11

Human Rights and Private Actors in the Online Domain

Rikke Frank Jørgensen

I INTRODUCTION

The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression recently stated that the Internet has become the central global public forum with profound value for human rights.[1] In this global public forum, control over infrastructure and services is largely in the hands of companies, with some of the most powerful being from the United States. To participate in the online sphere, individuals must engage with online platforms such as Google and Facebook and rely on them for exercising rights and freedoms such as freedom of expression, freedom of information, and freedom of assembly.

In this sense, these companies have increasing power to influence rights in the online domain. The power of the major platforms flow from their control over a wide range of resources crucial to information search and public participation in the online realm. In 2013, *The New York Times* had a print and digital circulation of nearly two million and claimed to be the most visited newspaper site, with nearly thirty-one million unique visitors every month. YouTube, in contrast, had one billion unique visitors a month in 2014, or as many in a day as *The New York Times* has in a month.[2] In terms of company valuations, as of April 2014 *The Times*'s market value was around 1 percent of the value of Facebook or Google.[3] By the end

[1] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, ¶ 11, U.N. Doc. A/HRC/29/32 (May 22, 2015) ("2015 Kaye Report").

[2] M. Ammori, "The 'New' New York Times: Free Speech Lawyering in the Age of Google and Twitter" (2014) 127 *Harvard Law Review* 2259–94 at 2266.

[3] Ibid., at 2267.

of 2015, Facebook had more than 1.6 billion users a month[4] and Google more than one billion searches a month.[5]

Online platforms are used every day by billions of people to express themselves and to comment on, debate, critique, search, create, and share views and content. As such, the Internet's distributed architecture and the decrease in communications costs have fundamentally altered the capacity of individuals to be active participants in the public sphere. On a positive note, this networked public sphere facilitates new means for civic engagement, public participation, social change, and countering repressive governments.[6] On a more cautious note, scholars have warned that the new infrastructure for exercising freedom of expression carries with it new modalities of interference with fundamental rights, and that adequate legal responses have yet to be found.[7]

One area of concern – not least among legal scholars, data protection authorities, and groups set up to protect fundamental rights on the Internet[8] – is the privatized law enforcement and self-regulatory measures of these corporate platforms. The concern is particularly related to the platforms' means of "content regulation" and privacy practices; for example, their day-to-day decisions on which content to remove or leave up, and the extent to which they collect, process, and exchange personal data with third parties.[9] Several cases in the United States and Europe have addressed this concern, and new cases continue to appear.[10] Scholars have also warned of a governance gap, where private actors with strong human rights impacts

[4] "Number of monthly active Facebook users worldwide as of 2nd quarter 2016," Statista, www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

[5] C. Smith, "100 Google Search Statistics and Fun Facts," DMR, http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/.

[6] Yochai Benkler argues that the Internet and the networked information economy provide us with distinct improvements in the structure of the public sphere over mass media. This is due to the information produced by and cultural activity of non-market actors, which the Internet enables, and which essentially allow a large number of actors to see themselves as potential contributors to public discourse and potential actors in political arenas. Y. Benkler, *Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven, CT: Yale University Press, 2006), p. 220. "The network allows all citizens to change their relationship to the public sphere. They no longer need to be consumers and passive spectators. They can become creators and primary subjects. It is in this sense that the internet democratizes." Ibid., p. 272.

[7] J. M. Balkin, "Old-School/New-School Speech Regulation" (2014) 127 *Harvard Law Review* 2296–342.

[8] This includes groups and networks such as the Electronic Privacy Information Center (US), the Electronic Frontier Foundation (US), Privacy International (UK/global), European Digital Rights (European), Access Now(US), and the Association for Progressive Communications (global).

[9] A key issue in the human rights context may be that content with historical or legal value – e.g., information that may serve as evidence of a human rights violation or war crime – is taken down for violation of terms of service or community standards.

[10] In the United States, the Federal Trade Commission has focused on Internet platforms on several occasions. For example, since 2011, Facebook Inc. has been under a consent order by the FTC for deceiving consumers by telling them they could keep their information on

operate within the soft regime of guidelines and corporate social responsibility with no direct human rights obligations.[11] International human rights law is binding on states only, and despite an increasing take-up of human rights discourse within Internet companies, their commitment remains voluntary and nonbinding. In addition, limited information is available in the public domain concerning the corporate practices that affect freedom of expression and privacy.

Although a part of public discourse has always unfolded within private domains, from coffeehouses to mass media, the current situation is different in scope and character. In the online realm, *the vast majority* of social interactions, discussions, expressions, and controversies take place on platforms and services provided by private companies. As such, an increasing portion of our sociality is conducted in privately owned spaces. In addition, these practices are entangled in a business model in which the conversations and interactions that make up online life are directly linked to revenue. This arguably represents yet another stage of the trend of privatization. Prior examples include the dominance of corporate-owned media over the civic public sphere, the outsourcing of government functions to private contractors, and the reduction of public spaces to malls and privately owned town squares.[12] However, the increasing significance of online platforms for public life gives rise to a large number of unresolved questions related to the techno-social design, regulation, and human rights impact of these companies as "curators of public discourse."[13]

As several scholars have argued, these online platforms have an enormous impact on human rights globally through the policies they adopt for their users. Within "Facebookistan" and "Twitterland,"[14] these polices have just as much

Facebook private and then repeatedly allowing it to be shared and made public. The order requires that Facebook obtain periodic assessments of its privacy practices by independent third-party auditors for the next twenty years. For more information on the case, please refer to "Facebook, Inc.," Federal Trade Commission, www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc. In Europe, the Dutch Data Protection Authority (DPA) imposed an incremental penalty payment on Google in 2013 based on practices introduced with Google's privacy policy in 2012. According to the DPA, Google combines the personal data collected by all kinds of different Google services without adequately informing users in advance and without asking for their consent. In July 2015, the DPA announced that Google had revised its privacy policy following the demands of the DPA, and that Google had until the end of December 2015 to obtain the unambiguous consent of all of its users at each step. For more information on the case, please refer to "Dutch DPA: privacy policy Google in breach of data protection law," *Autoriteit Persoongegevens*, https://cbpweb.nl/en/news/dutch-dpa-privacy-policy-google-breach-data-protection-law.

[11] E. B. Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge: Cambridge University Press, 2015).

[12] Z. Tufekci, "Facebook: The Privatization of our Privates and Life in the Company Town," Technosociology: our tools, ourselves, http://technosociology.org/?p=131.

[13] T. L. Gillespie, "The Politics of Platforms" (2010) 12 *New Media & Society* 347–64 at 347.

[14] In *Consent of the Networked: The World-Wide Struggle for Internet Freedom* (New York: Basic Books, 2012), p. 150, Rebecca MacKinnon refers to Facebook's "digital kingdom" as Facebookistan. In *Foreign Policy*, she further argues that "Facebook is not a physical country, but with

validity as traditional legal rules and standards.[15] Moreover, the companies have wide discretion in enforcing the policies, as they weigh potential precedents, norms, competing interests, and administrability in developing the rules of expression and privacy that effectively govern their users worldwide. Arguably, Google's lawyers and executives have as much power to determine who may speak and who may be heard around the world than does any president, king, or Supreme Court justice[16] – or, as expressed by Marvin Ammori, "Technology lawyers are among the most influential free expression lawyers practicing today."[17] At the same time, the core business of these companies is built around expression, and most of them talk about their business in the language of freedom of expression and freedom of information. Google's official mission is "to organize the world's information and make it universally accessible and useful."[18] Twitter stresses that its goal is "to instantly connect people everywhere to what is most meaningful to them. For this to happen, freedom of expression is essential."[19] Twitter also states that tweets must flow as a default principle. Facebook's vision is to "give people the power to share and make the world more open and connected."[20]

In relation to privacy, the online infrastructure of free expression is increasingly merging with the infrastructure of content regulation and surveillance. The technologies, institutions, and practices that people rely on to communicate with one another are the same technologies, institutions, and practices that public and private parties employ for surveillance.[21] The online infrastructure simultaneously facilitates and controls freedom of expression, surveillance, and data mining. As such, it has become a new target for governments and corporate interests alike.

