The Labor of Digital Privacy Advocacy in the Era of Big Tech[1]

Jennifer Holt[2]
UNIVERSITY OF CALIFORNIA, SANTA BARBARA
holt813 [AT] ucsb.edu

Lisa Parks[3]
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
lparks [AT] mit.edu

Abstract

This article explores the labor of contemporary digital privacy advocates and their myriad efforts to protect and preserve public interests during the era of Big Tech companies. It is based on qualitative interviews with professional staff, lawyers, and policy analysts at multiple major advocacy organizations in Washington, DC. We have employed a grounded theory approach to address four labor-related themes that consistently emerged across our interviews: coalition building, agenda formulation, the art of navigating public- and private-sector relationships, and balancing a domestic and global policy landscape. In the current policy landscape, there is an intensifying degree of advocacy–industry coordination taking place, in part because of US regulatory roll-backs under the Trump administration and a gridlocked Congress. As a result, advocacy organization staff members often rely on companies for information to do their assessment and agenda-setting work. They also apply pressure to these companies and force them to think about how their technologies and operations impact users and publics around the world; they mount legal challenges to various media and tech initiatives to ensure public interests are protected; and some end up working with *or* for *these companies in ways that may impart and integrate the values of advocacy organizations within profit-driven organizations. This article explores the multiple dimensions of advocacy labor which itself is often excluded from media policy and industry analysis.*

Keywords: *Privacy, Labor, Digital Rights, Big Tech, Advocacy*

As Big Tech companies like Google, Facebook, and Amazon have expanded their digital empires over the past decade, internet users have faced unprecedented privacy breaches.[4] Google archives and sells users' browser data to advertising companies. Facebook claims users' posts, photos, and videos as its own intellectual property. And Amazon tracks all consumer purchases and mines that data to target advertising and sell more products. By exploiting every opportunity to collect and monetize personal information and digital traces, these companies have normalized what Shoshana Zuboff has termed "surveillance capitalism," defined as "a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales." As Zuboff explains,

> surveillance capitalism operates through unprecedented asymmetries in knowledge and the power that accrues to knowledge. Surveillance capitalists know everything about us whereas their operations are designed to be unknowable to us. They accumulate vast domains of new knowledge *from* us, but not *for* us.[5]

These practices have led to a new world order for media industries and have altered everything from business models and content development to advertising metrics and marketing strategies. Surveillance capitalism has supported the transformation of digital media audiences into monetized data subjects, yielding a trove of investigative reporting,[6] academic scholarship,[7] and documentary films,[8] which have exposed and critiqued these problematic developments.

European governments responded to digital privacy concerns by implementing the General Data Protection Regulation (GDPR) in 2018. This European Union regulation recognizes the growing power of US-based Big Tech firms and has tried to limit that power by establishing data subject rights, strengthening legibility regarding conditions of consent, and imposing fines for companies in violation.[9] Thus far, the US government has refused to enact similar regulations to protect American citizens and their digital rights, even though Russian interference in the 2016 Presidential election and the Cambridge Analytica scandal (in which the data of over 87 million Facebook users was sold to political campaigns without their consent) has made US officials starkly aware of what is at stake in ignoring digital privacy issues.[10] Despite growing public concerns about these matters, US regulators have continued to look the other way, clinging to corporate-driven neoliberal policies,[11] succumbing to lobbying pressure from Big Tech, and allowing these companies to "self-regulate," with occasional and inconsequential fines.[12] At the time of this writing, dozens of State Attorneys General are going after Facebook and Google on antitrust violations, and the US House of Representatives Judiciary Committee has multiple ongoing investigations into the practices of Google, Amazon, Facebook, and Apple.

That US federal regulators have largely adopted a fine-oriented, "hands-off" approach to data security and protection does not mean that citizens do not care about their digital rights or that advocacy organizations have been asleep at the wheel. On the contrary, the rise of Big Tech has brought forth an armada of digital rights advocacy groups fighting on behalf of publics in this space. Some of them—such as the Electronic Privacy Information Center (EPIC), American Civil Liberties Union (ACLU), and Electronic Frontier Foundation (EFF)—have existed before the web 2.0 era and have since reoriented their efforts around

new technologies as consumer rights continue to be under attack. Others, such as Public Knowledge, the Center for Democracy & Technology (CDT), Access Now, and Ranking Digital Rights (RDR), formed more recently to protect public interests from wrongdoing by governments and Big Tech in the United States and beyond. Together, these groups confront huge challenges in keeping people informed about emerging technologies and potential and actual digital rights violations.[13]

Related to this advocacy work is a growing body of interdisciplinary scholarship on privacy and computing that has drawn public attention to concerns around the collection of personal information, workplace surveillance, and new forms of social control.[14] Recent research on privacy has also engaged with historical perspectives,[15] sociopolitical contexts,[16] legal battles over design,[17] resistance and protest,[18] and the all-encompassing societal tilt toward surveillance and informational capitalism.[19] Only a few scholars have examined the work of privacy advocates tasked with addressing such concerns. Information policy scholars, such as Milton Mueller, Brenden Kuerbis, and Christiane Page, explored the role of advocacy in US information policy from 1960 to 2002. Pointing to some of the limitations of advocacy work, they called for a broader and more integrative analytical framework that "deeply comprehends the relationships between free expression, privacy, infrastructure regulation, intellectual property, digital identity and government information policy. . . ."[20] In *The Privacy Advocates: Resisting the Spread of Surveillance* (2008), political scientist Colin Bennett further investigates the organizations, resources, and strategies of privacy workers and argues that privacy advocates' work combines the roles of researcher, consultant, technology developer, journalist, and artist and requires navigating between government and corporate forces.[21] More recently, Bamberger and Mulligan's *Privacy on the Ground* (2015) engaged with privacy professionals working in corporations across five countries and contends that "The work of corporate privacy and human rights professionals is rarely visible to the outside world. Their hard-fought battles over product design or data collection, storage, use, and disclosure do not often see the light of day." These authors found that "corporate orientation toward privacy" can make a difference in advancing advocacy agendas.[22]

While media industry scholars have explored issues of deregulation in the digital era,[23] and the politics of net neutrality,[24] surveillance,[25] labor,[26] and platforms,[27] precious few in the field have addressed advocacy work as an area of central importance to these industry dynamics. Becky Lentz and Allison Perlman's co-edited special issue of the *International Journal of Communication* provides "an interdisciplinary look at the many labors of media advocacy to foreground the 'how' and the 'why' of how media advocacy operates."[28] By situating policy advocacy work within the broader purview of media labor, Lentz and Perlman hoped

> not only to flag how media policy advocacy groups are players within this broader ecology—poised to affect the discursive and material environments in which media are produced, circulated, and regulated—but also to elucidate the many labors—tactical, political, interpersonal, informational, communicative—required to engage in media advocacy work.[29]

Engaging with digital privacy advocacy offers a perspective on the inner-workings of contemporary media industries that recognizes the impact of this vital labor centered in

Washington, DC. Such labor does not usually conform to traditional categories of labor in media industries research. Allison Perlman has noted, for instance, that most scholars in this field "share an understanding of media advocacy as a *social movement* or as a form of *civic participation* that has sought to transform the media to meet the communication needs of citizens in a democracy."[30] However, she argues that

> many contemporary media advocacy groups in the United States are engaged in *media work*, labor that contributes to, rather than interferes with, media production and the interests of media companies. Media advocacy, however, has been invisible to scholars of media labor.[31]

We share Perlman's view and have written this article not only to make the labor of digital privacy advocacy more visible, but also to analyze its important functions and relevance for media industry studies in the era of Big Tech.

