to ICT companies. These efforts help address "governance gaps" that arise when laws do not adequately protect human rights.[39]

In June 2011, the UN Human Rights Council endorsed the Guiding Principles on Business and Human Rights,[40] which affirm that states have a duty to protect human rights, businesses have a duty to respect human rights, and both have an obligation to provide remedy for individuals whose human rights are violated. The Guiding Principles are a norms-based instrument to foster greater accountability among governments and businesses with regard to human rights. This approach has faced criticism because it lacks the legal force of a binding instrument like a treaty.[41] The Guiding Principles by no means represent a complete solution to align corporate actions with human rights. But they do offer a structure through which companies can institutionalize efforts to respect human rights, and through which their efforts can be compared. To advance this work, the Office of the High Commissioner for Human Rights published an implementation guide for the principles.[42] Six multinational companies are pilot testing a framework for reporting on their implementation of the Guiding Principles; others can self-report their progress to a publicly available database.[43]

38 Peter Newell, "From responsibility to citizenship?: Corporate accountability for development", *IDS Bulletin,* vol. 33, No. 2 (2002), p. 2. For more information, see Renginee G. Pillay, "The limits to self-regulation and voluntarism: From corporate social responsibility to corporate accountability", *Amicus Curiae*, No. 99 (Autumn 2014) and Carmen Valor, "Corporate social responsibility and corporate citizenship: Towards corporate accountability", *Business and Society Review*, vol. 110, No. 2 (2005).

39 For a discussion of these frameworks, see Rebecca MacKinnon, Nathalie Maréchal and Priya Kumar, "Corporate accountability for a free and open Internet", *Global Commission on Internet Governance Paper Series* (Waterloo, Canada, Centre for International Governance Innovation and Chatham House, December 2016). Available from https://www.cigionline.org/publications/corporate-accountability-free-and-open-internet.

40 A/HRC/RES/17/L.17/Rev.1, para. 1.

41 Penelope Simons, "International law's invisible hand and the future of corporate accountability for violations of human rights", *Journal of Human Rights and the Environment*, vol. 3, No. 1 (March 2012).

42 United Nations, Office of the High Commissioner on Human Rights, *Guiding principles on business and human rights: Implementing the United Nations "Respect, Protect and Remedy" framework*. (Geneva, Switzerland, 2011). Available from http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

43 The companies are Unilever, Ericsson, H&M, Nestlé, Newmont, and Abn-Amro. Shift and Mazars. (2016). "UN guiding principles reporting framework". Available from http://www.ungpreporting.org/.

With respect to the ICT industry, the European Commission sponsored the development of a guidebook on how ICT companies can implement the Guiding Principles.[44] In 2008, the Global Network Initiative (GNI) formed as a multi-stakeholder venue to protect and advance users' rights to free expression and privacy within the ICT industry. As discussed in the introduction, ICT companies play a unique role in facilitating these rights, which are essential for defending and promoting human rights more broadly. The GNI's mandate focuses on respect for human rights in the face of increasing government pressure to engage in censorship and surveillance.

Member companies agree to uphold the GNI Principles on Freedom of Expression and Privacy, which are based on international human rights standards.[45] They include commitments to narrowly interpret government requests for content restriction or access to user information, to consider human rights within decision-making frameworks, to engage with various types of stakeholders, and to provide transparency into their implementation of the principles. Every two years, an independent assessor vetted by the GNI board evaluates companies on their implementation of the principles, and the GNI board determines whether each company complies with the principles.

The GNI's multi-stakeholder approach means its decisions and actions are vetted by individuals who represent various perspectives and operate under different incentives. For example, investors, who seek to maximize their returns, want to ensure that companies manage risk appropriately, while those in civil society, who work to defend and advance human rights, want to ensure that companies address the concerns of marginalized users. The GNI's board includes representatives from companies, investment organizations, civil society, and academia, and thus its decisions represent consensus among various types of participants.

The GNI's company assessments are currently the only systematic audit framework that evaluates how ICT companies have met their human rights responsibilities. But their voluntary nature means the GNI on its own cannot hold

44 European Commission, *ICT sector guide on implementing the UN Guiding Principles on Business and Human Rights*. (Brussels, 2013). Available from https://ec.europa.eu/anti- trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf.