Since 2009, several of the major Internet companies have upgraded and formalized their human rights commitment. Most notably this has been via industry initiatives, such as the Global Network Initiative, that focus on a company's compliance with international human rights standards on privacy and freedom of

900 million users, its 'population' comes third after China and India. It may not be able to tax or jail its inhabitants, but its executives, programmers, and engineers do exercise a form of governance over people's online activities and identities." R. MacKinnon, "Ruling Facebookistan," *Foreign Policy*, June 14, 2012, http://foreignpolicy.com/2012/06/14/ruling-facebookistan/; *see also* A. Chander, "Facebookistan" (2012) 90 *North Carolina Law Review* 1807–42.

[15] Ammori, "The 'New' New York Times" at 2263.

[16] J. Rosen, "The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google" (2012) 80 *Fordham Law* Review 1525–38 at 1536.

[17] Ammori, "The 'New' New York Times" at 2265.

[18] Google, www.google.com/about/company/.

[19] B. Stone, "The Tweets Must Flow," Twitter, January 28, 2001, https://blog.twitter.com/2011/tweets-must-flow.

[20] Facebook, http://investor.fb.com/faq.cfm.

[21] *See* Balkin, "Old-School/New-School Speech Regulation" at 2296–342.

expression.[22] Also, as Lisl Brunner points out in Chapter 10, in the wake of the NSA contractor Edward Snowden's revelations of state surveillance, there has been increasing public focus on the exchange of personal data between Internet companies and government agencies. As a result, several companies have started to publish transparency reports to document (at an aggregated level) the numbers and types of content removal requests they receive and accommodate.[23] Despite these efforts, there is still limited public knowledge of companies' internal mechanisms of governance; e.g., how they decide cases with freedom of expression implications or how they harness user data.[24] As illustrated by a number of cases in the European Union as well as in Europe more broadly, a number of human rights related practices continue to cause concern among scholars and regulators alike.[25]

Using the example of Internet companies, this chapter will critically examine current challenges related to human rights protection in the online domain. This will include questions such as: How shall we understand the role of Internet companies vis-à-vis freedom of expression? What does human rights law – and soft law such as the UN Guiding Principles on Business and Human Rights – say about private actors and their human rights responsibilities? How have major Internet companies taken up these challenges in their discourse and practices? What are some of the dynamics that work for or against stronger human rights protection online? And are the frameworks that currently govern the activities of these Internet companies sufficient to provide the standards and mechanisms needed to protect and respect human rights online?

II THE ROLE OF INTERNET COMPANIES IN THE ONLINE DOMAIN

Over the past ten years, the Internet's potential positive and negative impacts on human rights have been iterated time and again by the UN World Summit on the

[22] Global Network Initiative, www.globalnetworkinitiative.org.

[23] A transparency report discloses statistics related to government requests for user data or content over a certain period of time. Google was the first online platform to publish a transparency report in 2010, with Twitter following in 2012.

[24] Ranking Digital Rights published its first annual Corporate Accountability Index in November 2015. The index ranks sixteen Internet and telecommunication companies according to thirty-one indicators, focused on corporate disclosure of policies and practices that affect users' freedom of expression and privacy. Ranking Digital Rights, https://rankingdigitalrights.org.

[25] Examples include the US Federal Trade Commission (FTC) investigation into Google's practices in connection with its YouTube Kids app (2015), the FTC Consent Order on Facebook (2011), the Dutch Data Protection Authority case against Google (2013), the Austrian class action privacy lawsuit against Facebook (rejected by the Austrian Court in July 2015 due to the lack of jurisdiction), the Google/Spain ruling of the European Court of Justice (2014), the Belgian Privacy Commissioners' recommendations to Facebook (2015), the Irish Data Protection Authority's audit of, and recommendations to, Facebook (2011), the European Union's antitrust case against Google (2015), and the Article 29 Working Party's examination of Google's Privacy Policy (2012).

Information Society,[26] the UN Human Rights Council,[27] and UN thematic rapporteurs.[28] The former UN Special Rapporteur on the Promotion and Protection of Freedom of Opinion and Expression, Frank La Rue, for example, has emphasized the unprecedented opportunity presented by the Internet to expand the possibilities for individuals to exercise a wide range of human rights, with freedom of opinion and of expression as prominent examples.[29] Special Rapporteur La Rue also expressed concerns about the multiple measures taken by states to prevent or restrict the flow of information online, and he highlighted the inadequate protection of the right to privacy on the Internet.[30] Of specific relevance to this chapter is his emphasis on the way private actors may contribute to violating human rights online, given that Internet services are run and maintained by companies.[31] In parallel to this, policy reports and scholarship have increasingly addressed the specific challenges related to human rights protection in the online domain.[32]

[26] At the first UN World Summit on the Information Society (WSIS), held in two phases in 2003 and 2005, it was confirmed that international human rights law serves as the baseline for information and communications technology (ICT)-related policy. Since WSIS, UN agencies such as the International Telecommunication Union, the United Nations Development Programme, and UNESCO have been responsible for follow-up action to ensure that the WSIS vision is implemented. This implementation process was reviewed in December 2015. World Summit on the Information Society, www.itu.int/wsis/review/2014.html.

[27] Human Rights Council, Res. 20/8, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, U.N. Doc. A/HRC/RES/20/8 (July 16, 2012); Human Rights Council Res. 26/13, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, U.N. Doc. A/HRC/RES/26/13 (July 14, 2014); "The right to privacy in the digital age," U.N. Doc. A/HRC/27/37 (June 30, 2014).

[28] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, U.N. Doc. A/HRC/17/27 (May 16, 2011) ("2011 La Rue Report"); *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, U.N. Doc. A/HRC/23/40 (April 17, 2013) ("2013 La Rue Report"); 2015 Kaye Report.

[29] 2011 La Rue Report.

[30] 2013 La Rue Report.

[31] 2011 La Rue Report, ¶ 44.

[32] R. F. Jørgensen (ed.), *Human Rights in the Global Information Society* (Cambridge, MA: MIT Press, 2006); C. Garipidis and N. Akrivopoulou, *Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies* (Hershey, PA: Information Science Reference, 2012); W. Benedek and R. Madanmohan, "Human Rights and Information and Communication Technology – Background Paper," in *Proceedings of the 12th Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights* (Singapore: Asia-Europe Foundation, 2013), Seoul, Republic of Korea, June 27–29, 2012, pp. 34–87; D. Korff, *The Rule of Law on the Internet and in the Wider Digital World – Issue Paper for the Council of Europe* (Strasbourg: Council of Europe, 2014); R. F. Jørgensen, *Framing the Net: The Internet and Human Rights* (Cheltenham: Edward Elgar Publishing, 2013); C. Padovani, F. Musiani, and E. Pavan, "Investigating Evolving Discourses on Human Rights in the Digital Age: Emerging Norms and Policy Challenges" (2010) 72 *International Communication Gazette*, 4–5, 359–78; L. Horner, D. Hawtin, and A. Puddehatt, Directorate-General for External Policies of the Union Study, "Information and Communication Technologies and Human Rights," EXPO/B/DROI/2009/24 (June 2010).

It is now widely recognized that access to the Internet and participation in discourse through the Internet have become integral parts of democratic life. What is less debated is the fact that facilitating this democratic potential critically relies on private actors. Access to the Internet takes place through Internet service providers, information search is facilitated by search engines, social life plays out via online platforms, and so on. Despite the increasing role that these private actors play in facilitating democratic experience online, the governance of this social infrastructure has largely been left to companies to address through corporate social responsibility frameworks, terms of service, and industry initiatives such as the Global Network Initiative.[33] Moreover, there is limited research critically assessing the frameworks that govern the activities of these Internet companies and questioning whether they are sufficient to provide the standards and compliance mechanisms needed to protect and respect human rights online.