Our article follows up on the critical work of these and other scholars who have identified advocacy work as an important dimension of the media production, distribution, and policy landscape.[32] We extend their research by exploring the labor of contemporary digital privacy advocates and their ongoing struggle to protect and preserve the "public interest" in the digital space. While advocates have necessarily engaged with the television industry, which Perlman explores in her crucial research, the sites of their labor, companies, and practices they focus on, along with their "advocacy toolkits" have had to expand exponentially in the digital era. Moreover, the public interest standard used by US regulators and advocates in the past (based on the 1927 Radio Act and 1934 Communication Act) does not apply to digital media platforms or the companies that own and operate them. An entirely new landscape of technologies and corporations has become part of what we now think of as the media industries. This sea change compels new research on the ways advocacy labor functions in the current environment.

To explore the labor of digital privacy advocacy further, we conducted qualitative, long-form, in-person interviews with ten professional staff members at six major advocacy organizations in Washington, DC in December 2018, as well as with five other experts/researchers in person and over the phone.[33] We engaged with staff from organizations that have been actively involved in US digital advocacy work for decades as well as more emergent and international ones. Most of our interviewees were lawyers and policy analysts. Since some of our interviewees work in very politicized situations, they preferred to remain anonymized. In addition to our interviews, we read advocacy organization websites and white papers, relevant trade press and scholarly literature in media industry studies, privacy and computing, and surveillance studies to help contextualize our interview findings. During our interviews, we asked questions such as: given expanding state and corporate surveillance, how do you decide where to focus their attention and formulate your agendas? With Big Tech's blackboxing of technical information as trade secrets, what sources and practices do you rely on to build understandings of emerging technologies and their impacts? Finally, what kind of relationships do you have with Big Tech, elected officials, and the media industries at large?

To analyze our data, we used a grounded theory approach: we reviewed interview transcripts, identified four labor-related themes that consistently emerged across the transcripts, and developed analytical discussions around these themes: coalition building; agenda

formulation; the art of navigating public- and private-sector relationships; and juggling a domestic and global policy landscape. As federal US officials cling to and normalize deregulation in the media and information sectors, there is an urgent need for media scholars and citizens to further understand and support the work of advocates. They are redefining and fighting for public interests against all odds, and yet in many ways remain dependent on Big Tech to do their work. Incorporating advocacy labor into our rubrics for defining power relationships in the digital policy space affords media industry scholars a more informed vantage point from which to discern how digital rights are treated by the state, by private corporations, and by the organizations designed to protect them. This nuance also demands a less reductive formula for understanding how digital privacy operates as a growing yet still elusive dimension of the "public interest." The strategies employed by advocacy groups are as varied as our understandings of this term.

Furthermore, as media industries are increasingly interwoven with other sectors—whether energy, computing, data storage, or intelligence gathering—there is a need for research and methodologies that can engage with these crossover relationships. Foregrounding these complexities is necessary to keep the study of "media industries" dynamic and agile. This has inspired our exploration of the myriad efforts undertaken by digital privacy advocates to reshape corporate practices, influence federal regulations, and track technologies that have been used to threaten the rights of citizens all over the world. Particularly in the age of surveillance capitalism and neoliberalism, media industries are in a state of heightened integration with the digital economy that often leaves public interests as collateral damage of media mergers and developing business models. Our research thus prompts us to make the case for media industry research focused not just on Hollywood or Silicon Valley or other media capitals, but on the forces of computing, surveillance, and advocacy labor as they intersect with and shape the contours of public interests in the digital realm.

Coalition Building: Lessons in Seizing Opportunities

Digital privacy is often understood within the broader rubric of digital rights advocacy. Digital rights encompass everything from freedom of speech online and access to an open internet, to limiting government surveillance, ending human rights abuses taking place in the largely unregulated global digital ecosystem, and of course, protecting the fundamental right to privacy. Coalition building is an essential aspect of work in this space, as advocacy organizations are regularly fighting a tech industry that is better funded, more powerful, and perfectly aligned with the neoliberal ideology guiding US governance principles. Primarily non-partisan, digital rights advocates work with a host of different players in a delicate balancing act, including political officials, private companies, and consumers. The largest and most visible organizations in this "loose coalition," as several of our interviewees called it—the ACLU, Consumers Union, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), Public Knowledge, and the Center for Democracy & Technology (CDT)—are also joined by others of varying sizes and areas of emphasis, including Free Press, the National Hispanic Media Coalition (NHMC), Media Alliance, Access Now, Common Cause,

the Center for Privacy and Technology at Georgetown Law, New America's Open Technology Institute (OTI), and the Consumer Federation of America.

These organizations have been able to build a "loose coalition" related to digital privacy because their stated missions align around several key issues—the importance of an open internet, equitable access to digital technology, rights of free speech and privacy, and human rights in digital contexts. The OTI, for instance, promotes "universal access to communications technologies that are both open and secure. . . ." Public Knowledge works to advance "freedom of expression, an open internet, and access to affordable communications tools and creative works." And the EFF champions "user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development." Other organizations describe their missions in similar ways, but each has its own unique approach to framing and fighting for public interests in the arena of privacy and the attendant landscapes of surveillance, human rights, internet governance and access, free expression, and corporate accountability, as indicated in Figure 1.

The collaboration of coalition members, as several of our interviewees explained, allows for more tactical and efficient advocacy as opposed to dozens of specialized silos working at cross-purposes. Together, these groups share information, coordinate communication and lobbying strategies, and even develop joint recommendations, such as the 2018 Public Interest Privacy Legislation Principles. These Principles were released by thirty-four organizations and urged Congress to pass privacy legislation that "ensures fairness, prevents discrimination, advances equal opportunity, protects free expression, and facilitates trust between the public and companies that collect their personal data."[34] This document was based on polling coalition members on fifty-three different privacy positions and culling the results to focus on broad areas of consensus among the group's members. This intervention seems to have had some influence as Democratic members of Congress introduced a digital privacy bill in November 2019.