45 For more information, see Global Network Initiative, *Principles* (November 6, 2016). Available from http://globalnetworkinitiative.org/principles/index.php.

the industry accountable; only member companies are assessed.[46] In addition, the GNI's focus on government actions related to censorship, surveillance, and access to user information addresses only one facet of the challenge to protect human rights online. It does not include the involvement of private entities, such as individuals or organizations focused on the removal of material that may infringe copyright, nor a company's own actions that can undermine or imperil users' freedom of expression or privacy, such as the conditions laid out in company terms of service or privacy policy documents.[47]

As described earlier in this article, governments and ICT companies can act in ways that contravene human rights. While governments increasingly order telecommunications companies to shut down mobile and Internet access or request companies to restrict content and turn over user information, companies themselves also design product features and develop policies and processes that can put human rights at risk. Companies determine how they respond to reports of harassment on their platform, set policies for whether users can participate in the platform anonymously, establish the parameters for what content and actions are permitted on the platforms, and assign default settings on the platform. The technical features, design decisions, and policy choices embedded in ICTs also significantly affect users' security, a crucial consideration for high-risk users such as journalists, human rights defenders, or political dissidents.

Understanding the extent to which freedom of expression and privacy rights are protected online means navigating a complex ecosystem that includes companies, investors, governments, policymakers, civil society, advocates, and activists. To provide greater clarity on the role that companies play in this ecosystem, the Ranking Digital Rights (RDR) project developed a methodology to evaluate ICT companies and their public disclosure related to policies and practices that affect freedom of expression and privacy online.[48] In 2015, RDR released its inaugural Corporate Accountability Index, which evaluated sixteen of the world's largest Internet and telecommunications companies against 31

46 The five company members of GNI are: Facebook, Google, LinkedIn, Microsoft, and Yahoo. In February 2016, seven member companies from the Telecommunications Industry Dialogue, an industry organization that explores the role of telecommunications companies in respecting freedom of expression and privacy rights, joined GNI as observers. This gives them 12 months to understand GNI's operations and participate before deciding on full membership. For more information, see Global Network Initiative, "The Global Network Initiative and the Telecommunications Industry Dialogue join forces to advance freedom of expression and privacy", 1 February 2016. Available fromhttps://www.globalnetworkinitiative.org/news/global-network-initiative-and-telecommunications-industry-dialogue-join-forces-advance-freedom.

47 Rebecca MacKinnon, Nathalie Maréchal, and Priya Kumar, *Corporate accountability...,* supra note 39.

48 The three authors of this article are current or past members of the RDR project team.

indicators. The project plans to publish the second edition of the index in 2017 and to release annually after that. By publicly evaluating companies against each other, RDR incentivizes companies to provide transparency into how their business processes affect users' free expression and privacy rights. This in turn gives investors, civil society, policymakers, and others baseline information they can use to hold companies accountable for their respect of these human rights.

The index methodology is based on international human rights standards, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Guiding Principles and the GNI Principles. The methodology was developed in consultation with stakeholders from companies, investment organizations, civil society, and academia. The index report includes examples where laws and regulations in a company's headquarters country may hinder the company from performing well. This helps to clarify where advocacy campaigns and other types of pressure are best directed at companies, and where such efforts could be more effective when directed at policymakers and governments. The index methodology and raw data are publicly available for others to adapt and analyse.[49]

ICT companies face increasing pressure from governments to act in ways that undermine, rather than protect, human rights. And where laws may not be barriers, companies frequently lack market or regulatory incentives to respect their users' human rights. The Guiding Principles, the GNI, and RDR exemplify innovative efforts to push companies to heed their human rights responsibilities. These efforts do not operate under the force of law or regulation; rather they harness the power of norms to promote accountability where the law has failed to do so. Their evaluations shed light on where companies stand, offer a roadmap on how they can improve, and instil an expectation of regular assessment to monitor company progress. This is not to say that legal and regulatory reform, litigation, or a binding treaty are unnecessary. Rather, norm-based accountability initiatives represent an avenue to effect incremental change while also fighting for human rights on other fronts.[50]

49 For the 2017 index methodology, see Ranking Digital Rights, "2017 Indicators", 14 September 2016. Available from https://rankingdigitalrights.org/2017-indicators/. For the raw data from the 2015 index, see Ranking Digital Rights, "Download the data", 6 November 2016. Available from https://rankingdigitalrights.org/index2015/download/.

50 For more information about the challenges of pursuing a binding treaty on business and human rights, see John Gerard Ruggie, *Just business: Multinational corporations and human rights* (New York City, New York, W. W. Norton & Company, 2013).