The Internet's democratic potential is rooted in its ability to promote "a culture in which individuals have a fair opportunity to participate in the forms of meaning making that constitute them as individuals."[34] Democratic culture in this sense is more than political participation; it encompasses broad civic participation where anyone, in principle, may participate in the production and distribution of culture. This democratic potential is linked to the Internet's ability to provide its users with unprecedented access to information and to decentralized means of political and cultural participation.[35] By decentralizing the production of content, supplementing mass media with new means of self-expression, and enabling collective action across borders, the Internet has the potential to be a more participatory public sphere. This potential has been widely addressed in the body of literature that considers the Internet as a new or extended public sphere, yet with limited evidence of the actual democratic impact of these new modalities.[36] Moreover, the democratic implications of having private actors with no public interest mandate controlling the sphere is still not sufficiently clear, yet several challenges surface.

A *No Public Streets on the Internet*

In the United States, the protections of a speaker's right to speech vary based on the chosen forum. The Supreme Court distinguishes among three types of forums: traditional public forums, designated forums, and nonpublic forums.[37] The traditional public forum doctrine protects speech in public places such as streets,

[33] Laidlaw, *Regulating Speech in Cyberspace*, p. 59.
[34] J. M. Balkin, "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society" (2004) 79 *New York University Law Review* 1–55 at 40.
[35] Laidlaw, *Regulating Speech in Cyberspace*, p. 18.
[36] For an elaboration of the Internet as a new kind of public sphere, please refer to Jørgensen, *Framing the Net*, pp. 81–106.
[37] *Perry Educ. Ass'n* v. *Perry Educators' Ass'n*, 460 U.S. 37 (1983).

sidewalks, and parks, which are traditionally recognized as being held in common for the public good.[38] Expressive activity in these spaces can, in specific and narrowly defined cases, be subject to "time, place, and manner restrictions," but only in exceptional cases can such restrictions be based on the messages themselves.[39] In contrast, the owners of private property are relatively free in the restrictions they may place on the speech that takes place on their property.

When Internet users search for information, express opinions, debate, or assemble, they largely do so within privately owned forums. Accordingly, the company that provides the service is free to set the conditions for allowed expressions and actions on its platform. As Stacey Schesser explains, "Each private URL owner controls the traffic on his or her website, therefore limiting the application of the First Amendment to the site. Although a website author may choose not to censor postings on her blog or remove discussion threads on his bulletin board, each URL owner retains the right to do so as a private actor."[40] Legally speaking, the online sphere holds no public streets or parks, and social media platforms such as Facebook and Google Plus do not constitute public forums, but rather private property made open to the public. In line with this, there is no First Amendment protection of speech on these platforms. On the contrary, the communications that users provide as they tweet or contribute to Facebook, Google, or LinkedIn is largely private property, owned by the company that provides the service.[41]

Moreover, these companies have broad power to restrict speech that would otherwise be protected by the First Amendment. The highly praised liability regime for online Internet services in the United States, which immunizes intermediaries from liability for third-party content[42] as codified in Section 230 of the Communication Decency Act, effectively gives Internet companies the discretion to regulate content. Without Section 230, Internet companies could be secondarily responsible for the content posted on their platforms, including defamatory speech, if they took steps to censor this content to remove speech that might be offensive to other users. Section 230's so-called Good Samaritan provision protects Internet services from liability if they restrict access to material or give others the technical means to do so.[43]

[38] R. Moon, "Access to State-Owned Property," in *The Constitutional Protection of Freedom of Expression* (Toronto: University of Toronto Press, 2000), pp. 148–81.

[39] Ibid., p. 148.

[40] Stacey D. Schesser, "A New Domain for Public Speech: Opening Public Spaces Online" (2006) 94 *California Law Review* 1791–825 at 92.

[41] Arguably, public streets and parks today are less significant than online platforms as spaces for public discourse.

[42] *See, e.g.*, "CDA 230: The Most Important Law Protecting Internet Speech," Electronic Frontier Foundation, www.eff.org/issues/cda230.

[43] Schesser, "A New Domain for Public Speech" at 99. At the other end of the spectrum are countries where the state imposes liability regimes on Internet intermediaries in order to control online content. For a global overview of such practices and their negative impact on online freedom of expression, see, for example, the global surveys presented by the OpenNet

B *Online Gatekeepers*

In an attempt to categorize the Internet companies in control of the online public sphere, Emily Laidlaw focuses on their democratic impact, identifying three different types of gatekeepers: micro gatekeepers, authority gatekeepers, and macro gatekeepers.[44] According to this typology, macro gatekeepers maintain significant information control due to their size, influence, or scope, and due to the fact that users must pass through them to use the Internet. Examples of companies in this category would be Internet service providers, mobile network providers, and major search engines. Authority gatekeepers control high amounts of information traffic and information flow, although users are not dependent on them to use the Internet. Examples include sites such as Wikipedia and Facebook. In contrast, micro gatekeepers are sites that play a less important role as sources of information, but still facilitate information and debates of democratic significance, such as certain news sites.[45] Laidlaw's framework suggests that the human rights obligations of Internet gatekeepers should increase when they have the power to influence democratic life in a way traditionally reserved for public bodies. The scale of responsibility is reflected not only in the reach of the gatekeeper, but also in the infiltration of that information, process, site, or tool in democratic culture[46].

C *Expressions Are Products*

The current communications environment is also unique because user expressions constitute the products on which the business models of Internet companies are built. The business models of most, if not all, of the major online services are based on targeted advertising, which means that when individuals participate online – for example, by engaging in conversation or searching for information – these actions are captured, retained, and used for advertising purposes and, as such, constitute products that feed into the online business model. This is essentially different from the predigital age, when individuals' conversations, social networks, preferences, and information searches were neither captured nor *the* core element of the intermediary's business model.

Initiative (ONI), https://opennet.net/. Please note that the ONI stopped collecting data as of December 2014.

[44] This model, which builds on Karine Barzilai-Nahon's network gatekeepers theory (K. Barzilai-Nahon, "Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control," [2008] 59 *Journal of the American Society for Information Science and Technology* 1493–512), is elaborated in Laidlaw, *Regulating Speech in Cyberspace*, pp. 44–46.

[45] Laidlaw, *Regulating Speech in Cyberspace*, p. 53.

[46] Ibid., p. 48.

Because expressions are products, the relationships that people have with Internet companies are fundamentally different from traditional company-customer relationships. As Bruce Schneier explains:

> Our relationship with many of the internet companies we rely on is not a traditional company-customer relationship. That's primarily because we're not customers. We're products those companies sell to their *real* customers. The relationship is more feudal than commercial. The companies are analogous to feudal lords, and we are their vassals, peasants, and – on a bad day – serfs. We are tenant farmers for these companies, working on their land by producing data that they in turn sell for profit.[47]

Although this feudal analogy may appear extreme, Schneier reminds us that what appear to be free products are not. The information and communications that users provide when using the services are essential elements in the online business model and, as such, represent the core source of income for the companies.

There should be nothing new or controversial about an Internet company seeking to optimize its revenue via advertising. The disturbing bit is that these platforms *de facto* control large chunks of the online public sphere and users have limited choice to opt out of the business scheme. There are no public streets on the Internet, and there are limited means of participating in political or cultural life outside the commercial realm. Moreover, contributing to the online economy via online expressions, habits, and preferences has become a premise for participation in the networked public sphere. Thus, according to Schneier: "It's not reasonable to tell people that if they don't like data collection, they shouldn't e-mail, shop online, use Facebook, or have a cell phone. . . . Opting out just isn't a viable choice for most of us, most of the time; it violates what have become very real norms of contemporary life."[48]

On an equally skeptical note, Shoshana Zuboff argues that the economic characteristics of the online business model are in the process of undermining long-established freedoms and represent a largely uncontested new expression of power.[49] Scholars such as Julie Cohen and Niva Elkin-Koren have cautioned that the digital era represents threats to fundamental freedoms whose ramifications we are yet to understand.[50] Elkin-Koren notes, "As information becomes crucial to every aspect of everyday life, control over information (or lack thereof) may affect our ability to participate in modern life as independent, autonomous human beings."[51]

[47] B. Schneier, *Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World* (New York: W. W. Norton & Company, 2015), p. 58.

[48] Ibid., pp. 60–61.

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

[50] J. E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven, CT: Yale University Press, 2012).