Still, due to the wide range of constituencies, issues, and diverse ideological positions within the coalition, consensus is not always possible. Often, coalition partners have different opinions on an issue or different emphases. Some organizations focus on US Constitutional protections (ACLU), whereas others deploy international human rights law (Access Now). Some value the libertarian ethos of the internet (EFF), whereas others view policy and legislation as the best way forward (Public Knowledge). Many try to influence corporate practices (OTI, CDT) and/or develop technology-based solutions and apps (Glianet; OTI; Access Now). These differences have created an interesting dynamic wherein most organizations see themselves both as independent, working toward their own stated mission, and as part of a larger community, pushing a broader agenda. They never undermine one another, but they are forced to juggle competing interests when working together. As one advocate put it,

> we will take advantage of any means of furthering an advocacy objective . . . continuing to have conversations with relevant privacy officers and the administration to further dialogue on something until we see an opportunity to get something passed . . .

Our interviewees also noted that they actually do a surprising amount of work with companies engaging in data collection activities themselves, and sometimes advocacy interests are even aligned with those companies. For example, tech companies do not want to see

Organization	Mission Statement Excerpt
Access Now	Defending and extending the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.
American Civil Liberties Union	Preserving and protecting the liberties and privileges guaranteed to each individual by the Bill of Rights. These liberties include freedom of speech and expression, equal protection under the law, due process of law, and the right to personal privacy.
Center for Democracy and Technology	Working to strengthen individual rights and freedoms by defining, promoting, and influencing technology policy and the architecture of the internet that impacts our daily lives . . . including: preserve the unique nature of the internet; enhance freedom of expression globally; protect our fundamental right to privacy; limit government surveillance; and define the boundaries of technology in our daily lives.
Consumer Reports (formerly Consumers Union)	Working side by side with consumers for truth, transparency, and fairness in the marketplace . . . we work with other organizations, including media, consumer groups, research and testing consortiums, and philanthropic partners to inform purchase decisions, improve the products and services that businesses deliver, and drive regulatory and fair competitive practices.
Electronic Frontier Foundation	Championing user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.
Electronic Privacy and Information Center	Focusing public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC works to promote the Public Voice in decisions concerning the future of the Internet.
Free Press	Closely watching as the decisions shaping the media landscape are made and sounding the alarm when people's rights to connect and communicate are in danger. We focus on saving Net Neutrality, achieving affordable internet access for all, uplifting the voices of people of color in the media, challenging old and new media gatekeepers to serve the public interest, ending unwarranted surveillance, defending press freedom and reimagining local journalism.
Open Technology Institute	Working at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits . . . and promoting universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.
Public Knowledge	Promoting freedom of expression, an open internet, and access to affordable communications tools and creative works. We work to shape policy on behalf of the public interest.
Ranking Digital Rights	Working to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights . . . We work with companies as well as advocates, researchers, investors, and policymakers to establish and advance global standards for corporate accountability.

Figure 1. Mission Statement Excerpts of Digital Rights Advocacy Organizations, 2019–2020*

*These excerpts were pulled from the organizations' websites.

backdoor encryption bills passed; they want to be able to tell their consumers that their data is protected. According to one advocate, "That's just the straight up business interest," and the advocacy community takes advantage of such strategic affinities to move their agendas forward, particularly in challenging political times.

Further complicating the work of coalition building, the privacy and surveillance landscape is extremely complex and nuanced. As Harold Feld, Senior Vice President of Public Knowledge, remarked, "the problems and shape of [this landscape] change over time, particularly with regard to evolving technologies and the way that people think about it." While many in the general public might be concerned about one issue (Facebook and data harvesting, for example), the privacy advocacy community is concerned with the aggregate of threats, relevant policies, and critical vulnerabilities in the global digital ecosystem. This has created a rather daunting agenda for a relatively small but undeniably mighty coalition.

This expansive agenda has led the coalition to be involved with lobbying related to everything from the enhanced surveillance powers in the US PATRIOT Act and the National Security Agency's (NSA) PRISM program's spying on US citizens (with the aid of Big Tech companies as Edward Snowden revealed) to the Broadband Consumer Privacy Rules designed to protect consumer data created by the Federal Communications Commission (FCC) in 2016.[35] While these rules were quickly decimated by Congress in 2017, just three months into the Trump administration, it was an important moment for privacy advocates. According to Feld, this was when it became clear to those who had been working on digital privacy issues in coordination with the Obama FCC that

> FCC privacy was now a dead end and, therefore, to the extent that we were still going to pursue privacy, it wouldn't just be within the context of the FCC; it had to be in a more broader coalition effort that looked to legislation.

This perspective was shared by everyone we interviewed, and recognized by many advocates as of late 2016. After Republicans won majorities in the House and Senate, there was a sense among advocates that nothing was going to pass in Congress, so accomplishing anything related to digital privacy would have to involve working with private companies as well. As one interviewee put it, "If we can't get it passed via law, maybe we can get it passed via practice and encourage companies to do X, Y, or Z and achieve the functional equivalent of what we want to see in statute." The current approach has been to turn to companies and states, and attempt to make progress that way, as opposed to the federal legislative route.

Privacy advocates not only interface and work with one another, but also must navigate dynamically changing political, economic, and technological conditions. Media industry scholars often default to the role of neoliberalism as an explanation for advocates' shift away from pressuring the FCC and Congress and toward corporate engagement, yet our interviews revealed that such an explanation is too facile. Advocates engage in a complex calculus, constantly researching the political climate, industrial practices, and digital rights concerns and assessing what is possible. Sometimes advocates' agendas align incidentally with the companies they scrutinize, and a certain amount of progress can be made. Sometimes congressional leaders introduce bills that integrate principles they have elaborated in policy recommendations. And sometimes they bang their heads against the wall in conditions of

regulatory inertia. Suffice it to say, their coalition building does not always lead to major reforms, but it has kept digital rights on the regulatory radar.

Agenda Formulation: Juggling the Proactive and Reactive

It is one thing to engage in the work of forming and sustaining coalitions. It is quite another to formulate shared digital privacy agendas. The extremely broad purview of the coalition makes it challenging to develop a proactive agenda and create buy-in among coalition members for maximum effectiveness and efficiency. Each group brings different skill sets, areas of focus, and expertise. Some like the ACLU, EFF, Public Knowledge, and CDT specialize in legislative drafting and policy recommendations via amicus briefs and lobbying Congress and regulatory agencies. Members of these groups also write and distribute white papers, blogs, and other materials such as advocacy and activist training documents, consumer education tools, technologies for enhanced privacy such as browser extensions, and online courses designed to engage and inform the public about digital rights. These public-facing tactics run the gamut from educating the public about sustainable cybersecurity measures, providing tips for avoiding surveillance on digital devices, and creating technology for defeating ad trackers. Access Now even runs a twenty-four-hour multilingual, free helpline resource to support "civil society around the world" (detailed further below).

