7 Rights Talk: In the Kingdom of Online Giants

Rikke Frank Jørgensen

Introduction

Powerful companies like Facebook and Google have the ability to influence human rights in ways traditionally reserved for governments yet operate outside the direct reach of human rights law. Although their impact on a number of human rights is widely acknowledged, including within the industry itself, the regulation of this impact varies considerably. In the European Union context, for example, the privacy rights of Facebook's and Google's users are regulated via data protection regulation, whereas their potential negative impact on freedom of expression is not. It is fair to say that in most national contexts (including that of the United States), the companies' responsibilities in regard to international human rights law are governed by soft-law frameworks and voluntary measures defined and enforced by the industry itself (for an extensive elaboration of this point, see the chapters by Callamard and Land in this volume).

Whereas some of the subsequent chapters extensively discuss the responsibility of these companies vis-à-vis human rights law, the focus of this chapter is on the internal storytelling around human rights. Using Google and Facebook as empirical case studies, the chapter focus on three corporate narratives related to the companies' commitment to respect human rights. The first narrative concerns the role the companies are depicted to play as safeguards against government overreach. The second narrative relates to their role as cooperators with governments. Finally, the third narrative concerns the way privacy is constructed within company discourse.

With reference to Luhmann's (1993) communicative theory of social systems, the narratives represent specific ways of producing, reproducing,

and legitimizing meaning by staff at Facebook and Google. As part of this sense making, the narratives serve to maintain the boundary between a relatively closed system and its environment and to legitimize specific practices within the organizations. The analysis also draws on the notions of *platform* and *infrastructure*, which are used to unpack and critically discuss some of the underlying assumptions in the corporate storytelling.

The chapter will argue that the companies' efforts vis-à-vis human rights tend to focus exclusively on state interference and pays limited attention to the companies' own business practices and the way the data-driven economy informs those practices.

Methodology

The analysis draws in part on empirical data collected as part of a two-year research project on the commercialized public sphere (Jørgensen 2017a, 2017b). The research project relied on a context-oriented qualitative approach, including publicly available statements from the two companies, terms of service, and policies, as well as semistructured interviews with company staff, primarily in Europe and the United States. The interviews focused on the internal discourse and sense making related to human rights; the translation of this normative basis into specific features or products, and the governance mechanisms set up to enforce the norms. The interviewed were staff with responsibility for human rights (e.g., participation in the Global Network Initiative; GNI), public policy, privacy, community operations (Facebook), and removal requests (Google). However, meetings were also conducted with technical staff (Google), as well as more research-oriented staff working on education and user experience (Google). With a few exceptions, the respondents had been with the companies for some years and carried some level of responsibility within the organization. In total, twenty-one interviews were conducted (thirteen Google, eight Facebook), and twenty publicly available talks and testimonies were analyzed in relation to the above themes. The public talks and testimonies were selected on the basis of topic (relevance) and located via YouTube and the Zuckerberg Files, which is a digital archive of all public statements made by Mark Zuckerberg, from 2004 to 2018.[1]

While the three narratives presented in the following are derived from the research project, it is important to note that they are neither exclusive

nor exhaustive. Rather, they are chosen for this chapter as telling examples of how the two organizations understand their role and responsibility in relation to human rights.

Analytical Framework

The analysis relies on the concept of frames (Goffman 1974; Johnston 2005; Tannen 1993), as sets of relatively coherent meanings that organize the identity and activities of an individual or organization. As such, frames are used to situate events, fashion a shared understanding of the world, and guide problem-solving (Barnett and Finnemore 2004, 33). In short, concepts such as *freedom of expression* and *privacy* do not have an objective meaning but are framed in particular ways deemed to give meaning in a specific context—in this case, that of Google and Facebook. This implies attention to ways in which individuals and organizations frame and explain particular meanings, as well as how these meanings are translated into practice (Latour and Woolgar 1986).

It also considers organizations as communicative systems, inspired by the German sociologist Niklas Luhmann and his extensive theory on social systems (Luhmann 1993). According to this framework, each system (e.g., an organization) has a distinctive identity that marks the border between system and the environment and is constantly reproduced through communicative processes. These communicative processes (sense making) are governed by "interpretation codes" that guide how information is selected, processed, and understood within the specific organization—for example, true/false (a scientific system), economic gains/losses (a business system), legal/illegal (a justice system) (Luhmann 1992, 253). In relation to human rights such as the right to privacy, this has the function of protecting the boundaries of specific systems—for instance, by preventing sensitive information from one context from proliferating into other ones (Hornung and Schnabel 2009, 85).

In terms of understanding the services that Facebook and Google provide, the analysis is inspired by the literature on platforms and infrastructures as two notions increasingly used to describe the companies, but with different policy implications. The notion of infrastructure is generally used to describe the underlying foundation of a system or organization. Examples include transportation systems such as highway, railway, and airline

systems; communication systems such as telephone networks and postal services; and basic public services and facilities such as schools and water systems (Frischmann 2012, 4). Infrastructure often exists as an invisible, taken-for-granted resource, whereas a breakdown in the infrastructure can make its design and effects visible (Bowker et al. 2010, 97–98). The term "platform" is commonly used to characterize the economic model of the social web (Helmond 2015, 5) and connotes openness, functionality, empowerment, and neutrality (Pangrazio 2016, 2–3), whereas in fact the economic model, technical design, and policies of platforms steer user interaction in certain directions. Van Dijck (2013, 29) has importantly noted that "a platform is a mediator rather than an intermediary," because it shapes sociocultural performance rather than merely facilitating it. As such, the owners of the platforms—the companies—hold great power over the wide range of social activities they facilitate, which include small- or large-scale communication, public debate, social interaction, information search, and so forth (van Dijck and Poell 2013). Since online platforms serve varied audiences that include users, shareholders, third parties, and advertisers, part of their governance challenge is to manage expectations between a diverse range of interests in order to serve the company's business interests (Ananny and Gillespie 2016).