[51] N. Elkin-Koren, "Affordances of Freedom: Theorizing the Rights of Users in the Digital Era" (2012) 6 *Jerusalem Review of Legal Studies* 96–109 at 97.

Thus, access to the Internet and participation in discourse through the Internet have become integral parts of modern life. The exercise of this public life, however, takes place almost exclusively via privately owned platforms. Moreover, it is entangled in a business model in which knowledge of individual behavior and preferences is closely linked to revenue. In effect, this means that private actors have unprecedented power to impact the way that billions of users are able to express themselves, search and share information, and protect their privacy. Yet as private actors, they remain largely outside the reach of human rights law.

In the following, I will examine some of the legal and extralegal dimensions of this challenge. First, what does human rights law say about the obligations of private actors? Second, how have the companies themselves responded to these challenges? And third, do these approaches suffice to protect human rights online?

III HUMAN RIGHTS LAW AND PRIVATE ACTORS

Human rights law is state-centric in nature in the sense that states – not individuals, not companies – are the primary duty bearers. Legally speaking, only the state can be brought before a human rights court, such as the European Court of Human Rights, and examined for alleged human rights violations. Part of this obligation, however, is a duty upon the state to ensure that private actors do not violate human rights, referred to as the horizontal effect of human rights law. National regulation related to labor rights or data protection, for example, serves as machinery for enforcing human rights standards in the realm of private parties.

Whereas human rights law is focused on the vertical relation (state obligations to the individual), it recognizes the horizontal effect that may arise in the sphere between private parties.[52] The horizontal effect implies a state duty to protect human rights in the realm of private parties, for example, via industry regulation. A large amount of the literature related to online freedoms has been occupied with new means of state interference with human rights, for example, through new means of restricting content, engaging in surveillance, or involving Internet companies in law enforcement. These new means of state interference have been explored in several comprehensive studies, for example, by the Open Net Initiative[53] and by scholars such as Jack Balkin, who have examined the characteristics of "old-school" (pre-Internet) versus "new school" speech regulation. In contrast, less attention has been paid to the implications that arise in the sphere of horizontal relations, such as when companies, on their own initiative, remove content because it violates their terms of service, or when they exchange personal data with third parties as part of their

[52] P. van Dijk et al. (eds.), *Theory and Practice of the European Convention on Human Rights* (Antwerp, Oxford: Intersentia, 2006), p. 6.

[53] R. Deibert et al. (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010); R. Deibert et al. (eds.), *Access Denied the Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008).

business model. In the analysis that follows, emphasis will be on horizontal relations and the human rights duties and responsibilities that may be invoked in this realm.

Over the past decade, the interface between human rights law and private actors has been the focus of considerable attention, resulting in the adoption of broad soft law standards[54] and the launch of many multistakeholder initiatives, including the UN Global Compact. The UN Global Compact represents one of the core platforms for promoting corporate social responsibility (CSR), a concept that refers to a company's efforts to integrate social and environmental concerns into its business operations and stakeholder interactions. According to the UN Global Compact's framing of corporate social responsibility, businesses are responsible for human rights within their sphere of influence. While the sphere of influence concept is not defined in detail by international human rights standards, it tends to include the individuals to whom a company has a certain political, contractual, economic, or geographic proximity.[55] Arguably, CSR has some normative base in the human rights discourse, but these rights have not been well integrated:

> On the whole, relatively few national CSR policies or guidelines explicitly refer to international human rights standards. They may highlight general principles or initiatives that include human rights elements, notably the OECD Guidelines and the Global Compact, but without further indicating what companies should do operationally. Other policies are vaguer still, merely asking companies to consider social and environmental "concerns," without explaining what that may entail in practice.[56]

Even where CSR pays attention to human rights, it primarily addresses social and economic rights, in particular as it relates to working conditions and environmental and community impact, with limited attention to civil and political rights.[57] The critique of the CSR framework that it was too limited in scope, with a focus on selected rights only, was one of the drivers of the work of John Ruggie, who served as the special representative to the secretary general on issues of human rights and transnational corporation from 2005 to 2011.

[54] *See* "OECD Guidelines for Multinational Enterprises," Organization for Economic Co-operation and Development, http://mneguidelines.oecd.org/text/; "ILO Declaration on Fundamental Principles and Rights at Work," International Labour Organization, www.ilo.org/declaration/lang–en/index.htm.

[55] Business Leaders Initiative on Human Rights, U.N. Global Compact, and Office of the High Commissioner for Human Rights, "A Guide for Integrating Human Rights into Business Management," (2007), p. 8, www.ohchr.org/Documents/Publications/GuideHRBusinessen.pdf. For literature on the normative grounding of CSR in the human rights discourse, see, e.g., T. Campbell, "The Normative Grounding of Corporate Social Responsibility: A Human Rights Approach," in D. McBarnet (ed.), *The New Corporate Accountability: Corporate Social Responsibility and the Law* (Cambridge: Cambridge University Press, 2007). According to Campbell, human rights offers primarily a discursive rather than legal framework for CSR.

[56] *Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie*, ¶ 35, U.N. Doc. A/HRC/14/27 (April 9, 2010).

[57] *United Nations Global Compact*, www.unglobalcompact.org/.

In 2011, Ruggie's work culminated with an endorsement of the United Nations' Guiding Principles on Business and Human Rights (UNGP).[58] The UNGP provides a set of principles that states and businesses should apply to prevent, mitigate, and redress corporate-related human rights abuses. Contrary to the sphere of influence approach, the UNGP focuses on the potential and actual human rights impact of any business conduct.[59] The UNGP elaborates the distinction that exists between the state *duty to protect human rights* and the corporate *responsibility to respect human rights* based on three pillars, often called the "Protect, Respect, and Remedy" framework. The first pillar (Protect) focuses on the role of the state in protecting individuals' human rights against abuses committed by non-state actors; the second pillar (Respect) addresses the corporate responsibility to respect human rights; and the third pillar (Remedy) explores the roles of state and non-state actors in securing access to remedy. Ruggie's report to the Human Rights Council, which provided the basis for the UNGP, explains:

> Each pillar is an essential component in an inter-related and dynamic system of preventative and remedial measures: the State duty to protect because it lies at the very core of the international human rights regime; the corporate responsibility to respect because it is the basic expectation society has of business in relation to human rights; and access to remedy because even the most concerted efforts cannot prevent all abuse.[60]

The second pillar affords a central role for human rights due diligence by companies. Due diligence comprises four steps, taking the form of a continuous improvement cycle.[61] Companies must publish a policy commitment to respect human rights. As part of its due diligence process, a company must assess, using a human rights impact assessment, the actual and potential impacts of its business activities on human rights; remediate the findings of this assessment into company policies and practices; track how effective the company is in preventing adverse human rights impacts; and communicate publicly about the due diligence process and its results. Companies are expected to address all their impacts, though they may prioritize their actions. The UNGP recommends that companies first seek to prevent and mitigate their most severe impacts or those where a delay in response would make consequences irremediable.[62]

Since the corporate responsibility to respect human rights refers to all internationally recognized human rights, not just those in force in any one particular

[58] *Report of the Special Representative John Ruggie, Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*, U.N. Doc. A/HRC/17/31 (March 21, 2011) ("2011 Ruggie Report").

[59] See, for example, John Ruggie's annual reports from 2006 to 2011, http://business-humanrights.org/en/un-secretary-generals-special-representative-on-business-human-rights/reports-to-un-human-rights-council.

[60] 2011 Ruggie Report, p. 4.

[61] Ibid., pp. 17–20.

[62] Ibid., p. 24.

jurisdiction,[63] human rights due diligence should encompass, at minimum, all human rights enumerated in the International Bill of Human Rights.[64] The UNGP guidance on human rights impact assessments remains at a general level, without detailed descriptions of the process or orientation on how it should be adapted to particular industries. Various initiatives have since attempted to address this, which we will return to below.[65]

Whereas pillars one and three combine existing state obligations under international human rights law with soft law recommendations, pillar two is soft law only, reflecting the lack of direct human rights obligations for companies under international law.[66] The debate on whether and how to create binding human rights obligations for companies has been ongoing for more than two decades, but there is little indication that companies will be bound by human rights law in the foreseeable future.[67]

With regard to the state duties, the UNGP reiterates two existing human rights obligations. First, states must protect against human rights abuses within their territory and jurisdiction by third parties,[68] and second, states must provide individuals access to remedies for human rights abuses.[69] According to the first obligation, the state is required to take appropriate steps to prevent, investigate, punish, and redress private actors' human rights abuses that take place in its jurisdiction. Such steps include effective policies, legislation, and regulation; access to remedies; adjudication; and redress. The second obligation iterates that states must take appropriate steps to ensure that injured parties have access to effective remedies when business-related human rights abuses occur within the state's territory or jurisdiction. This includes remedies provided via judicial, administrative, legislative, or other appropriate means.