Given the proliferating threats to individual privacy, digital privacy advocates have sought to seize all opportunities—whether legislative reform, research, influence on corporate operations or terms of service agreements, or tech development—to ensure Constitutional rights are upheld in the digital realm. While advocates do not always agree on issues or use the same tactics, they approach the "public interest" in this context in relation to citizens' rights to free speech and privacy under the First and Fourth Amendments. A "digital violation," then, involves federal or corporate practices that infringe upon these rights in digital spaces. In addition, some advocates emphasize the ways that social inequalities (e.g., those faced by racial communities of color; immigrants; inmates) often inform and shape these violations as well.

To keep track of the privacy-encroaching potentials of digital technologies, some digital rights advocacy organizations, such as EFF, CDT and Access Now, have staff members considered as "technologists" who specialize in understanding how digital technologies, software, apps, and devices work. These advocates download and test new apps on burner phones so that they can understand terms of service agreements and functionality of apps, and identify potential privacy vulnerabilities. In the Big Tech era, advocates have to understand and communicate about the operations of technologies in ways that advocates working in the analog era never did. Not only do they closely read terms of service conditions and test apps, they also have to contend with the Big Tech requirement to sign non-disclosure agreements (NDAs) in the course of their work. Yet signing them, according to our interviewees, does not preclude advocates from writing about or publicizing general digital privacy concerns linked to the technology.[36] As Joseph Jerome, staff at CDT, explained, in these situations, "It's always

slanted to what they want to show us, but we do get access to things sometimes, which I think is useful to help us know a little bit more about what we're talking about." Natasha Duarte, also staff at CDT, characterized these situations as companies providing a "look under the hood" and indicated that advocates learn the most from private companies when approaching them with a technical description and asking, "Is this an accurate description of how this technology works?" Given the secrecy around privacy and surveillance-related activities, it can be challenging to figure out how algorithms are set up, even with an NDA. Because of this, digital privacy advocates also read a lot of technical reports, product descriptions on company websites, and academic research to try and understand technological trends, proprietary algorithms, and device designs and capabilities. Our interviewees indicated that even acquiring baseline understandings of emerging technologies can be helpful in proactively confronting the proliferation of digital privacy invasions.

In addition to leveraging technologists' research for agenda-setting, digital privacy advocates also must react to major breaking news and security events. This is a critical element of these organizations' mandates. If they did not respond to developments such as the Equifax data breach or the Cambridge Analytica scandal, for example, privacy advocates would risk appearing irrelevant or out of touch. When such events occur, congressional leaders and news media often look to digital privacy advocates for context or explanation. Breaches and violations often end up drawing attention to the value of digital privacy advocacy while revealing new concerns on the horizon that need to be addressed. Thus, advocates must strike a balance between reactive and proactive postures in their agenda formulation. One interviewee noted that it is a constant struggle to maintain a proactive agenda while also having to react to so many privacy-related developments in a rapidly changing technological landscape. It is also very challenging to even define the line between the proactive and reactive as events and strategies unfold and overlap. For example, working proactively on the policy implications of automated content moderation related to hate speech and disinformation led one organization to utilize that research in relation to an entirely separate project on the Trump administration's proposal to conduct surveillance of immigrant populations using automated analysis of their social media accounts. Agenda formulation occurs through relational understanding of different situations and juggling of proactive and reactive efforts, complicating many common understandings of advocacy labor—and policy change—as a fundamentally linear path.

Another aspect of the coalition's agenda-setting, which is sometimes directly acknowledged but more often unstated, is adjusting what is known as the "Overton window"—the range of policy ideas that are acceptable to the political mainstream at a given moment. One of our interviewees addressed this issue in relation to the issue of encryption. Instead of continuing to debate with the Department of Justice whether or not there is an actual "secure backdoor," they convened a conference on encryption policy that explored how such tools affect people, who is protected by encryption, who is most at risk, and what kind of personal information is at stake. The conference, in other words, attempted to shift the range of policy ideas about encryption by discussing the technology's social dimensions—its effects on particular people rather than fixating on the technicalities of the "backdoor." Bringing together members of vulnerable communities, industry experts, and high-ranking government officials to discuss how encryption affects public and personal safety, individual rights, and economic security,

in addition to national and cyber-security, enabled advocates to expand and redirect the encryption policy discussion and weave it into their agenda formulation work.

Also crucial to this work is legibility. Several of our interviewees emphasized the importance of being able to describe agenda items and public advocacy work in accessible ways "so that people can understand and take ownership of them." Advocates truly want people to have the ability to be engaged in conversations and decision-making processes about the impacts of digital surveillance technologies and privacy protections. Harold Feld underscored this issue, which was repeated throughout our interviews: "there is an educational issue that has to happen . . . you need to draw connections for the public and you need to draw connections for the decision makers." The educational work of creating these connections for and between various parties was viewed as critical to building salient advocacy agendas and achieving long-term success, and all of our interviewees implored us to get academics and students further engaged in this process.

Navigating Regime Changes: Big Picture and Long Game

Whether agendas are proactive or reactive, privacy advocates must ride the treacherous waves of election cycles and political transitions while maintaining focus on their overall goals. There are persistent frustrations in navigating regime changes as well as experiences of working for many years on an issue only to see it refiled, sidelined, struck down, or deprioritized (e.g., the 2017 Congressional nullification of the FCC's Broadband Privacy Rules created in 2016). One advocate bemoaned what they called the "government in exile" function—that is, when political regime change prevents progress on an issue from being made. Such conditions can bring about strategic retrenchment, triaging, and damage control, but they also can create time to work on long-term agenda items and writing projects. In this sense, even the most challenging times can be generative for the long game of digital privacy advocacy, which is of primary importance to coalition members.

Beyond dealing with new political administrations, there continue to be major challenges getting legislation passed due to bipartisan congressional gridlock. This situation stalls advocacy work that is oriented around legislation and policy-making, and requires continuing to "play in the orchestra on the Titanic," as one advocate, Allie Bohm, policy counsel for Public Knowledge, put it. In such conditions, Bohm explains, advocates push for "a strong losing vote, because we're setting ourselves up for the future." Harold Feld called the Trump administration the "100-year flood of policy," meaning that "it was totally unexpected." Feld continued, "We never prepared for something this awful. Even those of us who had experience with previous Republican administrations were astounded at the absolute indifference the Trump Administration had for the broader consequences of their actions." Trump's FCC Chairman, Ajit Pai, has aligned himself with internet service providers (ISPs) and Big Tech from day 1, leaving the public behind in actions ranging from destroying net neutrality to abandoning almost all government-enforced privacy protections for US broadband users. Other interviewees echoed Feld's concern, emphasizing the serious challenges for all forms of civil and human rights at this time. Another explained, "We just have to deal with a Congress

that is very partisan right now and will refuse to move on certain issues. That's making a lot of our work difficult to do [when] we want to see legislation passed." Regulatory agencies change as well with each new administration, as do their ideologies and approaches to safeguarding the "public interest." As one advocate put it, "The old FCC worked with us on common goals and the new FCC works against us and is hostile."