Arguably, major online platforms effectively function as social infrastructures—that is, as foundational and largely unseen services that govern public action (Bowker and Star 1999). They are embedded, taken for granted, ruled by unquestioned standards, and visible only when seen to be failing (Star and Ruhleder 1996). While traditional infrastructures undergo *platformization* (Plantin et al. 2016, 298), online platforms experience *infrastructuralization* as companies exploit the power of platforms to "gain footholds as the modern-day equivalents of the railroad, telephone, and electric utility monopolies of the late 19th and the 20th centuries" (Ananny and Gillespie 2016, 14–15). The increasingly infrastructural nature of major platforms makes it difficult for people to leave them (Ananny and Gillespie 2016), just as the platforms benefit from the socio-technical investments users have made over time: "profiles and identities that have been tended to for years; networks and relationships that exist nowhere else and would be nearly impossible to recreate; media and metadata embedded within particular platforms and difficult to extract" (ibid., 1).

The above perspectives on platforms and infrastructures remind us that the notions used to describe the services provided by Google and Facebook carry specific—and often contested—meanings. Moreover, if major platforms are considered to function as societal infrastructures, this prompts consideration of the appropriate regulatory response—a point I return to in the Conclusion.

First Narrative: Google and Facebook Protect Their Users against Government Overreach

In March 2016, US lawyer and commentator Jeffrey Rosen argued that he was happy with the governance of freedom of expression conducted by Facebook, Google, and Twitter. Rosen had previously described these companies as more powerful than any king when it comes to free speech decisions in the online domain (Rosen 2012).

> Especially in light of these new pressures, I really have to express admiration for Monica, and Juniper and their colleagues at Twitter . . . they are trying to tread an incredibly delicate and difficult line where (one has) all of these pressures from Europe and from society to take speech down and to ban speech, and yet this constitutional principle that says it has to stay up unless it is intended to cause harm. . . . I really have concluded that if someone has to do it I would rather that it be these two incredible powerful women than a government, like Europe, or an international body like the illiberal groups that are calling for repression of speech at the network level, led by China and Russia. (Rosen 2016)

The Rosen quotation reflects the first narrative discussed here, namely, how staff at both Google and Facebook frame their human rights responsibility as an obligation to safeguard users against overreach by governments. The interviewees from both companies explicitly acknowledge the importance of protecting and advancing human rights and emphasize their services as enablers of specific rights, most notably freedom of expression. Services such as Google Search and Facebook's social network are seen to counter existing inequalities and contribute to making the world a more just place. "There is asymmetry. Those in power can call a newspaper or television and get access. Ordinary people can't. We want to rectify that asymmetry in communication power" (Facebook interview #2, 2015). "Googlers share a common view of the world; more access to information makes the world a better place" (Google interview #3, 2015). Also, staff at both companies

refer to freedom of expression as a crucial element of the corporate identity and as a guiding normative base. "Censorship is against everything Facebook stands for" (Facebook interview #2, 2015). "Freedom of expression runs deep in Google's engineering culture" (Google interview #10, 2015).

When questioned about perceived threats to human rights in relation to their services, all respondents referred to government intervention at either a formal or an informal level. The examples of government intervention included shutting down or blocking access to services, requesting access to user data, or attempting to gain greater control over the platforms. Respondents from both companies stress that they push back fiercely against government attempts to narrow the boundaries for allowed expression, or to withdraw user data, whenever these attempts are not lawful and consistent with international human rights standards. By contrast, none of the respondents highlight the fact that corporate practices may themselves have a negative impact on users' rights, for example, the enforcement of terms of service. "Our purpose is to highlight Government action. That's where the focus should be. That's where the pressure is, and that pressure is increasing. Takedown is not really a user concern" (Facebook interview #6, 2015). "It will impact the scope of expression, but we don't consider ourselves to be deciding on freedom of expression. We take decisions on a specific product. We don't take down political speech; it's hate, pornography, and so on" (Facebook interview #6, 2015). "In relation to human rights, we mostly focus on minimizing harm from governments" (Google interview #7, 2015).

This focus on the company–government relationship is also reflected in the main industry initiative in this field—the GNI, which was established in 2008 as a multistakeholder initiative to help the companies enact policies to anticipate and respond to situations in which local law and practice differ from international standards on the rights to privacy and free expression online (Maclay 2014, 11). The corporate member base is limited and includes Google, Oath, Facebook, Microsoft, and LinkedIn, while seven telecommunication companies have joined the affiliated initiative, the Telecommunications Industry Dialogue. On the basis of international law, the GNI has developed a set of standards that the companies should follow to mitigate violations of privacy and freedom of expression caused by governments. The standards focus entirely on company pushback

against illegitimate government requests, while failing to provide similar benchmarks for other types of business practices. It is also unclear how these standards translate into corporate practices. In November 2015, GNI cofounder Rebecca MacKinnon launched the Ranking Digital Rights corporate accountability index in an attempt to increase the transparency of human rights-related business practices.[2] The index measures the human rights commitment of twenty-two major Internet and telecommunication companies at an annual basis, based on the information they disclose on their policy and practices related to freedom of expression and privacy.