In line with this, the case law of the European Court of Human Rights (ECtHR) confirms that states have an obligation to protect individuals against violations by

[63] Ibid., p. 11.

[64] Ibid., p. 12. The International Bill of Human Rights consists of the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), and the International Covenant on Economic, Social, and Cultural Rights (1966).

[65] For guidance on human rights impact assessment, see, for example, "Rights and Democracy, Getting it Right: Human Rights Impact Assessment Guide," International Centre for Human Rights and Democratic Development, http://hria.equalit.ie/en/; FIDH, "Community-based Human Rights Impact Assessments," www.fidh.org/en/issues/globalisation-human-rights/business-and-human-rights/community-based-human-rights-impact-assessments.

[66] For an elaboration of the argument see, for example, J. Knox "The Ruggie Rules: Applying Human Rights Law to Corporations," in R. Mares (ed.), *The UN Guiding Principles on Business and Human Rights: Foundations and Implementation* (Leiden, Boston: Martinus Nijhoff, 2012).

[67] For an account of this development, see J. Ruggie, "Business and Human Rights: The Evolving International Agenda" (2007) 101 *American Journal of International Law* 819–40; Mares, *UN Guiding Principles on Business and Human Rights*, pp. 1–49.

[68] 2011 Ruggie Report, p. 1.

[69] Ibid., p. 25.

business enterprises. This entails an obligation to protect individuals against violations by business enterprises as third parties as well as those acting as state agents. In the first case, the human rights violation is constituted by the state's failure to take reasonable measures to protect individuals against abuse by business enterprises; in the latter, the abusive act of the business enterprise is attributed to the state, so that the state is considered to directly interfere with the rights at stake.[70] The case law of the ECtHR on violations by business enterprises acting as state agents concerns both the case where the state owns or controls business enterprises and the case where private corporations exercise public functions through procurement contracts and privatization of public services.[71]

Ruggie's framework, which has been widely praised and endorsed by states as well as business enterprises, has also been criticized for its slow uptake, its ineffectiveness, and for not creating binding obligations on companies.[72] Yet, a hard-law punitive approach has also long had its skeptics, and numerous empirical studies have spoken to the significance of social factors, both internal and external, in affecting companies' behavior.[73]

The UNGP has resulted in several follow-up initiatives at both the global and regional level. At the global level, a UN working group on human rights and transnational corporations and other business enterprises was established in June 2011 to promote the effective and comprehensive dissemination and implementation of the UNGP.[74] After completing its initial three-year appointment in 2014, the group had its mandate extended for another three-year term.[75] The group has, among other things, produced a "Guidance" on the development of national action plans on business and human rights.

[70] S. Lagoutte, "The State Duty to Protect against Business-Related Human Rights Abuses: Unpacking Pillar 1 and 3 of the UN Guiding Principles on Human Rights and Business," Working Paper, *Human Rights' Research Papers*, No. 2014/1 (2014), p. 9.

[71] *See, e.g.*, *Tatar* v. *Romania*, Eur. Ct. H.R., App. No. 67021/01 (January 27, 2009); *Fadeyeva* v. *Russia*, Eur. Ct. H.R., App. No. 55723/00 (June 9, 2005); *Öneryildiz* v. *Turkey*, Eur. Ct. H.R., App. No. 48939/99 (Grand Chamber, November 30, 2004); *Guerra & Others* v. *Italy*, Eur. Ct. H.R., App. No. 14967/89 (Grand Chamber, February 19, 1998); *López Ostra* v. *Spain*, Eur. Ct. H.R., App. No. 16798/90 (December 9, 1994).

[72] S. A. Aaronson and I. Higham, "'Re-Righting Business': John Ruggie and the Struggle to Develop International Human Rights Standards for Transnational Firms" (2013) 35 *Human Rights Quarterly* 333–64; D. Bilchitz, "A Chasm between 'Is' and 'Ought'?: A Critique of the Normative Foundations of the SRSG's Framework and the Guiding Principles," in S. Deva and D. Bilchitz (eds.), *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect?* (Cambridge: Cambridge University Press, 2013), pp. 107–37.

[73] C. Methven O'Brien and S. Dhanarajan, "The Corporate Responsibility to Respect Human Rights: A Status Review," Working Paper, National University of Singapore, 2015/005 (2015), 4.

[74] See the presentation of the working group by the UN High Commissioner for Human Rights, www.ohchr.org/EN/Issues/Business/Pages/WGHRandtransnationalcorporationsandotherbusiness.aspx.

[75] The website of the working group is available at: www.ohchr.org/EN/Issues/Business/Pages/WGHRandtransnationalcorporationsandotherbusiness.aspx.

At the European level, the European Commission has produced sector-specific guides on UNGP implementation in relation to three business sectors, including the information and communication technology (ICT) sector.[76] The guide is not a legally binding document, but translates the expectations of the UNGP to the specifics of the business sector at a rather generic level. In relation to the ICT sector, the guide stresses that the right to privacy and to freedom of expression can be particularly impacted by companies in the ICT sector.[77] The guide focuses on the state pressure that companies may be subjected to when they operate in contexts where the national legal framework does not comply with international human rights standards (i.e., a vertical conflict). In contrast, the negative human rights impact that may flow from the company's governance of content or tracking of user behavior is not addressed, and, as such, the guide provides limited guidance on horizontal conflict (i.e., relations between private actors). This focus on the vertical conflict is also dominant in the Global Network Initiative (addressed below) and indicates that the human rights discourse by Internet companies tends to highlight push-back strategies against illegitimate government requests, with less attention being paid to the human rights impact of the company's own actions.

This points to an unanswered question: What would human rights law and supplementary guidelines such as the UNGP say about the responsibility of private actors that potentially affects the rights of billions of individuals worldwide?

As stated above, states are obligated to prevent human rights violations by private actors, and private actors have a moral obligation to respect human rights. States cannot delegate their human rights obligations to a private party, and they are obligated to ensure that appropriate regulations result in human rights–compliant business practices. Moreover, each company has a responsibility to assess its actual human rights impact, i.e., the way that its operational practices, services, and products impact on its users' human rights.

The state obligation to ensure human rights entails both a positive and negative element. It requires the state to refrain from certain conduct, but also to take positive steps to ensure the enjoyment of the right in question. Freedom of expression, for example, requires that the state refrain from engaging in censorship, but also that it – via national regulation – enables freedom of the press.[78] The measures and behavior required of businesses to fulfill their responsibility to respect human rights should be

[76] The guide is available at: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_0.pdf.

[77] Institute for Human Rights and Business and SHIFT for the European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights," 2012, Section 2.

[78] In the ruling *Editorial Board of Pravoye Delo and Shtekel* v. *Ukraine*, Eur. Ct. H.R., App. No. 33014/05 (May 5, 2011), the European Court of Human Rights for the first time acknowledged that Article 10 imposes on states a positive obligation to create an appropriate regulatory framework to ensure effective protection of journalists' freedom of expression *on the Internet*.

provided for by each state's respective national laws and policies in all the various areas in which these laws and policies touch on business activities.[79]

Arguably, in many specific cases, such regulation exists and businesses do, to a large extent, respect human rights standards by complying with legal rules. It would be too optimistic, however, to assume that governments and subordinate public authorities always have the ability and the will to regulate business conduct in line with human rights requirements,[80] not least in relatively new policy areas such as online freedom of expression. Moreover, in the case of online service providers, there is an additional layer of responsibility. Not only does the company have responsibilities in relation to its employers and community, it also directly or indirectly affects its users, who in practice might be billions of people.