Yet for digital privacy advocates, continuing to fight for better policies remains critical because, as Allie Bohm explained, "no victory is permanent, and no loss is permanent. We have to defend the victories we have or we will lose them, and we have to continue to build the record to eventually win on the issues we've lost on in the past." Nevertheless, it is still important to document for the historical record how terrible decisions get made; this helps to prepare for the future as, inevitably, many of the same fights will continue. Moreover, it allows scholars and citizens to better understand the longue durée of policymaking, which only these historical struggles can illuminate. Typically, the advocacy community faces a "sliding scale of victory" as they note it is rare to ever get a total win, even in the best of times. So a defeat can be an orderly retreat, or a complete rout, but the goal will always be to secure future opportunities and accomplish what is possible, as opposed to simply giving up and going home—even in the worst of times. Sometimes that translates into education—for the public and for legislators or policymakers. At other times, it results in increased fundraising, advancing conversations with adversaries, or expanding the network of relationships to be able to fight more effectively in the next round. An advocate with OTI explained this consistent sentiment across the coalition: "even when you know you're fighting a losing battle and it's preordained that you will lose . . . everybody still feels tremendous responsibility to continue to fight because it's about the very long game."

Beyond navigating election cycles and committing to the long game of advocacy work, digital privacy advocates have been laser-focused on the protection and security of personal information, which involves working with citizen-consumers, government officials, and companies. Advocates have continued to question what types of data the government can collect and access about individuals and how that access is afforded. This labor includes monitoring everything from the national security surveillance programs conducted under the Foreign Intelligence Surveillance Act (FISA) and/or reliant on Executive Order 12333 (an order that significantly expanded the surveillance authorities and mandate of the NSA originally signed in 1981), to criminal wiretapping, digital security issues, and the growing state use of biometrics and facial-recognition technologies. As one interviewee put it, there are "perpetual efforts by the FBI to expand national security letter authorities."[37] Beyond this, privacy advocates must ensure they are well positioned to participate in debates about new technologies and related government encroachments and abuses. Through such work, advocates apply and maintain pressure on government agencies, demanding that they provide information about their surveillance practices so that advocates can effectively recognize and prioritize needed reforms.

Another aspect of digital privacy advocacy is more commercially directed: What kinds of personal data do Big Tech companies, advertisers, health insurers, or hardware manufacturers have access to? And how is this access expanding in ways that diminish privacy or enhance

surveillance? Some advocates who have worked in various capacities for both private companies and public organizations believe the biggest challenge is to create technical solutions to digital privacy that are somewhat "future proof or at least have a future open approach." For instance, one interviewee has envisioned personalized gateways to the internet using "TrustMediaries," which serve as digital interfaces between the user and web that are designed to create a "more decentralized ecosystem of digital trust"—see, for example, GliaNet. This project was inspired by experiences with the rapid-fire pace at which corporate legal teams must respond to various privacy matters and the desire to develop more structural and long-term solutions for digital privacy protection.

Such projects are contingent upon securing the necessary funding to continue advocacy work. Most of these organizations receive funding from a combination of public and private sources. Some avoid taking funding from the US government in order to prevent interference with their organization's mission, but do accept funding from European governments for networking initiatives related to global issues and coalition partners, for example. Some also have branches in Latin America, South Asia, and Europe, and typically receive funding from national governments in those regions. Interestingly, advocacy groups often receive significant support from the companies they are critiquing or opposing in their various campaigns. The CDT, for example, counts 43 percent of its revenue from corporations and lists Amazon, Apple, Google, Facebook, Microsoft, Twitter, and Verizon among their top supporters.[38] Public Knowledge "limits contributions from any single corporation to 5–10% of its budget to ensure that no funders can attempt to assert undue influence" on the organization. Their highest level donors include many companies that Public Knowledge clashes with in their various initiatives, including AT&T, Sprint, T-Mobile, Google, Microsoft, Charter Communications, DISH Network, and Netflix.[39] While donations from these companies certainly create the possibility for "advocacy capture," defined by Perlman as "the process by which public interest groups adopt the priorities of their funders over those of their communities,"[40] such pressures were not evident in our interviews or our research on the work of these particular digital privacy organizations. All of the financials for these companies are readily available online in their annual reports. These records detail the individuals, foundations, grants, corporate donors, fundraising events, and other in-kind contributions that support their independent missions.

Ultimately, the line between advocacy communities and the Big Tech companies they lobby is murky. There is regular coordination and cooperation between digital advocates and the private sector, from consulting on hot button issues to advocacy groups accepting donations from tech companies. Interviewees explained that they embraced opportunities to work *with* tech companies and urge company representatives "to be aggressive in defending their users' rights." Often this corporate outreach yields favorable outcomes or increased access to information for advocates. In the wake of the 2013 Snowden revelations, for instance, advocacy groups pressured companies to provide information about their data collection and surveillance activities. This resulted in the routine release of corporate transparency reports, which provide unique insights into the workings and privacy protection commitments of Big Tech companies and help to hold them accountable. Troublingly, however, these reports are increasingly being phased out, and a key privacy safeguard for consumers is being lost with their removal. Interviewees further indicated that a combination of

patterns has taken shape: newer tech firms are not adopting the practice; existing companies are dropping the reports; and the reports have become the casualties of mergers and new management that "lacks the old management's commitment to transparency . . . [so] the momentum has faded."[41] However, some do still exist,[42] thanks in large part to the continued pressure coming from privacy advocates.

Given the abysmal records of the FCC, Federal Trade Commission (FTC), and Congress on the digital privacy front, advocates must play a multidimensional long game. As one interviewee insisted, it is critical to remain at the table in discussions, even if both parties completely disagree. There is always hope that

> if you could figure out a way to show them alternative business models or use the market to put pressure on them . . . [they could] be more willing to look at things other than what they're sort of tied into now. . . . and they might change things.