In relation to Facebook, the 2017 and 2018 index found evidence that the company's senior leadership exercises oversight of issues related to freedom of expression and privacy, an improvement from the initial 2015 index.[3] Facebook's disclosure regarding its human rights due diligence has also improved, as has as the company's commitment to conduct regular human rights impact assessments. By contrast, there is still a lack of information on remedy and grievance mechanisms for users who allege infringements of their rights. There is also limited information about the volume and nature of content that Facebook restricts or removes in the course of enforcing its terms of service, although this has improved in the 2018 index. Facebook now publishes some data on the volume and nature of content restricted for violating rules against hate speech and inauthentic accounts, yet there should be more transparency on how it identifies and restricts content found to violate its rules. As for privacy, the 2018 index found that while Facebook offers some disclosure about the types of information it collects, it revealed less about what it shares and with whom, for what purpose, and for how long it retains such information. Its disclosure of options users have to control what information the company collects, retains, and uses was especially poor. The company offers some ways to opt out of targeted advertising, suggesting it is on by default. The index found no evidence that Facebook respects the "Do Not Track" standard that allows users to opt out of certain types of web tracking. By contrast, its transparency reporting on government requests for user data is fairly strong.

As for Google, a founding member of the GNI, the 2017 and 2018 index found no evidence of executive oversight of business practices that affect users' freedom of expression and privacy.[4] The index found that although Google is committed to conducting human rights risk assessments when

entering new markets, there is no evidence that it conducts assessments of risks related to terms of service enforcement. It also had notably weak remedy and grievance mechanisms. Google discloses more than any other company in the index about how it handles government and private requests to restrict content and accounts, yet the company´s disclosure of private requests could be significantly improved. For example, in 2015, Google reported removing 92 million videos from YouTube for terms of services violations, but there has been no follow-up disclosure since or evidence of similar disclosures for other Google services evaluated. Google does, however, report on requests related to copyright infringement (globally) and the de-indexing of particular search entries following the "right to be forgotten" ruling (for Europe).[5] As for privacy, Google lacks clarity and specificity in its disclosures related to the handling of personal data, in particular the collection of user data from, and the sharing of it with, third parties. The 2018 index noted that Google has improved its disclosure of options users have to control the collection of some user information, including their location, search history and browsing activity. In line with Facebook, there is no evidence that it respects the "Do Not Track" standard that allows users to opt out of certain types of web tracking.

The Ranking Digital Rights assessment highlights the key point of this section, namely, the disproportionate focus on governments as the cause of human rights problems in the online domain. While it must be acknowledged that governments pose significant threats to human rights around the globe, and that standards are needed to ensure that companies respond to government pressure in ways that comply with human rights law, this is only part of the picture. Arguably, Internet giants such as Facebook and Google have a substantial impact on human rights globally through the corporate policies they adopt and enforce for their users. As stressed in the initial quote from Rosen, the companies tread "an incredibly delicate and difficult line" subjected to a complex mix of pressures to take speech down. These pressures are exercised not only by governments but also by users, advertisers, shareholders, specific interest groups, public opinion, and so forth. Effectively, a small minority of removed content is removed because of government requests, whereas the majority of removed content originates from users flagging specific content in violation of the terms of service.[6] With more than a million posts flagged every day at Facebook

(Bickert 2016a) and 400 hours of video uploaded to YouTube every minute (Downs 2016), the exact drawing of this line greatly impacts the scope of allowed expression. "The real hard part is how we can enforce those policies when we receive more than one million reports per day of violations on Facebook" (Bickert 2016a). "We do try to strike a balance to make sure there's plenty of due process and transparency in how we approach this" (Downs 2016).

Likewise, the collection of personal data represents an unprecedented social graph of users' communications, habits, networks, and preferences, with great ramifications for billions of users' ability to enjoy the right to privacy. In this light, focusing entirely on responses to government requests and leaving out, for example, terms of service enforcement and business practices related to data collection and user profiling provides a partial and limited assessment of the potential negative impact on human rights that these companies' business practices may cause.

From a policy perspective, the corporate approach to translating the companies' human rights responsibility is based on a selective understanding of human rights threats, in which governments are depicted as the main violators and the role of the company is to protect users and thus to safeguard the boundaries of the system from unjustified interference. Government requests potentially pose a threat to the autonomy of the companies, which in response have established subsystems to deal with these disturbances in the form of specific organizational units trained to respond to this particular kind of interference. The subsystems dealing with government requests do so through a number of procedures and checks related to due diligence—for example, is the request submitted via a legitimate public authority, does the request have a valid legal basis, is it proportionate, and so on. After having approved a government request, the interference is documented in a transparency report that serves to maintain users' trust in the system and provide evidence that the companies guard the boundaries of their users' rights to freedom of expression and privacy.

In the interviews I conducted, staff from neither Google nor Facebook reflected critically on their potential negative human rights impact, outside the company–government axis. Nor are these human rights impacts addressed in the context of GNI, which is instrumental in developing benchmarks for corporate compliance with human rights law. While both

companies are heavily engaged in policy discussions around freedom of expression and privacy in a number of policy venues, not least in Washington and Brussels, these debates have mostly focused on how the companies may support the Internet freedom agenda (Carr 2013; Morozov 2011; Powers and Jablonski 2015) and have rarely involved a critical take on the business practices of these major services vis-à-vis human rights. The companies' potential negative impact on freedom of expression by terms of service enforcement, for instance, has only recently started to emerge as a policy topic, although it has been flagged as a human rights concern for several years, for example, in the Ranking Digital Rights Index. The recent Cambridge Analytica/Facebook case, in which Mark Zuckerberg provided testimony in a joint hearing of the Senate Judiciary Committee and the Senate Committee on Commerce, Science, and Transportation and then to the House Energy and Commerce Committee, marks a significant change in this regard, since it explicitly addresses the democratic implications of Facebook's business practices.[7]