IV. How ICT Companies Can Better Respect Human Rights

This article has described the human rights risks associated with ICTs and traced the development of global frameworks to hold ICT companies accountable for respecting human rights. SDG 9.c aims to significantly increase access to ICTs in the next 15 years. This section describes specific measures that ICT companies can take to ensure that this increased access does not compromise users' rights.[51]

A. Clearly communicate company policies to users

ICTs make it easier for users to communicate with each other across time and distance. However, companies should also communicate with their own users in a clear, accessible, and organized way, notably by improving their terms of service and privacy policies. These policies dictate what users can do on the platform and outline company practices regarding the collection, use, sharing, and retention of user information. Companies require users to agree to these terms; anyone who disagrees with them has little option but to avoid using the platform. While many policies take this to represent user consent, in practice, it creates the illusion of consent.[52] Significant work remains to improve this process, but at an absolute minimum, companies should make their policies publicly available and provide translations in the languages commonly spoken by users. In addition, companies should provide users meaningful notice and documentation of changes to these policies.

Laws sometimes require companies to act in ways that put human rights at risk, for instance, by censoring speech or shutting down a network. Companies should explain, in a way that users can understand, what laws and regulations affect users' freedom of expression and privacy in the jurisdictions where they operate. These explanations should describe how companies comply with those laws and what that compliance means for users.

Companies should also clearly explain how they collect, use, share, and retain information from their users. Users should be able to understand what information about them the company collects; when and how it collects that information; whether the collection is optional; what information about users the company shares, with whom, and why; whether the sharing is optional; whether users can

51 Ranking Digital Rights, "2015 corporate accountability index", November 2015. Available from https://rankingdigitalrights.org/index2015/assets/static/download/RDRindex2015report.pdf.

52 Emily Taylor, "The privatization of human rights: Illusions of consent, automation and neutrality", *Global Commission on Internet Governance Paper Series*, No. 24 (Waterloo, Canada, Centre for International Governance Innovation and Chatham House, January 2016). Available from https://www.cigionline.org/sites/default/files/gcig_no24_web_2.pdf, p. 6.

access their own information; for how long the company retains information about users; and whether and how it destroys information after users delete their accounts or cancel their service.

B. Institutionalize human rights commitments throughout the company

Beyond making public commitments to respect users' rights, companies should also disclose evidence that they have institutionalized these commitments, for example by incorporating human rights into employee training and maintaining a whistle-blower program through which employees can report concerns related to how the company treats its users' freedom of expression and privacy rights. This bolsters confidence that companies will honour and implement such commitments even when leaders come and go.

One of the most meaningful steps companies can take is to regularly conduct human rights risk assessments (HRIAs) to determine how their products, services, and business operations affect freedom of expression and privacy. Such assessments are particularly salient when companies plan to enter new markets or appeal to new groups of users, as the human rights risks people face vary based on national and cultural context. The 2030 Agenda calls for all people, irrespective of age, gender, or any vulnerable or marginalized status, to participate fully in society, and an HRIA is one tool to help companies understand how to mitigate any risks that people from marginalized populations face when using their technologies.

While it would be counterproductive for companies to publish all details of their assessment processes and findings[53] several companies disclose information about the fact that they conduct assessments, as well as basic information about the scope, frequency, and use of these assessments. If business operations are not compatible with respect for human rights, companies may need to divest from certain markets. For example, the Swedish telecommunications operator TeliaSonera began conducting HRIAs in 2013 after controversies concerning its subsidiaries' involvement in political repression in Belarus and corruption scandals in Azerbaijan and Uzbekistan.[54] In 2015, TeliaSonera announced that it was exiting the Eurasian market. Since then, the company has made several

53 For example, the HRIA process often involves consultations with civil society organizations that have relevant expertise on human rights situations in a given country. Publicizing such contacts may put those organizations at risk.

54 Business & Human Rights Resource Centre, "NGO alleges TeliaSonera contributing to repression in Belarus", 16 September 2009. Available from https://business-humanrights.org/en/ngo-alleges-teliasonera-contributing-to-repression-in-belarus; Business & Human Rights Resource Centre, "NGO alleges TeliaSonera pulls out of Eurasia market because of corruption scandals in Azerbaijan & Uzbekistan; Company responds", 9 October 2015. Available from https://business-humanrights.org/en/ngo-alleges-teliasonera-pulls-out-of-eurasia-market-because-of-corruption-scandals-in-azerbaijan-uzbekistan-company-responds.

public statements supporting users' rights in relation to legal developments in Moldova and Tajikistan, and an Internet shutdown in Kazakhstan.[55] The company also committed to carrying out further HRIAs in Eurasia to integrate human rights in the divestment process and provide recommendations to the operating companies' current and future owners on how to manage and mitigate human rights impacts.[56]

C. Provide transparency on the extent to which companies restrict content and release user information

Companies should improve transparency regarding all types of third-party requests they receive to restrict content or share user information. These include requests from government agencies, law enforcement, courts, private entities or individuals. For example, a private entity can request a website to remove content that infringes copyright, or a law enforcement agency can request access to real-time user information to police a social movement. Such transparency reporting on government requests for user information has already become a standard practice across the ICT industry. As of early 2016, 61 ICT companies had issued at least one transparency report disclosing a range of information about requests from governments, courts, and other entities to restrict content or share user information.[57] These reports may include the number of requests, how often companies comply, and the processes companies follow when deciding how to respond to requests.