Some viewed employees within tech companies as "another potential pressure point" because, as our interviewee explained, "they tend to have a perspective of technology as a positive force, and they're seeing their leaders taking their companies off course and they're not happy about it." This optimistic perspective was shared by several of our interviewees, who perceive tech company employees as potentially agitating for change from the inside, which is consistent with the findings of Bamberger and Mulligan.[43]

To that point, three of the most prominent and experienced lawyers in the digital privacy advocacy and information security space were poached by Facebook to join the company's legal counsel just after we conducted our interviews. The fact that Big Tech companies recruit advocates with deep expertise—people who started their careers working in the public sector and who bring significant experience working with congressional leaders and government agencies—is not new or surprising. In fact, the "revolving door" between public- and private-sector jobs in Washington, DC is quite routine and, for better or worse, often leads to charges of "regulatory capture" or the corruption of agencies that come to adopt the interests of those they are charged with regulating. The appointment of current FCC Chair, Ajit Pai, perfectly exemplifies this dynamic. Pai was previously a Verizon corporate attorney who came into his FCC position and immediately repealed net neutrality and consumer privacy laws, both of which favored his former employer and the US telecommunication and ISP sectors. Advocacy workers often move to private companies for the astronomically better pay. And some advocates embrace the challenge of trying to implement progressive changes from within Big Tech companies, which perhaps motivated the three lawyers who recently moved to Facebook. Whatever their reasons are for "crossing over," the loss of advocacy talent is a blow to the community as it affects the continuity of policy struggles as well as institutional memory. It can also leave a mentorship vacuum and require time and resources to recover from so that advocacy momentum can be restored. Perhaps most importantly, the continued blurring of lines between the public sector and private industry, especially in the digital media ecosystem, which remains largely unregulated, save for the corporations' own Terms of Service (TOS) and End User License Agreements (EULAs), is an unhealthy condition that contributes to the erosion of public interest provisions and protections that are desperately needed at this time.

Monitoring of Global Conditions: Human Rights and Corporate Transparency

Given the resurgence of conservative populism and authoritarianism in recent years, digital privacy advocates have spent increasing time and effort monitoring internet policies and data collection practices of nation states and transnational companies, as well as their impacts on people in different parts of the world. Digital privacy advocacy, in other words, extends far beyond the United States and Europe to Brazil and India, Egypt and Ethiopia, China and Iran, to name a few countries. Organizations such as Privacy International, Citizen Lab, ACLU, OTI, EFF, Access Now, and Ranking Digital Rights all undertake global monitoring and advocacy projects. Access Now, for instance, has offices in multiple regions with staff who work in teams focused on policy, advocacy, grants, and technology. Formed in response to the Iranian government's repression of digital activists during the 2009 Green Revolution, Access Now addresses digital privacy concerns through an international human rights framework concerned with user harms, rather than civil liberties, as many US-based digital rights groups. Access Now's work, explains Drew Mitnick, the organization's US Policy and Global Policy Counsel, involves "thinking about the effects of US surveillance for people all over."

As part of its global monitoring work, Access Now operates an international Digital Security Helpline, which provides assistance to journalists, human rights workers, digital activists, and others who need technical assistance related to their internet use. The helpline accepts calls twenty-four hours a day in nine languages. Members of the group's tech team field questions from the helpline. Callers typically seek advice on issues ranging from government shutdowns of civil society blogs to digital safety for journalists and human rights workers. As Mitnick put it, human rights workers' lives "depend on secure communications." Advocates also rely on these calls to understand the changing digital rights challenges faced by internet users in different parts of the world. Each call is also an opportunity for advocates to spread awareness about the helpline's existence and usefulness.

Advocates also undertake other global monitoring activities, from analyzing export controls to calling out corporate security breaches to tracking national or regional policy developments. Scrutinizing export records enables advocates to infer which equipment—particularly surveillance—is going where. Privacy International has been particularly active in tracking the international distribution of digital eavesdropping and lawful interception technologies as well as how these technologies are used in ways that compromise privacy and other human rights. Advocacy organizations also monitor international data protection issues by tracking security breaches and issuing press releases when Big Tech companies violate users' privacy. For example, Access Now critiqued WhatsApp for a 2019 security breach that exposed 1,400 international civil society workers. When asked about assuming such risks on the job, Joseph Jerome of CDT stated, "Privacy advocates don't have privacy."

Several digital privacy advocates we interviewed mentioned the importance of GDPR in Europe and perceived this regional policy development as a sign of international progress in the digital privacy arena. One interviewee insisted that GDPR is an important model of digital privacy legislation in the world, and also indicated that open support of GDPR can alienate

some Silicon Valley companies as they are nervous about similar legislation in the United States. Here again, digital privacy advocates must engage in a delicate balancing act when formulating and pushing for privacy-related legislation. They must know the intricacies of GDPR while tempering their enthusiasm for such policies in order to sustain relations with digital companies that are resistant to such measures.

Increasingly, advocates' global monitoring focuses on emergent technologies such as the Internet of Things (IoT), biometrics, sensors, and artificial intelligence. This work requires not only learning about these technologies, but also investigating where they are made and sold, national laws pertaining to their use, and how their use impacts diverse populations. Within some organizations, advocacy workers with law degrees and expertise in international human rights law conduct industry research and apply international law to various tech scenarios in a steady production of white papers and advisory reports. Examples of recent reports include the following: "Human Rights in the Age of Artificial Intelligence", "A Human Rights Response to Government Hacking", and "Recommendations on Privacy and Data Protection in the Fight Against COVID-19."

Monitoring of global conditions also entails studying and providing information about the Big Tech companies that dominate the world's media and information industries. The project Ranking Digital Rights (RDR) reviews publicly disclosed records of two dozen telecommunications and internet and mobile ecosystem companies, and generates a Corporate Accountability Index that ranks these companies based on their policies and commitments to freedom of expression, privacy, and security. RDR also produces "company report cards" that offer discussions of each company's performance in these categories. Housed at the New American Foundation and co-founded by internet researcher, Rebecca MacKinnon, these rankings are now used by internet users, governments, and companies around the world. Sometimes they are even used by investment firms such as Fidelity and Goldman Sachs in determining companies' valuation. As MacKinnon explained to us, "We're looking for enough disclosure that people can credibly be confident that companies are taking appropriate measures and that their policies are responsible. . . . And that people understand what's happening to their data."

Generating the RDR rankings is extremely labor-intensive and is based on a rigorous methodology with multiple rounds of data analysis, described in detail on the organization's website. Producing the rankings requires back-and-forth communication with the companies assessed, review of publicly disclosed corporate records, comparative analysis of findings, development of public information campaigns, writing of reports, and updating of the rankings. The review of the digital privacy category is, according to MacKinnon, "very much grounded in international human rights law"[44] and takes into account community standards across international contexts. In 2019, assessments in the privacy category were based on eighteen indicators that measured corporate commitments and disclosure of policies affecting users' privacy. These indicators range from "users' control over their own user information" to "processes for responding to third-party requests for user information." Russian and Qatari companies (Mail.ru and Ooredoo, respectively) scored the lowest and German and US companies (Deutsche Telecom and Microsoft, respectively) scored the highest in the report's

2019 privacy index. Since these Big Tech firms operate around the world, RDR's advocacy labor "is geared toward equipping global publics with knowledge about these companies."

Since 2015, RDR has released four sets of rankings and the group has built a strong reputation for its salient take on Big Tech. Because of this, some companies have become extremely concerned about these rankings. In the wake of Cambridge Analytica, explains MacKinnon, "Anything that risks harming users is a risk to the value of the business. . . . We know that they're making changes in response to the index." Some company employees have reported back to RDR and indicated they were able to get their managers to pay attention to and address particular privacy concerns because of poor scores in the RDR index. As a sign of the index's powerful influence, some companies have even adopted RDR's methodology to do their own internal self-assessments.