Interestingly, the respondents from both companies describe an organizational culture that is fairly blunt and open to debate with top-level management yet mostly anchored within a technical discourse, for example on specific solutions and developments, rather than a critical sociopolitical discourse. In addition, from a research perspective both companies appeared as closed systems, both in terms of gaining access and in terms of the interview situation itself. Such entry and interview barriers are not unique to these two companies but well described in the literature on elite interviews within corporations (Dexter 2006; Harvey 2011), and in this case included difficulty with obtaining contact details of specific staff members, circular responses referring me continuously to a single point of contact, restrictions on the interview situation itself (no recording of conversations), and difficulty in obtaining more elaborated responses. While both companies have an extensive number of policies available on their website, it was difficult to get staff to elaborate on these policies beyond what is already in the public domain. In relation to obtaining information from policy documents vis-à-vis interviews, the interviews provided limited information beyond the official policies but rather illustrated the high degree of coherence in the way these issues are presented in corporate policies, official statements, and interviews. As for descriptions of internal processes—for example, the escalation procedure for content removal—such information

was (not surprisingly) treated as confidential and only provided at a very general level.

Contrary to recent scholarship on platforms that emphasizes the way the economic model, technical design, and platform policies direct social practices in certain directions, the findings indicate that Facebook and Google staff generally depict their services as neutral platforms that facilitate communicative practices among users but have no role in curating this communication. The process of coding is described as detached from political considerations, and algorithms are described as neutral tools for providing the services. "We take all the information that we can find on these crawls and we organize them with algorithms. We try very hard not to have biases" (Schmidt 2013). "The way that Google makes money is by understanding what you want and giving it to you in the moment that you want it. We have the technology, the algorithms that can understand intent" (Green 2015). Specific algorithms (e.g., the PageRank and EdgeRank algorithms) are depicted as important corporate assets, and the respondents generally take great pride in the technical innovations produced by their respective companies. As for policies, these are spoken of as *product guidelines*, not as measures that essentially influence how expression and privacy rights may be exercised. Mark Zuckerberg also emphasized the "neutral platform view" in a response to allegations about the role of Facebook in spreading fake news that influenced the US presidential election. In his response, Zuckerberg stressed that 99 percent of the content users see on Facebook is authentic, that Facebook facilitates access to news of all kinds but does not "identify truth," and that the company has no intention of becoming "arbiters of truth" (Zuckerberg 2016).

In sum, the first narrative refers to Facebook and Google services as neutral products or platforms guided by a commitment to human rights, and free speech in particular. Both companies identify governments as the core threat to their users' rights and freedoms and have established systems and processes to secure their services from governmental interference. From this perspective, the boundaries of their users' right to freedom of expression and privacy is protected by the companies, whereas there is no acknowledgment of the fact that such rights are vulnerable to intrusion by the companies themselves. In short, Facebook and Google treat their users' rights *as part of* the Facebook/Google social system, not as outside systems with independent borders.

Second Narrative: Google and Facebook Assist Law Enforcement by Removing Illegal Content

In May 2016, the European Commission and social media platforms Facebook, Microsoft, YouTube, and Twitter agreed on a Code of Conduct to tackle hate speech online. With the agreement, the companies committed to take the lead on tackling illegal hate speech online. This includes the continued development of internal procedures and staff training to guarantee that they review the majority of valid notifications for removal of illegal hate speech in less than twenty-four hours and remove or disable access to such content if necessary. The companies will also strengthen their partnerships with civil society organizations that will help flag content promoting incitement to violence and hateful conduct. The Code of Conduct on Countering Illegal Hate Speech Online adopted between the European Commission and Facebook, Microsoft, YouTube, and Twitter relates to the second narrative discussed in this chapter—that is, the way that company–government cooperation on law enforcement is framed.

In the fight against unwanted content on the Internet (extremism, terror, hate), governments are increasingly turning to the major online services and enlisting their assistance via more or less formalized cooperation. From a regulatory perspective, this is not surprising, since the private ownership of online communication platforms confronts states with obstacles when they seek to sanction speakers or listeners directly. In consequence, governments enlist private actors as proxy censors to control the online flow of information (Kreimer 2006, 1). Practical measures to control the information flow require either cooperation from these companies, commonly referred to as "gatekeepers" of the online sphere (Laidlaw 2015), or coercion exercised upon them. The policy models that derive from this challenge are addressed extensively in the literature on self- and coregulation as mentioned in the Introduction to this volume. Coregulation refers to a legal model for public authorities based on the voluntary delegation of all or some part of implementation and enforcement of norms to private actors. Self-regulation, by contrast, refers to practices whereby private actors define, implement, and enforce norms without public intervention (Frydman, Hennebel, and Lewkowicz 2008, 133–134). As addressed in the chapters by Land, Callamard, and McGonagle, such policy models carry

human rights implications due to the lack of due-process safeguards and the risk of overreach by companies.

While the first narrative concerns the way the companies are seen to safeguard the freedoms of their users from overreach by governments, this narrative relates to their role in assisting law enforcement by removing illegal content. The recently adopted EU Code of Conduct is an example of such cooperation. The code defines illegal hate speech according to EU Framework Decision 2008/913/JHA of November 28, 2008, as "all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, color, religion, descent or national or ethnic origin" (Code of Conduct on Countering Illegal Hate Speech Online 2016, para. 2). The code is not a legally binding document but establishes a public commitment for the companies, including the requirement to review the majority of valid notifications for removal of illegal hate speech in less than twenty-four hours and to make it easier for law enforcement to notify the companies directly. Currently, there is no uniform definition of what constitutes hate speech around the world, and the Framework Decision has been criticized for lack of compliance with international standards on freedom of expression.[8] When the code was launched in June of 2016, public policy staff at both Google and Facebook stressed that the code is a continuation of work they are already doing in terms of fighting illegal content on their platforms. "We're committed to giving people access to information through our services, but we have always prohibited illegal hate speech on our platforms. . . . We are pleased to work with the Commission to develop co- and self-regulatory approaches to fighting hate speech online" (Junius 2016). "With a global community of 1.6 billion people, we work hard to balance giving people the power to express themselves whilst ensuring we provide a respectful environment. As we make clear in our Community Standards, there's no place for hate speech on Facebook" (Bickert 2016b).