Likewise, companies should also disclose meaningful information about the volume and nature of content and/or accounts that companies themselves restrict when enforcing their terms of service. While best practices regarding the optimal

55 Telia Company, "Respecting freedom of expression: Telia company view on new legislation in Moldova", 25 April 2016. Available from http://www.teliacompany.com/en/newsroom/news/news/news-articles/2016/respecting-freedom-of-expression--telia-company-view-on-new-legislation-in-moldova/; Telia Company, "Respecting freedom of expression: Information about and Telia company view on new legislation in Tajikistan", 8 June 2016. Available from http://www.teliacompany.com/en/newsroom/news/news/news-articles/2016/respecting-freedom-of-expression--information-about-and-telia-company-view-on-new-legislation-in-tajikistan; Telia Company, "Respecting freedom of expression: Recent major event as to service limitations in Kazakhstan, June 2016", 1 July 2016. Available from http://www.teliacompany.com/en/newsroom/news/news/news-articles/2016/Respecting-Freedom-of-Expression-Recent-major-event-as-to-service-limitations/.

56 TeliaSonera," Human rights impact assessments: Focus on region Eurasia", 4 November 2016. Available from http://annualreports.teliasonera.com/en/2015/sustainability-work/human-rights-impact-/.

57 These companies include Amazon, Apple, AT&T, Cisco, Deutsche Telekom, Facebook, Google, Kakao, LinkedIn, Microsoft, Naver, Orange, Rogers, Telenor, Teliasonera, Twitter, Vodafone, and Yahoo. See AccessNow, "Transparency reporting index", 4 November 2016. Available from https://www.accessnow.org/transparency-reporting-index/.

form of – and approach to – such disclosures are still emerging, companies should engage with stakeholders to determine what information related to terms of service enforcement would bolster trust and accountability.

D. Enable users to keep themselves secure

Companies should communicate basic information about account access, encryption of data in transit and at rest, and delivery of software security updates. They should also publish educational materials to help users mitigate security threats. As the SDGs encourage greater access to ICTs, these educational efforts will be vital to ensure that users understand the risks and vulnerabilities they face when adopting new technology. Companies should also work with external security researchers to discover vulnerabilities. In August 2016, researchers from the University of Toronto's Citizen Lab and Lookout Security discovered a particularly insidious attack that allowed an adversary to turn a target's iOS device into a roving bug. The attack, attributed to Israeli company NSO, relied on three distinct "zero-day" vulnerabilities[58] and has been used against a human rights defender in the United Arab Emirates, several journalists in Mexico, and potentially others. Apple developed and issued a security update within days of learning about it.[59]

Companies that are serious about maximizing users' security should enable users to fully encrypt their content in a way that companies themselves cannot access it. Such "end-to-end" or "zero-knowledge" encryption would help reassure users that their private communications are more secure against data breaches, interception, and sharing with third parties, and that such information can only be accessed by the desired recipients.

E. Provide grievance and remedy mechanisms for users

Under the Guiding Principles, companies and states share a duty to offer effective remedies to users whose rights have been violated. Grievance mechanisms and remedy processes should be more prominently available to users. Companies should more clearly indicate that they accept concerns related to potential or actual violations of freedom of expression and privacy as part of these processes. Beyond this, disclosure about how companies process complaints, along with

58 Written as either "zero-day" or "0-day," this refers to a weakness in a software program that is unknown to the vendor and exploited by hackers before the vendor has a chance to issue a security patch. The term refers to the number of days (zero) that the vendor has had to develop a software update to defend against the attack.

59 Bill Marczak and John Scott-Railton, "The million dollar dissident: NSO group's iPhone zero-days used against a UAE human rights defender. *Citizen Lab*, 24 August 2016. Available from https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

general reporting on complaints and outcomes, would help stakeholders ensure that companies take grievance and remedy processes seriously. Marking a step in the right direction, Twitter created a Trust and Safety Council in February 2016 that includes dozens of civil society organizations and individuals to provide input on how the company can better balance its free expression values with the need to protect its users.[60]

F. Engage with policymakers for changes that will help companies better respect users' rights

Finally, companies should advocate for legal and regulatory changes that support their ability to respect users' freedom of expression and privacy. The 2030 Agenda repeatedly calls upon national governments to reform legislation, and ICT companies can work with governments to address human rights and development goals simultaneously. For example, national legislation in several countries prevents companies from engaging in transparency reporting around government requests for user information. Companies should work with civil society advocates and responsible investors to convince national governments to enact legal and regulatory reform that maximizes users' freedom of expression and privacy. Governments in turn must evaluate these corporate advocacy appeals while remaining vigilant about regulatory capture and ensuring that their policies do not undermine competition or limit citizens' ability to access the free and open Internet.