Historically, controversial cases have involved privacy and freedom of expression in particular, yet with some legal subtleties that distinguish the two rights in question. As Lisl Brunner notes in Chapter 10, the right to privacy has some protection in national legislation (in particular in Europe) in the form of data-protection laws that stipulate principles, procedures, and safeguards that public and private actors must adhere to when collecting and processing personal data.[81] In the EU context, for example, Google is subject to the European Data Protection Directive, which imposes conditions and safeguards for data collection, processing, and exchange on public institutions and private companies alike. When Google, as in the *Google Spain* case, violates a user's right to privacy, the company is the direct duty bearer under Spanish data protection legislation.[82]

In contrast, Internet platforms are rarely subject to regulation concerning the negative impact they may have on freedom of expression. When content is filtered, blocked, or taken down by Twitter because it allegedly violates the community standards, there is limited guidance in international human rights law, and rarely is there national legislation that applies. In these situations, the company is acting in a judicial capacity, deciding whether to allow content to stay up or to remove it according to internal governance practices and standards, but without the human rights requirements that would apply if Twitter were a state body rather than a private company. For example, if Twitter removes posts for violating its community standards, this does not trigger international human rights law. In contrast, if a state-owned Twitter were to remove content from the public domain, this practice would have to follow the three-part test governing limits on freedom of expression. According to the three-part test, any limitation on the right to freedom of expression must be provided by law that is clear and accessible to everyone; it must pursue one

[79] Methven O'Brien and Dhanarajan, "The Corporate Responsibility to Respect Human Rights," 5.

[80] Ibid.

[81] It should be noted that informational privacy covers only one aspect of privacy.

[82] *Google Spain SL, Google Inc.* v. *Agencia Española de Protección de Datos, Mario Costeja González*, CJEU, Case C-131/12 (May 13, 2014).

of the purposes set out in Article 19, paragraph 3 of the ICCPR; and it must be proven as necessary and the least restrictive means required to achieve the purported aim.[83]

A related challenge concerns the cases where content is taken down because it allegedly violates national law in the country of operation. As mentioned, Internet services hosted in the United States are insulated from liability under Section 230 of the Communications Decency Act. Concerning copyright infringements, however, Section 512 of the Digital Millennium Copyright Act codifies limited liability, which means that Internet services are required to remove alleged illegal content when notified of its presence on their service, or they will face liability for that content.[84] This is similar to the European approach, which imposes limited liability on online services through the Electronic Commerce Directives. Both regimes have been criticized for encouraging businesses to privately regulate their affairs, with freedom of expression implications.[85] When Facebook, for example, acts upon an alleged copyright violation by removing the content, it is making decisions with freedom of expression implications, yet as a private actor it is not obligated to follow the three-part test prescribed by human rights law. The regimes that insulate online platforms from liability for the third-party content they carry also effectively insulate them from liability when they take down protected content out of fear of liability (e.g., alleged copyright infringement).

In sum, the practices of online platforms (especially macro or authority gatekeepers) have effects on freedom of expression and privacy far beyond their roles as employers and members of a community. Do the power, influence, and capacity to affect democratic life qualify for a special class of public interest companies that invite additional corporate responsibilities beyond the duty to respect human rights?[86] Does it accentuate the positive obligation on the state to legislate the obligations of these companies? Although Ruggie briefly touched upon these issues (with prisons as an example), there is limited guidance in his work as to the answers. In addition, although these companies' negative impact on privacy is regulated in some regions of the world, their potential negative impact on freedom of expression is not. Neither the United States nor Europe has regulations to protect against the potential negative impact that the content-regulation practices of a major Internet company could have on freedom of expression. Moreover, the human rights

[83] 2011 La Rue Report.

[84] *See* US Copyright Office, "The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary," www.copyright.gov/legislation/dmca.pdf.

[85] *See* Schesser, "A New Domain for Public Speech"; I. Brown, "Internet Self-Regulation and Fundamental Rights," *Index on Censorship* (2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1539942; B. Frydman and I. Rorive, "Regulating Internet Content through Intermediaries in Europe and the USA," (2002) 23(1) *Zeitschrift für Rechtssoziologie* 41–59.

[86] *Business and Human Rights: Towards Operationalizing the "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/11/13 (April 22, 2009), at 17.

responsibilities of Internet companies are largely discussed in relation to illegitimate government requests, as exemplified by the Global Network Initiative, addressed below.

The above challenges are rooted in the gray zone where human rights law ends and corporate social responsibility begins, and it is in this zone that online platforms operate. Their practices may affect human rights immensely, yet they are not regulated with a view to their impact on freedom of expression, freedom of information, or privacy, except in some specific cases. Moreover, even when Internet companies are subjected to regulation, such as on data protection, the past ten years have illustrated the tremendous challenge of holding those companies accountable to these standards. As such, there is a lacuna in checks and balances concerning these private actors. This is paradoxical, since online, these private actors are at the center of the Internet's democratizing force and exercise significant human rights impacts on their users.

IV THE UPTAKE OF HUMAN RIGHTS WITHIN INTERNET COMPANIES

As previously mentioned, most human rights cases related to the ICT sector have concerned freedom of expression and the right to privacy. In December 2008, this led to the launch of the first industry initiative concerned with the human rights compliance of Internet companies, the Global Network Initiative, addressed below. First, however, it should be noted that most major global platforms emphasize freedom of expression as a core element of their business. Facebook's mission, for example, is framed in the language of freedom of expression and association by its founder, Mark Zuckerberg:

> There is a huge need and a huge opportunity to get everyone in the world connected, to give everyone a voice and to help transform society for the future. . . . By giving people the power to share, we are starting to see people make their voices heard on a different scale from what has historically been possible. These voices will increase in number and volume. They cannot be ignored. Over time, we expect governments will become more responsive to issues and concerns raised directly by all their people rather than through intermediaries controlled by a select few.[87]

At Twitter, the company vision is closely linked to freedom of expression and the new digital means of realizing this right: "Our legal team's conceptualization of speech policies and practices emanate[s] straight from the idealism of our founders – that this would be a platform for free expression, a way for people to disseminate their ideas in the modern age. We're here in some sense to implement that vision."[88]

[87] S. Ard, "Mark Zuckerberg's IPO Letter: Why Facebook Exists," Yahoo! Finance, February 1, 2012, http://finance.yahoo.com/news/mark-zuckerberg's-ipo-letter–why-facebook-exists.html.

[88] Ammori, "The 'New' New York Times" at 70.

Google stresses that the company "[has] a bias in favor of people's right to free expression in everything we do."[89]

The Global Network Initiative (GNI) has, since 2008, been the common venue for some of the major Internet companies' discourse on human rights norms related to freedom of expression and privacy.[90] The GNI is a multistakeholder group of companies, members of civil society, investors, and academics that was launched in the United States. Formation of the GNI took place against the backdrop of two particular incidents. One was Yahoo's handover of user information to Chinese authorities, thereby exposing the identity of a Chinese journalist, leading to his arrest and imprisonment. The second was Google's launch of a censored search engine in China.[91]

The goal of the GNI is to "protect and advance freedom of expression and privacy in the ICT sector."[92] At the time of writing, Google, Yahoo, Facebook, Microsoft, and LinkedIn were the Internet company members, whereas seven of the big telecommunication companies – united in the parallel initiative Telecommunications Industry Dialogue – were admitted as members in 2017.[93] The baseline for GNI's work consists of four core documents, developed in broad collaboration among the participants: the "Principles," the "Implementation Guidelines," the "Accountability, Policy and Learning Framework," and the "Governance Charter." The Implementation Guidelines operationalize the overall principles in detailed guidance to companies, whereas the Governance Charter describes how the GNI is governed in order to ensure integrity, accountability, relevance, effectiveness, sustainability, and impact. The Accountability, Policy, and Learning Framework supplements the Governance Charter with more detail on how the work of the GNI is carried out.[94]

Since its inception, the GNI has been criticized for lack of participation (including by smaller and non-US companies), for not being independent enough in the

[89] C. Cain Miller, "Google Has No Plans to Rethink Video Status," *The New York Times*, September 14, 2012, http://perma.cc/LX2F-DKE9. Commentators have argued that Google's philosophy likely impacts the thinking at companies across Silicon Valley, since its alumni have been shaped by shared experiences and an ongoing informal network, which shares experiences on difficult questions. Ammori, "The 'New' New York Times" at 69.