The code is a recent (but not unique) example of the way Internet companies are enlisted to cooperate with law enforcement in the fight against illegal content on their services.[9] It is also an example of the complex mix of legal and nonlegal standards that govern allowed expression and conduct on social media platforms. As stressed in the code, enforcement of criminal law sanctions against perpetrators of hate speech must be complemented by

"actions geared at ensuring that illegal hate speech online is expeditiously acted upon by online intermediaries and social media platforms" (Code of Conduct on Countering Illegal Hate Speech Online 2016, para. 6). In other words, law enforcement by public authorities must go hand in hand with privatized enforcement by companies. As stressed in the code, the increased effort to cut down on hate speech online is guided by the companies' *own activities* (Code of Conduct on Countering Illegal Hate Speech Online 2016, para. 7, my emphasis), and the notification of alleged illegal content is assessed against their community standards and "*where necessary* national laws transposing the Framework Decision" (Code of Conduct on Countering Illegal Hate Speech Online 2016, para. 10, my emphasis). In other words, the companies commit to consider expeditiously whether alleged illegal content (i.e., hate speech) is to be removed based on their internally defined community standards, rather than the law on hate speech in the country in question. Effectively, this form of coregulatory arrangement implies that the EU governments sanction a content-removal process based on privately defined standards and enforced by private actors. Hence, companies, rather than courts, decide on the legality of content. As pointed out by several commentators, this raises concerns both from a freedom-of-expression and a due-process perspective.[10] However, from the perspective of Google and Facebook, the process is not controversial, as it basically codifies a practice that is already in place. On the contrary, the code reinforces the narrative of assisting legitimate government requests while maintaining full autonomy over the process. As repeatedly stressed by policy staff at Facebook and Google, their services cover numerous jurisdictions and so the community standards cannot reflect the national law in each country where they operate. Rather, the standards represent a commonly agreed-upon baseline developed over time. This baseline—the corporate constitution for what is allowed—provides the basis for excluding expressions that are potentially unlawful (such as hate speech), as well as those that are lawful but unwanted (such as certain categories of nudity, graphic content, or misleading information). In short, the decision on when to sanction content, remove it, and ultimately close an account is an internal company decision based on the corporate logic that the community standards represent at YouTube and Facebook, respectively. "There's not one single source that provides us with an answer (on hate speech policy). What we

have to consider is what is best for the people that are in our community" (Bickert 2016a).

The companies' cooperation with law enforcement on tackling hate speech effectively means that the companies have government approval for removing content according to the corporate version of what constitutes hate speech. From a social system point of view, the partnership constitutes an uneven mix of communicative codes (legal/illegal, profit/loss). Government practice is driven by a need to target illegal content in a domain that they do not control, whereas company practice is guided by the need to keep users safe in order to maximize the user base and thus profit. Consequently, decisions that should be dealt with by the legal system (ideally a court) are transferred to a commercial system and decided upon on the basis of legally inspired but commercially defined norms. "To expect the kind of heavyweight process you get in the judiciary, or almost expect the police and judiciary to intervene in every dispute that you have in a domestic space or in one of the public spaces like this, is I think unrealistic" (Allan 2013).

In sum, the company narrative on assisting and cooperating with legitimate law enforcement serves several purposes. First, it affirms the role of the companies as law-abiding and socially responsible corporations that commit to assist law enforcement in the countries where they operate. Second, voluntary agreements on public–private cooperation, such as the one on hate speech, reaffirm the autonomy of the companies in deciding exactly how specific categories of unwanted content should be defined and processed within the company. In other words, such an agreement provides the content removal processes with legitimacy and governmental approval, while serving the companies' interest in keeping full control over the processes that determine how content on their platforms is governed.

Third Narrative: Privacy Equals User Control within the Platform

In March 2016, Joe Cannataci, in his position as newly appointed UN Special Rapporteur on the Right to Privacy, called for increasing attention toward companies' collection and use of personal data. Cannataci argued that the data available for the profiling of individuals is now of an unprecedented

magnitude and that the extent of the privacy risks associated with this data collection is yet to be understood:

> The first 25 years of the existence of the world-wide web have led to a largely unregulated organic growth of private corporations. . . . One of the hallmarks of this growth has been the collection and use of all forms of personal data: every search, every read, every e-mail or other form of messaging, every product or service purchased leaves hundreds of thousands of electronic tracks about an individual which are capable of being aggregated into forming a very accurate profile of that individual's likes, dislikes, moods, financial capabilities, sexual preferences, medical condition, shopping patterns as well as the intellectual, political, religious and philosophical interests and sometimes even the relevant opinions of the netizen. (Cannataci 2016, para. 9)

The third narrative refers to the way privacy is spoken of within the two companies. This narrative unfolds against the backdrop of an increasingly intense debate on platforms and privacy, raised especially within Europe over the past five years, and brought to the forefront of international attention by high-profile cases such as the class action *Europe v. Facebook* initiated by Austrian privacy advocate Max Schrems.[11] The European focus on privacy is also reflected in the new General Data Protection Regulation, which imposes an updated regime of data protection rules on public authorities as well as private actors that process personal data of European citizens.[12] At the international level, the increased focus on privacy is reflected in the appointment of the first UN Special Rapporteur on the Right to Privacy in 2015.