V. How Governments Can Help ICT Companies Better Respect Users' Rights

Cohesive, nationally owned strategies are central to meeting the SDGs.[61] Within this framework, governments can also help foster an ecosystem that supports, rather than challenges, Internet intermediaries' ability to respect human rights. Some operating environments lack fundamental governance tools such as respect for rule of law, an independent judiciary, and sufficient legal, policymaking, and technical capacity among civil servants. Improvement on those fronts would, of course, yield myriad benefits beyond greater respect for users' digital rights. For states that do have such governance structures in place, this section offers recommendations for ways that governments can advance users' digital rights.

A. Assess the human rights impacts of laws

As discussed above, the GNI and RDR standards expect companies to conduct impact assessments to evaluate how their business decisions, including those

60 Charlie Warzel, *A honeypot...* supra note 22.

61 A/RES/70/1.

about new products or features, affect human rights. Legislative bodies should conduct similar assessments on existing as well as proposed laws and regulations and revise those that imperil citizens' human rights.

For example, intermediary liability laws, which "formalize government expectations for how an intermediary must handle 'third-party' content or communications," significantly affect the extent to which companies can promote or limit freedom of expression.[62] Countries can adopt distinct intermediary liability regimes for different types of content. In the United States, Section 230 of the Communications Decency Act generally shields intermediaries from responsibility for the content their users post or share on their platforms, and from liability that stems from company decisions to remove content in accordance with their own terms. These protections mean that companies in the United States are not legally pressured to monitor the content on their services and are empowered to operate their business as they see fit (though human rights norms and standards emphasize that companies should be transparent about how they do so).

Intermediaries in the United States do not receive such broad immunity for content that may infringe copyright. The country's Digital Millennium Copyright Act takes what is known as a "notice-and-takedown" approach to intermediary liability. Companies are generally not liable if they unknowingly host material that infringes copyright; however, if they receive notice alleging that content on their platform violates copyright, they can be held liable for letting it remain available. While the law enables individuals whose content is restricted to protest the removal, the law incentivizes companies "to remove content immediately after receiving notice, rather than investing resources to investigate the validity of the request and risk a lawsuit. Legitimate content can end up being censored as a consequence."[63]

Finally, countries including China and Thailand maintain strict intermediary liability regimes where intermediaries are responsible for content that appears on their platforms. Companies there can face serious consequences, ranging from fines to revocation of their operating license, if prohibited content appears on their platforms.[64] This threat incentivizes companies to proactively monitor and censor content on their platforms, posing obvious challenges to free expression rights. The Manila Principles on Intermediary Liability represent a globally

62 Rebecca MacKinnon and others, *Fostering freedom...* supra note 6, p. 39.
63 Idem, p. 42.
64 Ibidem.

accepted framework that calls for very limited liability for companies.[65] As a first step governments, can evaluate their own intermediary liability laws against these standards to identify areas where laws can change to better protect users' free expression rights.

Regarding privacy rights, governments can evaluate the extent to which any privacy or data protection laws adhere to such standards as the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines[66] or the Code of Fair Information Practice first proposed by the then-US Department of Health, Education and Welfare.[67] In some countries, data retention laws mandate companies to store user information for a specific amount of time. Lengthy retention periods can pose security and surveillance risks to users. The more data companies keep, the more data is available for criminals, companies, governments, or other third parties to access. Governments should review the extent to any data retention regulations may pose a threat to human rights.

Governments should also evaluate any laws or regulations that can be interpreted as authorizing mass surveillance to ensure such laws adhere to the International Principles on the Application of Human Rights to Communications Surveillance.[68] These "necessary and proportionate" principles apply international human rights law to modern digital surveillance and articulate the circumstances in which surveillance, conducted within and beyond a state's borders, is permissible. The principles include a global legal analysis and an implementation guide with checklists and examples to help government officials operationalize the principles.

B. Provide transparency on requests for companies to restrict content or share user information

This article has referenced the transparency reports that many intermediaries publish to disclose the volume and nature of requests they receive to restrict content and/or release user information. While this reporting sheds light on the extent to which companies are compelled to act in ways that may undermine free expression and privacy, such a picture cannot be close to comprehensive

65 "Manila principles on intermediary liability", 2016. Available from https://www.manilaprinciples.org/.