Despite the success of RDR, the organization has faced two major challenges. The first has been finding time and resources to ensure there is "government take-up" of the rankings. As MacKinnon stated,

> We put out this robust index and then we don't have the staff to really engage. We were somewhat reliant on advocacy partners but now everybody's busy. We're trying to double our budget so that we can actually hire somebody who can engage with policymakers in a more systematic way.

This comment alludes to the second challenge—fundraising. RDR's staff must constantly fundraise in order to exist. This fundraising labor involves strategic planning, review of funding opportunities, grant-writing, outreach, and solicitation to sustain the organization's US$1.2 million per year budget, which in 2019 supported about twelve professional staff members. As MacKinnon bluntly put it, "We're basically unsustainable at our current staffing and funding."

Given the heavy workload required to produce the RDR Corporate Accountability Index, it is unclear whether RDR will be financially sustainable in the long term. This is unfortunate given how crucial RDR's reports have been, both in pressuring Big Tech companies to be more publicly accountable and in equipping internet users with information about how these global companies stack up against one another on key digital rights issues. Like the transparency reports discussed earlier, the RDR reports are crucial given the lack of international oversight and minimal regulation of Big Tech at national levels, but these reports are also at risk of being on the chopping block given the resources needed to generate them. To keep up with technological changes, RDR staff have consulted with *Consumer Reports* and the Digital Standard Project, and hope to begin assessing companies in emergent sectors such as the Internet of Things (IoT) and Digital Assistants, but needs to raise US$10 million per year for that to happen.

A final concern that emerged in our interviews was the expanding scope of their work in the context of the globalization of digital surveillance technologies. With "surveillance creep"—the proliferation of surveillance practices in everyday life—comes a constantly changing and growing amount of work for advocates. Cloud computing processes, sensors in the built environment, new forms of data collection, and artificial intelligence are just a few areas of emerging concern among advocacy groups. Some interviewees offered examples of

technologies they had investigated recently, including urban scooter sharing systems, automated/algorithmic moderation of social media content and surveillance data, and autonomous vehicles equipped with sensors. With a growing number of objects in the world collecting data, digital privacy workers are also reckoning with conditions of "advocacy creep," as they are tasked to investigate, monitor, and influence policies in relation to a skyrocketing number of technologies. This enlarging terrain for violating individual privacy also requires a renewed understanding of and respect for the work of the advocates that are devoted to protecting it. Many governments have abandoned their role as a steward of the public interest, corporations seem to be engaged in an arms race to see who can collect the most user data, and what remains is a coalition of technologists, lawyers, and privacy advocates who refuse to give up. Whatever is left of the public interest in the digital space, we owe to them.

Conclusion

The labor practices we have discussed have the potential to inform, improve, and impact media and tech companies and policymakers in significant ways, yet the activities of advocacy groups are typically not registered as relevant to media industry studies. Our research shows, however, that there is an intensifying degree of advocacy–industry coordination taking place, in part because of US regulatory roll-backs under the Trump administration and a gridlocked Congress. Not only do advocacy organization staff members rely on companies for information to do their assessment and agenda-setting work, advocates spend much of their time studying industry operations and engaging directly with workers in Big Tech companies. They apply consistent pressure to these companies and force them to think about how their technologies and operations impact users and publics around the world; they mount legal challenges to various media and tech initiatives to ensure public interests are protected; and they can ultimately wind up working *with* or *for* these companies in ways that might impart the values of advocacy organizations to a system that privileges profit above all else.

Several of our interviewees urged academics to become more involved in supporting their advocacy work, whether in the form of research, educational initiatives, or technology development. As Harold Feld stated, "It's important for the academic community to take stands . . . and to not be afraid of pushing the envelope." We believe advocacy work should be a topic of research and teaching in media industry studies as well as a workforce pipeline for media studies students and scholars. Digital rights advocates have devised tactics for accessing proprietary information about corporate practices and technologies; translated highly technical, legal, and corporate records into publicly intelligible information; formed coalitions to set advocacy agendas; and pressured corporations to uphold the law. Through these practices, and others, advocacy organizations and their devoted, relentlessly optimistic workers help us to connect the dots between digital privacy, online surveillance, and the erosion of democracy. Understanding these relations can inspire future generations of students and scholars to participate in the protection of digital rights themselves. Our scholarly community could apply additional

pressure on Big Tech not only through our research, but also by integrating advocacy labor into media industries courses, helping to establish and prepare students for advocacy internship programs, and designing collaborative research projects that bring together advocacy organizations, academic, and industry partners. "Life is too short to do bad policy," as Feld insisted, and it is our shared responsibility as media industries scholars and educators to help prevent that tragedy.

---

[1] The authors would like to thank the digital rights advocates and researchers who participated in our interviews and shared their experiences and insights in late 2018 and early 2019. We also thank MIT graduate students, Iago Camargo Bojczuk and Diego Cerna Aragon, for their helpful research assistance, the MIT International Policy Lab for a small grant that supported this research, and three anonymous reviewers for their helpful feedback and comments.

[2] Jennifer Holt is Associate Professor of Film and Media Studies at the University of California, Santa Barbara. She is the author of *Empires of Entertainment* and co-editor of *Distribution Revolution*; *Connected Viewing*; and *Media Industries: History, Theory, Method*. Her current projects include the monograph *Cloud Policy* and the co-edited *Sage Handbook of the Digital Media Economy*.

[3] Lisa Parks was Professor of Comparative Media Studies at MIT when this research was conducted, and in 2020 was appointed as Distinguished Professor of Film and Media Studies at UC Santa Barbara, where she directs the Global Media Technologies and Cultures Lab (https://globalmediaucsb.org/). She is the author of *Cultures in Orbit* and *Rethinking Media Coverage: Vertical Mediation and the War on Terror* and is working on a new co-edited collection called *Media Backends: Digital Infrastructure and the Politics of Knowing*.

[4] These include the data of 3.5 billion records from Yahoo user accounts in 2013–2014; over 150 million customers of credit reporting company Equifax in 2017; 500 million records from customers of Marriott International in 2018; and the accounts of 267 million Facebook users in 2019. Sony Pictures (2011) and the US Government (2006–2011) have also been the subjects of high profile hacks.

[5] Shoshana Zuboff, *Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (NY: PublicAffairs, 2019), 11.

[6] See, for example, Alexis Madrigal, "What Facebook Did to American Democracy," *The Atlantic*, October 12, 2017, https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/; Katharine Viner, "How Technology Disrupted the Truth," *The Guardian*, July 12, 2016, https://www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth; Samanth Subramanian, "Inside the Macedonian Fake-News Complex," *Wired*, February 15, 2017, https://www.wired.com/2017/02/veles-macedonia-fake-news/.