When interviewing staff at Google and Facebook, it was remarkable how much they emphasized the importance of privacy and acknowledged that the many European cases have made it increasingly important to get privacy right. "It was a very conscious decision to take privacy more seriously. Not only legal compliance, it's much broader than that. The whole idea of privacy is core to what Facebook does. But we often have a different approach compared to what the other companies do. We are very bold as to product development—constantly pushing the use of technology, the limits of what you can do" (Facebook interview #8, 2016). "There are people in every corner of the organization that care deeply about privacy" (Google interview #9, 2015). Arguably, awareness around privacy has developed with dedicated subsystems within both organizations. For example, extensive internal systems of control and governance around compliance with European

data protection regulation have been established, including several layers of checks and balances to ensure that no product revision or new product is released without privacy clearance. "So whenever a new product or feature is conceived of, the tech lead for that project has to complete a document that includes a lot of information about how information is going to be collected, processed, shared, used, deleted" (Enright 2015). "Every staff member gets privacy training when joining the company" (Facebook interview #8, 2016). The conversations revealed, however, that the respondents had a very specific understanding of privacy—as user choice *within* the boundaries of the platforms, and as protection against outside interference with these boundaries.

None of the staff I spoke to related privacy to either specific limits or general minimization of data collection by their services.[13] Rather, privacy is described as the ability of the users to foresee and control the sharing of personal information with other users. "Putting people in control is an art. Look at the dashboard in a car" (Facebook interview #8, 2016). "To get privacy right, to provide a solution of choice—is the leadership mantra" (Google interview #8, 2015). As long as users have measures of control, interviewees felt there is not a conflict between the right to privacy and their company's collection and sharing of data. When asked to exemplify how this user control is implemented, the respondents point to Facebook privacy features such as the Facebook Privacy Basics, Privacy Checkup, and Accessing and Downloading Your Information, and within Google, features such as Incognito Mode, Google Takeout, and the Privacy Dashboard, which are repeatedly mentioned as examples of how the idea of user control is implemented into the design of the platforms.

A privacy issue, however, is seen to arise when someone outside the corporate system demands access to user data. In line with the first narrative, governments are depicted as the main cause of privacy problems. "I don't think a democracy functions when your government collects data and doesn't at least fundamentally say what it's doing" (Page 2015). "I hear people say that it's okay to give the government all this data because you're giving it to Facebook anyway, and I'd say that's actually completely different, the power relationship between me and Facebook—however important Facebook is—is just fundamentally different from the power relationship between me and the government" (Allan 2014). In line with

the freedom-of-expression safeguards, both companies have subsystems for handling government requests for user data, and there is a corporate sense of protecting user privacy by pushing back against government requests for user data with due diligence standards. "We want to make sure that existing legal processes for legitimate government access to data work appropriately so that we can push governments to use the front door to use legitimate, transparent, accountable legal processes to access information and we will not, have not and have no intention of collaborating with any effort to give governments information through the back door" (Enright 2015).

While many respondents were willing to talk about privacy, both in terms of tools provided to users and due diligence standards in relation to governments, few were willing to discuss the negative privacy impact that may arise from a business model based on harnessing users' personal data. My interviews revealed the absence of a more critical corporate discourse on the companies' potential negative human rights impact as a result of their business model. Relying on the outlined construction of privacy, the respondents saw no conflict between users' privacy and the massive collection of personal data, as raised by Cannataci in the quote given above. The mapping and profiling that inform their business model are seen as an industry default and as uncontroversial as long as users are provides with means of controlling the flow of their information within the services provided. "To a significant degree the privacy discourse is paternalizing; people share what they want to share" (Google interview #8, 2015). "I don't see a conflict between the business model and privacy provided individual users are in control" (Facebook interview #4, 2015).

Whereas Facebook and Google both take great pride in the way their services push the boundaries for technosocial innovation, thereby breaking new ground for connecting people and information, their approach to human rights is conveniently conservative. Despite the explicit commitment to the industry benchmark in the field—the UN Guiding Principles on Business and Human Rights (UNGPs)—their practices do not take into account the practical implications of this soft-law framework. Whereas the UNGPs explicitly call for a human rights impact assessment of *all* business practices that may impact individuals' enjoyment of human rights, the implementation of these principles within the companies only addresses cases in which there is government interference with business practices.

Conclusion

In this final section, I will relate some crosscutting observations on how human rights responsibility is governed by the two companies, as well as the broader implications of these practices.

First, the analysis pointed to an exclusive focus on governments as the cause of human rights violations. While states have a legal obligation to respect human rights law, the UNGPs explicitly state that private companies have a responsibility to assess and mitigate business practices across their entire operations for any negative human impact they may cause. The framing of human rights within the two companies, however, reduces this human rights responsibility to an obligation to safeguard their users against government overreach. Corporate practices that have given rise to human rights concerns among scholars and activists alike, such as the extensive collection of users' personal data, is not framed as a privacy issue within either company. Privacy is constructed in terms of user control and pushback strategies against illegitimate government requests for user data, rather than as data minimization. Nor is the massive content moderation exercised each day, as the platforms govern compliance with their terms of service, spoken of as a human rights issue. These critical debates simply do not resonate with the human rights framing at Facebook and Google.

Second, the way the EU Code of Conduct enlists the companies to effectively carry out privatized law enforcement on their services normalizes a logic whereby decisions on legal/illegal content and behavior are sanctioned by private actors. From the perspective of Google and Facebook, cooperating with governments is part of a narrative of serving legitimate law-enforcement interests as law-abiding and socially responsible companies, while effectively the cooperation (Code of Conduct) legitimizes their internally defined community standards as *the* documents governing what content is allowed or removed within the boundaries of their services.