66 Organization for Economic Cooperation and Development, "The OECD privacy framework", 2013. Available from http://www.oecd.org/Internet/ieconomy/privacy-guidelines.htm.

67 United States, Department of Health and Human Services, "Records, computers and the rights of citizens, 1 July 1973. Available from https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

68 "International principles on the application of human rights to communications surveillance, 2013. Available from https://necessaryandproportionate.org/.

until governments provide the same level of transparency. The Freedom Online Coalition found the public increasingly expects such transparency, and that providing it can engender greater public trust in government activities related to law enforcement and national security.[69] The coalition's report provides examples of specific types of transparency from the governments of Australia, Sweden, the United Kingdom, and the United States.[70]

VI. Conclusion

ICTs have changed people's lives worldwide, and they promise to be valuable tools in advancing the Sustainable Development Goals. However, many ICTs are provided by private companies that establish the rules by which their platforms operate, enforce those rules, and set the terms of any appeal mechanisms. This flies in the face of modern governance principles, which hold that such roles should fall under the purview of separate institutions. It also raises a number of concerns for human rights, many of which this article has described. Several accountability mechanisms have arisen to address these gaps in governance. As the standards set forth by these mechanisms become more widely implemented, the public will gain greater insight into the role that such companies play in human rights and will be better positioned to pressure them (and the governments that sometimes incentivize or even compel companies to take such actions) to maximize, not restrict, human rights. Awareness of the key role that ICT companies play is especially important in the context of the SDGs. Governments, with assistance from the international community, are designing national plans for communications infrastructure and services that use ICTs and, in many cases, contract implementation to the private sector. These companies can use their mandates responsibly to strengthen human rights, for example by building privacy safeguards into service delivery databases, or to jeopardize them – perhaps irremediably – for example, by building covert access mechanisms into such databases. When choosing private sector partners for ICT4D projects, governments and the donor community should exercise due diligence in evaluating companies' commitment to human rights, notably privacy and free expression, and require that private-sector partners meet

69 Freedom Online Coalition, "Report: Working Group 3 Privacy and Transparency Online" November 2015. Available from https://www.freedomonlinecoalition.com/wp-content/uploads/2015/10/FOC-WG3-Privacy-and-Transparency-Online-Report-November-2015.pdf.

70 Idem. For example, the Australian attorney general issues annual reports about government interception of user information and use of surveillance devices. Sweden's government reports statistics annually about interception and collection of user information. The British Interception of Communications Commissioner's Office (IOCCO) conducts an annual audit into the country's use of interception, and the U.S. National Security Agency has also released surveillance-related statistics.

certain standards. At minimum, these standards should include transparency about company policies that affect human rights, evidence that companies have institutionalized their human rights commitments, measures that enable users to keep themselves secure, and mechanisms for remedy when users' rights have been violated.

VII. References

"International principles on the application of human rights to communications surveillance, 2013. Available from https://necessaryandproportionate.org/.

"Manila principles on intermediary liability", 2016. Available from https://www.manilaprinciples.org/.

A/HRC/32/L.20.

A/HRC/RES/17/L.17/Rev.1.

A/RES/217 (III).

A/RES/70/1.

AccessNow, "#KeepItOn", 28 November 2016. Available from https://www.accessnow.org/keepiton/.

AccessNow, "Transparency reporting index", 4 November 2016. Available from https://www.accessnow.org/transparency-reporting-index/.

Bertrand de La Chapelle and Paul Fehlinger, "Jurisdiction on the Internet: From legal arms race to transnational cooperation", Global Commission on Internet Governance Paper Series, No. 28 (Waterloo, Canada, Centre for International Governance Innovation and Chatham House, April 2016). Available from https://www.cigionline.org/publications/jurisdiction-internet-legal-arms-race-transnational-cooperation.

Bill Marczak and John Scott-Railton, "The million dollar dissident: NSO group's iPhone zero-days used against a UAE human rights defender. Citizen Lab, 24 August 2016. Available from https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Business & Human Rights Resource Centre, "NGO alleges TeliaSonera contributing to repression in Belarus", 16 September 2009. Available from https://business-humanrights.org/en/ngo-alleges-teliasonera-contributing-to-repression-in-belarus.

Business & Human Rights Resource Centre, "NGO alleges TeliaSonera pulls out of Eurasia market because of corruption scandals in Azerbaijan & Uzbekistan; Company responds", 9 October 2015. Available from https://business-humanrights.org/en/ngo-alleges-teliasonera-pulls-out-of-eurasia-market-because-of-corruption-scandals-in-azerbaijan-uzbekistan-company-responds.