[90] The website is available at: www.globalnetworkinitiative.org.

[91] *See* C. M. Maclay, "An Improbable Coalition: How Businesses, Non-Governmental Organizations, Investors and Academics Formed the Global Network Initiative to Promote Privacy and Free Expression Online," PhD thesis, Northeastern University (2014) (providing a detailed account of the formation of the GNI).

[92] The GNI Principles are available at: http://globalnetworkinitiative.org/principles/index.php.

[93] "The Global Network Initiative and the Telecommunications Industry Dialogue join forces to advance freedom of expression and privacy," Global Network Initiative, www.telecomindustrydialogue.org and http://globalnetworkinitiative.org/news/global-network-initiative-and-telecommunications-industry-dialogue-join-forces-advance-freedom.

[94] "Core Commitments," Global Network Initiative, https://globalnetworkinitiative.org/corecommitments/index.php.

assessment process,[95] for the lack of a remedy mechanism, for insufficient focus on privacy by design, and for a lack of accountability.[96] These criticisms speak to the inherent challenge of having an industry define its own standards and procedures for respecting users' rights to privacy and freedom of expression. Moreover, it has been argued that the protection of users' rights runs contrary to business interests.[97] In relation to the latter challenge, it is important to note some fundamental differences between the rights in question and the challenges they pose.

Both privacy and freedom of expression protect individual freedoms by setting limits on state (and private actor) intrusion. With privacy, these limits are formulated as principles that guide how and when personal information may be collected, processed, and exchanged with a third party. In relation to data protection, it seems paradoxical to expect that the boundaries for data collection and use will be most effectively protected by companies whose business model is built around harnessing personal data as part of their revenue model. Whereas companies may push back against illegitimate government requests for user data, they are less likely to be a sufficiently critical judge of their own business practices, not least when these are closely linked to their business model.

With freedom of expression, the issue is slightly different. Here, the potential conflict between human rights standards and business practices stems from several factors, more indirectly linked to the revenue model. These factors include: unclear liability regimes that might incentivize the company to remove alleged illegal content without sufficient due process safeguards and that position the company as the final authority regarding which content to remove; pressure from governments to block, filter, or remove content; and internally defined standards regarding content moderation and enforcement of the standards.

As reflected in its baseline documents, the GNI is strongly anchored in the initial narrative of providing guidance to Internet companies in countries where local laws conflict with international human rights standards, rather than the systematic human rights impact assessment suggested by the UNGP. The GNI Principles state:

> The right to freedom of expression should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws or

[95] In June 2014, the GNI board consolidated the assessment process into a two-stage model: first, self-reporting from the companies to GNI after one year of membership; second, assessment of each company member every two years. The assessment is carried out by a list of GNI-approved assessors and examines the policies, systems, and procedures put in place by the company to comply with the GNI Principles.

[96] MacKinnon, *Consent of the Networked*, pp. 179–82. For news coverage on this, see, for example, L. Downes, "Why no one will join the Global Network Initiative," *Forbes*, March 30, 2011, https://www.forbes.com/sites/larrydownes/2011/03/30/why-no-one-will-join-the-global-network-initiative/#275f5878d782.

[97] D. Doane, *The Myth of CSR: The Problem with Assuming That Companies Can Do Well While Also Doing Good Is That Markets Don't Really Work That Way* (Stanford, CA: Stanford Graduate School of Business, 2005), pp. 22–29.

> standards. . . . Participating companies will respect and protect the freedom of expression rights of their users when confronted with government demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to information and ideas in a manner inconsistent with internationally recognized laws and standards.[98]

Similarly, the Implementation Guidelines for Freedom of Expression discuss company practices in relation to "Government Demands, Laws and Regulations"[99] rather than human rights impacts. These principles illustrate that for the GNI, threats to freedom of expression are framed as illegitimate government behavior, and its role is to assist companies with human rights–compliant conduct when confronted with, for example, an overly broad request for filtering or blocking of content.

While industry push-back against illegitimate government requests undoubtedly addresses a relevant human rights problem, it is not sufficient to comply with the responsibilities set out in the UNGP. Those responsibilities require companies to know their actual and potential human rights impacts, to prevent and mitigate abuses, and to address adverse impacts they are involved in. In other words, companies must carry out human rights due diligence across all operations and products. The process of identifying and addressing the human rights impact must include an assessment of all internal procedures and systems, as well as engagement with the users potentially affected by the company practices. It follows that for GNI members such as Yahoo, Facebook, and Google, it is not sufficient to focus on government requests and human rights–compliant practices in this realm. Rather, assessment is needed on the freedom of expression impacts that may flow from all company practices, including, for example, when the company enforces community standards or takes down content based on alleged copyright infringement.

Internet platforms such as Facebook and YouTube influence the boundaries of what users can say and view online via their terms of service. Enforcement of these terms of service must work effectively at a scale of millions of users, including in high-profile controversies such as the "Innocence of Muslims" video,[100] as well as in more routine cases where users report objectionable content. In practice, the terms

[98] "GNI Principles: Section on Freedom of Expression," Global Network Initiative, http://globalnetworkinitiative.org/principles/index.php#18.

[99] "GNI Implementation Guidelines: Section on Freedom of Expression," Global Initiative Network, http://globalnetworkinitiative.org/implementationguidelines/index.php#29.

[100] In 2006, the "Innocence of Muslims" video sparked outrage in countries throughout the Middle East for its perceived criticism of Islam. While YouTube allowed the video to remain online in the United States, stating that the video did not break US law, it was removed in countries where it violated local laws, as well as in Libya and Egypt, where it did not violate local laws. Commentators have argued that the case is illustrative of the way private companies carry out worldwide speech "regulation" – sometimes in response to government demands, sometimes to enforce their own terms of service. S. Benesch and R. MacKinnon, "The Innocence of YouTube," *Foreign Policy*, October 5, 2012, http://foreignpolicy.com/2012/10/05/the-innocence-of-youtube/.

are translated into specific definitions and guidelines that are operationalized by employees and contractors around the world, who "implement the speech jurisprudence"[101] by making decisions on which content to leave up or remove.[102] According to Google, for example, deciding on the limits of freedom of expression for a billion users is "a challenge we face many times every day."[103] Yet, an intermediary's terms of service and the means of enforcing those terms are not part of the GNI norms and standards.

A similar challenge is found in relation to privacy. The GNI Principles iterate that

> the right to privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws and standards. . . . Participating companies will respect and protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards.[104]

The corresponding section in the Implementation Guidelines addresses "Government Demands, Laws and Regulations" as well as "Data Collection." The latter is concerned with risk analysis of the specific national jurisdiction in which the company operates.[105] In line with its counterpart on freedom of expression, the GNI Principles and the attached Implementation Guidelines focus merely on the negative human rights impact caused by external pressure from governments, whereas internal mechanisms related to data processing and exchange remain unchallenged.

This is unfortunate, given that the business model of online platforms, which is based on targeted advertising, is increasingly accused of promoting privacy violations. On Facebook, for example, advertisements are targeted to individual users' interests, age, gender, location, and profile. This enables advertisers to select specific groups and target advertisements either on the Facebook website or on other websites using Facebook's advertising services. This business model has caused a number of privacy-related controversies. Most recently, in 2015, a Belgian research study criticized Facebook's data-processing practices and concluded, in relation to Facebook's social media plug-ins, that it processes the personal data of its users as well as the data of all Internet users who come into contact with Facebook, without the necessary consent for "tracking and tracing" or consent for the use of cookies.[106]

[101] Ammori, "The 'New' New York Times" at 76.
[102] The main channel for identifying objectionable content is user reporting enabled by technical features in the platform.
[103] Cain Miller, "Google Has No Plans to Rethink Video Status."
[104] "GNI Principles: Section on Privacy," Global Network Initiative, http://globalnetworkinitiative.org/principles/index.php#19.
[105] "GNI Implementation Guidelines, Section on Privacy," Global Network Initiative, http://globalnetworkinitiative.org/implementationguidelines/index.php#28.
[106] "KU Leuven Centre For IT & IP Law and Iminds-Smit Advise Belgian Privacy Commission in Facebook Investigation," KU Leuven, www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation.