Third, despite the numerous policies, algorithms, and governance mechanisms that define the boundaries for possible user actions within the Facebook and Google services, these services are depicted as technically neutral products or platforms via which users may communicate, share, search, connect, and so forth. As such, there is limited (public) discourse by company staff on the way specific policies or platform features determine the

radius of allowed user action and, in effect, shape users' means of exercising privacy or freedom-of-expression rights. On the contrary, it is emphasized that users may at any time choose not to use the products offered or decide to leave the platform, while taking their data with them. Whereas scholars have called for a repertoire of governance strategies that "sees platforms as something other than simply market actors" or "privately owned public utilities" (Ananny and Gillespie 2016, 16), my analysis pointed to a discourse firmly anchored in free market terminology, emphasizing the right of the companies to set and enforce their own terms in a competitive and deregulated market.

Finally, from a public policy perspective, it is significant how these services are framed. Whereas the notion of infrastructure raises (and legitimizes) expectations of regulation, the notion of platform is anchored in a technology/market perspective with essentially different expectations. Arguably, Google and Facebook serve as a social infrastructure for billions of users, and although they are increasingly referred to as such in the public debate, this has not led to regulatory proposals, despite an increasing debate on these issues. In the United States, the Federal Trade Commission has begun to explore questions of platform governance through algorithmic accountability, but thus far there has not been the political will to address the broader implications that platforms may have for the social and political discourse (Ananny and Gillespie 2016, 2) nor for human rights more generally. Despite the fact that these services have an increasing impact on civic life (Moore 2016), their impact on rights of expression, access to information, public participation, and so forth have remained outside the scope of state regulation. By contrast, their impact on privacy and data protection is subjected to relatively detailed regulation in specific regions, such as the EU. While the companies acknowledge that they influence the rights of billions of users worldwide, they refer to their autonomy as private actors and require the freedom to set and enforce their own rules of engagement. The governance gap with regard to the Internet giants is increasingly giving rise to policy concerns, not only in Europe but also in the United States, and it will be interesting to see whether events such as the Cambridge Analytica/Facebook scandal mark a turning point toward regulation of technology giants such as Google and Facebook.

Notes

1. Available at https://www.zuckerbergfiles.org.

2. See https://rankingdigitalrights.org.

3. https://rankingdigitalrights.org/index2017/companies/facebook.

4. https://rankingdigitalrights.org/index2017/companies/google.

5. See, for example, the European Commission's factcheet on the right to be forgotten ruling (*C-131/12*) https://www.inforights.im/media/1186/cl_eu_commission_factsheet_right_to_be-forgotten.pdf.

6. In June 2018, the UN Special Rapporteur on Freedom of Expression issued a thematic report to the Human Rights Council on the regulation of user-generated online content. The rapporteur recommends among others things that companies apply human rights standards at all stages of their operation. The report is available at https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ContentRegulation.aspx.

7. Transcript of Zuckerberg's appearance before the House Energy and Commerce Committee April 11, 2018: https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee.

8. For a critical assessment of the Framework Decision in relation to international standards on freedom of expression, see the brief by Article 19; "EU: European Commission's Code of Conduct for Countering Illegal Hate Speech Online and the Framework Decision", June 2016. https://www.article19.org/resources/eu-european-commissions-code-of-conduct-for-countering-illegal-hate-speech-online-and-the-framework-decision.

9. See, for example, Europol's work with IT companies, covered in EDRi-gram, May 18, 2016: https://edri.org/europol-non-transparent-cooperation-with-it-companies.

10. See, for example, the brief by Article 19; "EU: European Commission's Code of Conduct for Countering Illegal Hate Speech Online and the Framework Decision", June 2016. https://www.article19.org/resources/eu-european-commissions-code-of-conduct-for-countering-illegal-hate-speech-online-and-the-framework-decision.

11. See http://europe-v-facebook.org/EN/en.html.

12. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

13. These are established data protection principles and part of the EU's General Data Protection Regulation.

References

Allan, Richard. 2013. "Richard Allan, Ulf Buermeyer: Speech at Scale." Keynote conversation at Re:publica 13, May 7. https://www.youtube.com/watch?v=1gSTwaYVERo.

Allan, Richard. 2014. The Campion (President's Invited) Lecture: "The Challenges of Operating at Scale," at RSS International Conference, September 2. https://www.youtube.com/watch?v=BWRjif53qt0.

Ananny, Mike, and Tarleton Gillespie. 2016. "Public Platforms: Beyond the Cycle of Shocks and Exceptions." Paper presented at IPP2016 The Platform Society, Oxford University, Oxford, October.

Barnett, Michael N., and Martha Finnemore. 2004. *Rules for the World: International Organizations in Global Politics*. Ithaca, NY: Cornell University Press.

Bickert, Monica. 2016a. Presentation at SXSW Harassment Summit, March 13. https://www.youtube.com/watch?v=WNgvlCuS6cc.

Bickert, Monica. 2016b. Quoted in Alex Harn, "Facebook, YouTube, Twitter and Microsoft Sign EU Hate Speech Code." *The Guardian*, May 31. https://www.theguardian.com/technology/2016/may/31/facebook-youtube-twitter-microsoft-eu-hate-speech-codequoted.

Bowker, Geoffrey C., Karen Baker, Florence Miller, and David Ribes. 2010. "Towards Information Infrastructure Studies: Ways of Knowing in a Networked Environment." In *The International Handbook of Internet Research*, edited by Jeremy Hunsinger, Lisbeth Klastrup, and Matthew Allen, 97–177. Dordrecht: Springer.

Bowker, Geoffrey C., and Susan Leigh Star. 1999. *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: MIT Press.