Carly Nyst, "Internet intermediaries and violence against women: Online executive summary and findings", End Violence: Women's Rights and Safety Online (Association for Progressive Communications, 2014). Available from http://www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf.

Carmen Valor, "Corporate social responsibility and corporate citizenship: Towards corporate accountability", Business and Society Review, vol. 110, No. 2 (2005).

Charlie Warzel, "A honeypot for assholes': Inside Twitter's 10-year failure to stop harassment", Buzzfeed, 11 August 2016. Available from https://www.buzzfeed.com/charliewarzel/a-honeypot-for-assholes-inside-twitters-10-year-failure-to-s?utm_term=.qgYzVJ4BL#.rrZWe6GEl.

David Bamman, Brendan O'Connor and Noah Smith, "Censorship and deletion practices in Chinese social media", First Monday, vol. 17, No. 3 (2012), dx.doi.org/10.5210/fm.v17i3.3943.

Elizabeth Stoycheff, "Under surveillance: Facebook online spiral of silence effects in the wake of NSA Internet monitoring", Journalism and Mass Communication Quarterly, vol. 93, No. 2 (2016).

Emily Taylor, "The privatization of human rights: Illusions of consent, automation and neutrality", Global Commission on Internet Governance Paper Series, No. 24 (Waterloo, Canada, Centre for International Governance Innovation and Chatham House, January 2016). Available from https://www.cigionline.org/sites/default/files/gcig_no24_web_2.pdf.

Eric Lichtblau, "In Apple debate on digital privacy and the iPhone, questions still remain", New York Times, 28 March 2016. Available from http://www.nytimes.com/2016/03/29/us/politics/in-apple-debate-on-digital-privacy-and-the-iphone-questions-still-remain.html?_r=0.

European Commission, ICT sector guide on implementing the UN Guiding Principles on Business and Human Rights. (Brussels, 2013). Available from https://ec.europa.eu/anti- trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf.

Evgeny Morozov, The net delusion: The dark side of Internet freedom (New York City, Public Affairs, 2011).

Facebook, "Encouraging respectful behavior: Hate speech", 4 November 2016. Available from https://www.facebook.com/communitystandards/#.

Facebook, "I believe my content was removed in error", 4 November 2016. Available from https://www.facebook.com/help/780814295267977.

Freedom Online Coalition, "Report: Working Group 3 Privacy and Transparency Online" November 2015. Available from https://www.freedomonlinecoalition.com/wp-content/uploads/2015/10/FOC-WG3-Privacy-and-Transparency-Online-Report-November-2015.pdf.

Global Network Initiative, "The Global Network Initiative and the Telecommunications Industry Dialogue join forces to advance freedom of expression and privacy", 1 February 2016. Available from https://www.globalnetworkinitiative.org/news/global-network-initiative-and-telecommunications-industry-dialogue-join-forces-advance-freedom.

Global Network Initiative, "Principles", 6 November 2016. Available from http://globalnetworkinitiative.org/principles/index.php.

International Telecommunication Union and United Nations Educational, Scientific and Cultural Organization, Doubling digital opportunities: Enhancing the inclusion of women & girls in the information society: A report by the Broadband Commission Working Group on Broadband and Gender (Geneva, Switzerland, 2013). Available from http://www.broadbandcommission.org/documents/working-groups/bb-doubling-digital-2013.pdf.

Jessa Lingel and Adam Golub. "In face on Facebook: Brooklyn's drag community and sociotechnical practices of online communication", Journal of Computer-Mediated Communication, vol. 20, No. 5 (2015), doi:10.1111/jcc4.12125.

Jessica Valenti, "Anita Sarkeesian interview: 'The word "Troll" feels too childish. This is abuse.'" Guardian, 29 August 2015. Available from https://www.theguardian.com/technology/2015/aug/29/anita-sarkeesian-gamergate-interview-jessica-valenti.

John Gerard Ruggie, Just business: Multinational corporations and human rights (New York City, New York, W. W. Norton & Company, 2013).

John Postill, "Freedom technologists and the new protest movements: A theory of protest formulas", Convergence: The International Journal of Research into New Media Technologies, vol. 20, No. 4 (2014) doi:10.1177/1354856514541350.

Jon Diamond, "Liberation technology", Journal of Democracy, vol. 21, No. 3 (2010).

Laura DeNardis and Andrea M. Hackl, "Internet control points as LGBT rights mediation", Information, Communication & Society, vol. 19 No. 6 (2016), doi:10.1080/1369118X.2016.1153123.

Laura DeNardis, The global war for Internet governance (New Haven, Connecticut, Yale University Press, 2015).

Lyz Lenz, "Inside the psyche of a troll who threatens a child." Daily Dot, 3 August 2016. Available from http://www.dailydot.com/irl/jessica-valenti-online-threats/.