As a follow-up to the study, the Belgian Privacy Commissioner issued a set of recommendations to Facebook.[107] This is just one example of how Internet platforms can impact the privacy of their users due to their online business model rather than government pressure. Yet, these aspects of company practice in relation to privacy are not included in the GNI norms and standards.

In sum, several of the major Internet companies frame their core mission in terms of freedom of expression and engage in industry networks such as the GNI that are dedicated to protecting human rights norms and standards in the online domain. Yet, the effectiveness of the GNI to protect human rights is challenged by several factors. First, it is based on a voluntary commitment, with no binding obligations on companies. Second, it is largely occupied with limiting and safeguarding against undue government pressure on companies, whereas content regulation and user tracking and profiling are not covered, despite their potential human rights impact.

V CHALLENGES TO HUMAN RIGHTS PROTECTION IN A PRIVATIZED ONLINE DOMAIN

In this final section, I will discuss whether the frameworks that currently govern the activities of online platforms are sufficient to provide the standards and mechanisms needed to protect and respect human rights online, drawing on the challenges outlined in the previous section.

A first challenge relates to the circumstance that core civil and political rights (privacy, freedom to search for information, freedom to express opinion) are exercised within a commercial domain, with companies holding unprecedented power over the boundaries and conditions for exercising those rights. Arguably, some of the most widely used platforms and services may affect public and private life in a way traditionally reserved for public authorities, yet they are largely free from binding standards to protect freedom of expression and privacy. Whereas this governance gap may have a positive impact on rights and freedoms in a state-repressive context, it does not take away the challenges that this raises within democratic societies. Companies that have a substantial impact on the environment are increasingly subjected to national regulations for business conduct, yet similar attention has not been paid to online platforms. Scholarship is only now beginning to address the broader societal implications of private ownership of the online infrastructure of search, expression, and debate that results in the double logic of user empowerment and commodification of online activity.[108]

[107] Commission for the Protection of Privacy, Recommendation No. 04/2015 (May 13, 2015), www.privacycommission.be/sites/privacycommission/files/documents/recommendation_04_2015_0.pdf.

[108] J. Van Dijck and T. Poll, "Understanding Social Media Logic" (2013) 1 *Media and Communication* 2–14.

Human rights law is state-centric in nature and holds no direct human rights obligations for private actors. The governance gap accompanying globalization was a core driver for the development of the UNGP, and therefore for asserting the corporate responsibility to respect human rights as a freestanding, universally applicable minimum standard of business conduct – one driven by global social expectation while at the same time based on international law.[109] Nonetheless, the soft law framework of the UNGP, however widely endorsed, remains voluntary by nature, as do industry initiatives such as the GNI.

Further, even these soft law frameworks have significant gaps. In 2016, the five GNI member companies were positively assessed by GNI-appointed assessors for compliance with GNI norms and standards.[110] There are, however, several shortcomings to this assessment process. First, it does not entail a comprehensive human rights impact assessment of all business practices as prescribed by the UNGP, but instead focuses more narrowly on the issues that the GNI members have chosen to include in their development of norms and standards. This means that push-back strategies against illegitimate government requests are the focus of assessment, whereas the impact of business processes concerned with taking down content that does not adhere to internally defined business standards is not considered. Second, the terms and conditions of the assessment process (including the selection of assessors) are carried out within the circuit of the GNI, providing the companies subject to review with influence on the baseline for this review.

Another human rights weakness in these soft law frameworks concerns the limited access to remedy mechanisms. As emphasized by the third pillar of the UNGP, states must take appropriate steps to ensure access to an effective remedy when business-related human rights abuses occur within their jurisdiction. Despite the impact that online platforms have on users' rights of expression and privacy, limited channels exist for users to address potential or actual infringements of such rights.[111] In sum, given the impact that these companies potentially have on human rights in terms of scope and volume, the voluntary approach seems insufficient to provide the billions of Internet users with the level of protection they are entitled to according to international human rights law.

This brings us to the second challenge, namely, whether the state has a positive obligation to legislate the obligations of these companies. Does the character of major online platforms call upon states to provide human rights guidance and

[109] C. Methven O'Brien and S. Dhanarajan, "The Corporate Responsibility to Respect Human Rights" at 5.

[110] The assessment report from July 7, 2016, is available at: http://globalnetworkinitiative.org/content/public-report-201516-independent-company-assessments-0.

[111] The importance of access to remedies in an online context is stressed in the Council of Europe's guide to human rights for Internet users. Council of Europe, "Recommendation of the Committee of Ministers to Member States on a Guide on Human Rights for Internet Users," MSI-DUI (2013) 07Rev7 (April 16, 2014).

possible regulation of these actors? Until now, neither the United States nor Europe has taken up this challenge. In April 2016, the European Union concluded a four-year-long comprehensive data protection reform, including, among other things, increased focus on the practices of online platforms.[112] Yet while online platforms' negative impact on privacy has received some attention, their impact on freedom of expression has not. As such, there is no national regulation to protect against the potential negative impact that a major Internet platform may have on freedom of expression. As previously mentioned, in the United States, the First Amendment and the public forum doctrine protect expressions in the public domain, but on the Internet, private companies in control of communicative platforms are free to decide the types of speech they support. This includes taking down or blocking and filtering expression that would otherwise be protected by the First Amendment. In consequence, expression is less protected in the online domain, despite the wide opportunities online platforms provide for new means of realizing freedom of expression. Likewise, in the United States, there is no general data protection regulation covering these private actors, and thus no clear boundaries for the companies' handling of personal data.

However urgent, several factors indicate that a solution will not be forthcoming in this area any time soon. The transnational nature of online platforms makes it difficult for states to address their impact on freedom of expression or privacy domestically. Moreover, up till now, the United States and European states have been unable to agree on the scope of freedom of expression, for example concerning protected speech, and they have lacked a common standard for data protection. Whereas the European approach is geared toward both negative and positive state obligations in the area of freedom of expression and privacy (e.g., imposing regulations on private actors), the US approach has focused on the negative state obligation to avoid interference. While the issues raised have received some scholarly attention, they have not surfaced as prominent policy issues in either Washington or Brussels. As such, it is not realistic to expect common US/EU policy for the major online platforms in the foreseeable future.

If European states were willing to invoke their positive state obligation in order to protect freedom of expression online, they would have to apply national standards for protected speech to the online domain. In consequence, Internet platforms would have to comply with a number of different standards for protected speech, depending on the location of their users. Although this would most likely cause controversy and resistance from the companies, it is in principle no different from the current situation, in which platforms adhere to different regimes for unlawful

[112] The General Data Protection Regulation (EU 2016/679) has been highly controversial and its implications widely addressed by scholars and activists alike. *See, e.g.*, A. Dix "EU Data Protection Reform Opportunities and Concerns" (2013) 48 *Intereconomics* 268–86; D. Naranjo, "General Data Protection Regulation: Moving forward, slowly," *European Digital Rights*, June 3, 2015, https://edri.org/author/diego/page/5/.

content depending on the national context in which they operate. In other words, while both Facebook and Google have processes for dealing with alleged unlawful content in a specific national jurisdiction, they might also have processes for ensuring that no content is taken down unless it satisfies the criteria set out in human rights law. Such a mechanism would ensure that the companies' commitment to freedom of expression is operationalized not only in relation to government pressure, but also in relation to the day-to-day practices that govern their communities of users.

In conclusion, divergence in the US and European approaches to privacy and freedom of expression, as well as the complexity of defining legal responsibilities in the face of conflicting local laws, means that a concerted state effort in this field is unlikely. Yet authoritative human rights guidance for the major online platforms is urgently needed in order to clarify the scope of their responsibilities and, more importantly, to ensure that their impact on billions of users' rights is mitigated and potential violations are remedied.