Cannataci, Joseph A. 2016. "Report of the Special Rapporteur on Privacy, Joseph A. Cannataci." Geneva: Human Rights Council.

Carr, Madeline. 2013. "Internet Freedom, Human Rights and Power." *Australian Journal of International Affairs* 67 (5): 621–637.

Code of Conduct on Countering Illegal Speech Online. 2016. European Commission, May 31. http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

Dexter, Lewis Anthony. 2006. *Elite and Specialized Interviewing*. Colchester, UK: European Consortium for Political Research.

Downs, Juniper. 2016. Presentation at SXSW Harassment Summit, March 13. https://www.youtube.com/watch?v=WNgvlCuS6cc.

Enright, Keith. 2015. "Hot Topics in Privacy: A Conversation with Facebook, Google and Microsoft." Presentation at the RSA Conference, May 5. https://www.youtube.com/watch?v=msc15s52ejc.

Frischmann, Brett M. 2012. *Infrastructure: The Social Value of Shared Resources*. New York: Oxford University Press.

Frydman, Benoit, Ludovic Hennebel, and Gregory Lewkowicz. 2008. "Public Strategies for Internet Co-regulation in the United States, Europe and China." In *Governance, Regulations and Powers on the Internet*, edited by Eric Brousseau, Meryem Marzouki, and Cécile Méadel. Cambridge: Cambridge University Press.

Goffman, Erving. 1974. *Frame Analysis: An Essay on the Organization of Experience*. New York: Harper & Row.

Green, Yasmin. 2015. Panel discussion at the UN Counter-terrorism Centre, June 16. http://webtv.un.org/search/an-exit-for-extermists-digital-solutions-for-online-counter-radicalization-panel-discussion/4302753216001?term=global%20public%20policy%20facebook#full-text.

Harvey, William S. 2011. "Strategies for Conducting Elite Interviews." *Qualitative Research* 11 (4): 431–441.

Helmond, Anne. 2015. "The Platformization of the Web: Making Web Data Platform Ready." *Social Media + Society* 1 (2): 1–11.

Hornung, Gerrit, and Christoph Schnabel. 2009. "Data protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination." *CLSR Computer Law and Security Review: The International Journal of Technology and Practice* 25 (1): 84–88.

Johnston, Hank, and John A. Noakes. 2005. *Frames of Protest: Social Movements and the Framing Perspective*. Lanham, MD: Rowman & Littlefield.

Jørgensen, Rikke Frank. 2017a. "What Platforms Mean When They Talk about Human Rights." *Policy & Internet* 9 (3): 280–296.

———. 2017b. "Framing Human Rights: Exploring Storytelling within Internet Companies." *Information, Communication & Society* 21 (3): 340–355.

Junius, Lie. 2016. Quoted in "Facebook, YouTube, Twitter and Microsoft sign EU hate speech code" by Alex Harn. *The Guardian*, May 31, 2016. https://www.theguardian.com/technology/2016/may/31/facebook-youtube-twitter-microsoft-eu-hate-speech-code.

Kreimer, Seth. F. 2006. "Censorship by Proxy: First Amendment, Internet Intermediaries, and the Problem of the Weakest Link." *University of Pennsylvania Law Review* 155: 11.

Laidlaw, Emily. 2015. *Regulating Speech in Cyberspace*. Cambridge: Cambridge University Press.

Latour, Bruno, and Steve Woolgar. 1986. *Laboratory Life: The Construction of Scientific Facts*. Princeton, NJ: Princeton University Press.

Luhmann, Niklas. 1992. "What Is Communication?" *Communication Theory* 2 (3): 251–259.

———. 1993. *Social Systems*. Copenhagen: Munksgaard.

Maclay, Colin M. 2014. "An Improbable Coalition: How Businesses, Nongovernmental Organizations, Investors and Academics Formed the Global Network Initiative to Promote Privacy and Free Expression Online." PhD diss., The Law and Public Policy Program, Northeastern University, Boston.

Moore, Martin. 2016. *Tech Giants and Civic Power*. London: King's College London.

Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Page, Larry. 2015. "One for All." *Zeit Online*, May. Translated by Marc Young. http://www.zeit.de/wirtschaft/unternehmen/2015-05/larry-page-google-inventor/seite-4.

Pangrazio, Luci. 2016. "Technologically Situated—The Tacit Rules of Platform Participation." Paper presented at IPP2016 The Platform Society, Oxford University, Oxford, October.

Plantin, Jean-Chirstophe, Carl Lagoze, Paul N. Edwards, and Christian Sandvig. 2018. "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook." *New Media & Society* 20 (1): 293–310.

Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana: University of Illinois Press.

Rosen, Jeffrey. 2016. Presentation at the SXSW Harassment Summit Second Panel, March 12, 2016. https://www.youtube.com/watch?v=WNgvlCuS6cc.

Rosen, Jeffrey. 2012. "The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google." *Fordham Law Review* 80 (4): 1525–1538.

Schmidt, Eric. 2013. "Eric Schmidt on the New Digital Age." Royal Geographical Society, May 25. https://www.youtube.com/watch?v=etmarYifipE.

Star, Susan Leigh, and Karen Ruhleder. 1996. "Steps toward an Ecology of Infrastructure: Design and Access for Large Information Spaces." *Information Systems Research* 7 (1): 111–134.

Tannen, Deborah. 1993. *Framing in Discourse*. New York: Oxford University Press.

Van Dijck, José. 2013. *The Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press.

Van Dijck, José, and Thomas Poell. 2013. "Understanding Social Media Logic." *Media and Communication* 1 (1): 2–14.

Zuckerberg, Mark. 2016. Facebook post from November 13, 2016: https://www.facebook.com/zuck/posts/10103253901916271.