Mary L. Gray, "Negotiating identities/queering desires: Coming out online and the remediation of the coming-out story", Journal of Computer-Mediated Communication, vol. 14, No. 4 (2009), doi:10.1111/j.1083-6101.2009.01485.x.

Milton Mueller, Networks and states: The global politics of Internet governance (Boston, Massachusetts: The MIT Press, 2010).

Organization for Economic Cooperation and Development, "The OECD privacy framework", 2013. Available from http://www.oecd.org/Internet/ieconomy/privacy-guidelines.htm.

Patrick Markey, "Algeria blocks Facebook, Twitter to stop exam cheats: State media", Reuters, 19 June 2016. Available from http://www.reuters.com/article/us-algeria-media-idUSKCN0Z50JX.

Paul M. Schwartz and Daniel J. Solove, "The PII problem: Privacy and a new concept of personally identifiable information", New York University Law Review, vol. 86, (2011).

Paul Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization", UCLA Law Review, vol. 57, (2010).

Peerzada Ashiq, "Jammu goes offline ahead of controversial wrestling event", Hindu, 22 June 2016. Available from http://www.thehindu.com/news/national/other-states/jammu-goes-offline-ahead-of-controversial-wrestling-event/article8756852.

Penelope Simons, "International law's invisible hand and the future of corporate accountability for violations of human rights", Journal of Human Rights and the Environment, vol. 3, No. 1 (March 2012).

Peter Newell, "From responsibility to citizenship?: Corporate accountability for development", IDS Bulletin, vol. 33, No. 2 (2002).

Ranking Digital Rights, "2015 corporate accountability index", November 2015. Available from https://rankingdigitalrights.org/index2015/assets/static/download/RDRindex2015report.pdf.

Ranking Digital Rights, "2017 Indicators", 14 September 2016. Available from https://rankingdigitalrights.org/2017-indicators/.

Ranking Digital Rights, "Download the Data", 6 November 2016. Available from https://rankingdigitalrights.org/index2015/download/.

Rebecca MacKinnon and others, Fostering freedom online: The role of Internet intermediaries (Paris, France, UNESCO, 2014).

Rebecca MacKinnon, Consent of the networked: The world-wide struggle for Internet freedom (New York City, New York: Basic Books, 2012).

Rebecca MacKinnon, Nathalie Maréchal and Priya Kumar, "Corporate accountability for a free and open Internet", Global Commission on Internet Governance Paper Series (Waterloo, Canada, Centre for International Governance Innovation and Chatham House, December 2016). Available from https://www.cigionline.org/publications/corporate-accountability-free-and-open-internet.

Renginee G. Pillay, "The limits to self-regulation and voluntarism: From corporate social responsibility to corporate accountability", Amicus Curiae, No. 99 (Autumn 2014).

Ronald Deibert, Black code: Inside the battle for cyberspace (Toronto, Canada: McClelland & Stewart, 2013).

Simon Parkin, "Pakistan's troll problem", New Yorker, 28 June 2016. Available from http://www.newyorker.com/tech/elements/pakistans-troll-problem.

Shift and Mazars. (2016). "UN Guiding Principles reporting framework". Available from http://www.ungpreporting.org/.

Telia Company, "Respecting freedom of expression: Information about and Telia company view on new legislation in Tajikistan", 8 June 2016. Available from http://www.teliacompany.com/en/newsroom/news/news/news-articles/2016/respecting-freedom-of-expression--information-about-and-telia-company-view-on-new-legislation-in-tajikistan.

Telia Company, "Respecting freedom of expression: Recent major event as to service limitations in Kazakhstan, June 2016", 1 July 2016. Available from http://www.teliacompany.com/en/newsroom/news/news/news-articles/2016/Respecting-Freedom-of-Expression-Recent-major-event-as-to-service-limitations/.

Telia Company, "Respecting freedom of expression: Telia company view on new legislation in Moldova", 25 April 2016. Available from http://www.teliacompany.com/en/newsroom/news/news/news-articles/2016/respecting-freedom-of-expression--telia-company-view-on-new-legislation-in-moldova/.

TeliaSonera," Human rights impact assessments: Focus on region Eurasia", 4 November 2016. Available from http://annualreports.teliasonera.com/en/2015/sustainability-work/human-rights-impact-/.

United Nations, Office of the High Commissioner on Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations "Respect, Protect and Remedy" framework. (Geneva, Switzerland, 2011). Available from http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

United States, Department of Health and Human Services, "Records, computers and the rights of citizens, 1 July 1973. Available from https://aspe.hhs.gov/report/records-computers-and-rights-citizens.