[7] An extensive literature is developing, but Safiya Umoja Noble's *Algorithms of Oppression* (NY: New York University Press, 2018), Joseph Turow's *The Aisles have Eyes* (New Haven, CT: Yale University Press, 2017), and Nick Srnicek's *Platform Capitalism* (Malden, MA: Polity Press, 2017) are some that highlight the many problems of our digital media ecosystem.

[8] For instance, *The Creepy Line* (2018), *Do You Trust This Computer?* (2018), *The Facebook Dilemma* (2018), and *The Great Hack* (2019).

[9] General Data Protection Regulation website, 2018, https://www.gdpr.org/.

[10] Kathleen Hall Jameison, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know* (Oxford: Oxford University Press, 2018); Yochai Benkler, Robert Harris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Oxford: Oxford University Press, 2018).

[11] See Paul Starr, "How Neoliberal Policy Shaped the Internet—And What to do About it Now," *The American Prospect*, October 2, 2019. https://prospect.org/power/how-neoliberal-policy-shaped-internet-surveillance-monopoly/.

[12] In 2019, for instance, the Federal Trade Commission required Facebook to pay a US$5 billion fine in connection with the 2018 Cambridge Analytica breach which resulted in the data of over 87 million of their users being harvested and sold without consent to assist political campaigns, including those of Ted Cruz and Donald Trump. Most critics felt the fine was grossly insufficient given the company's projected US$69 billion annual revenue. That same year, Google and YouTube agreed to pay US$170 million for illegally tracking the viewing habits of children in order to better target ads aimed at the site's youngest users. At the same time, the US Securities and Exchange Commission imposed a shockingly lenient penalty of US$100 million against Facebook for making misleading disclosures to investors about the abuses of user data related to the Cambridge Analytica scandal. See Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election; Aaron Mak, "How Much Facebook Has to Pay in Fines and Settlements this Year," *Slate.com*, October 8, 2019, https://slate.com/technology/2019/10/facebooks-2019-fines-and-settlements.htm.

[13] Their work is compounded by the blackboxing of corporate and technical information—conditions in which companies know more and more about consumers and we know less and less about them. Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

[14] Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, CO: Westview Press, 1993); David Lyon and Elia Zureik, eds, *Surveillance, Computers, and Privacy* (Minneapolis: University of Minnesota Press, 1996).

[15] Sarah Igo, *The Known Citizen: A History of Privacy in Modern America* (Cambridge, MA: Harvard University Press, 2018).

[16] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Palo Alto, CA: Stanford University Press, 2009); Daniel Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2010).

[17] Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (New Haven, CT: Yale University Press, 2017); Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, MA: Harvard University Press, 2018).

[18] Finn Brunton and Helen Nissenbaum, *Obfuscation* (Cambridge, MA: MIT Press, 2015).

[19] Zuboff, *Surveillance Capitalism*; Julie Cohen, *Between Truth and Power*: *The Legal Constructions of Informational Capitalism* (Oxford: Oxford University Press, 2019).

[20] Milton Mueller, Brenden Kuerbis, and Christiane Page, "Reinventing Media Activism: Public Interest Advocacy and the Making of U.S. Communication-Information Policy, 1960–2002," White Paper supported by the Ford Foundation's Knowledge, Creativity, and Freedom program, July 15, 2004, p. 87. Also see their article: Milton L. Mueller, Christiane Page, and Brenden Kuerbis, "Civil Society and the Shaping of Communication Information Policy: Four Decades of Advocacy," *The Information Society* 20 (3, 2004): 1–17.

[21] Colin Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge, MA: MIT Press, 2008), xiv

[22] Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, MA: MIT Press, 2015), 10.

[23] Jennifer Holt, "Regulating the Cloud and Defining Digital Markets," *Media Fields* 10 (2015): 1–13; Patrick Vonderau, "Beyond Piracy: Understanding Digital Markets," in *Connected Viewing*: *Selling*, *Streaming*, *& Sharing Media in the Digital Age*, ed. Jennifer Holt and Kevin Sanson (NY: Routledge, 2014), 99–123.

[24] Victor Pickard, *After Net Neutrality*: *A New Deal for the Digital Age* (New Haven, CT: Yale University Press, 2019); Russell Newman, *The Paradoxes of Net Neutrality* (Cambridge, MA: MIT Press, 2019).

[25] Mark Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (Lawrence: University of Kansas Press, 2007); Torin Monahan, *Surveillance in the Time of Insecurity* (New Brunswick, NJ: Rutgers University Press, 2010); Kelly Gates, *Our Biometric Future*: *Facial Recognition Technology and the Culture of Surveillance* (NY: New York University Press, 2011).

[26] For example, Vicki Mayer, Miranda Banks, and John Caldwell, eds, *Production Studies: Cultural Studies of Media Industries* (NY: Routledge, 2009); Miranda Banks, Bridget Conor, and Vicki Mayer, eds, *Production Studies*, *The Sequel!* (NY: Routledge, 2015); Michael Curtin and Kevin Sanson, eds, *Voices of Labor* (Oakland: University of California Press, 2017); Petr Szczepanik and Patrick Vonderau, eds, *Behind the Screen* (NY: Palgrave MacMillan, 2013); Richard Maxwell, *The Routledge Companion to Labor and Media* (NY: Routledge, 2015).

[27] José Van Dijck, Thomas Poell, and Martijn de Waal, *The Platform Society* (NY: Oxford University Press, 2018); Tarleton Gillespie, "The Politics of Platforms," *New Media & Society* 12 (3, 2010): 347–64; Jean-Christophe Plantin, Carl Lagoze, Paul N. Edwards, and Christian Sandvig, "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook," *New Media & Society* 20 (1, 2016): 293–310.

[28] Becky Lentz and Allison Perlman, "Net Neutrality: Working for Internet Freedoms: Network Neutrality in the United States and the Labors of Policy Advocacy—Introduction to Special Section," *International Journal of Communication* 10 (2016): 8, https://ijoc.org/index.php/ijoc/article/view/6522/1859.

[29] Lentz and Perlman, 5773. Beyond this, Allison Perlman's book *Public Interests* chronicles the complicated history of media advocacy and the many battles to influence and

reform American television in the twentieth century. Her scholarship brings forth "narratives of resistance long invisible in histories of American broadcasting" and the complex labor of preparing for, executing, and framing what are often contentious and political campaigns. See Allison Perlman, *Public Interests* (New Brunswick, NJ: Rutgers University Press, 2016). Also see Kathryn Montgomery's originary study of advocacy groups and their impact on television, *Target: Prime Time* (1989).

[30] Allison Perlman, "The Precarity and Politics of Media Advocacy Work," in *Precarious Creativity*, ed. Michael Curtin and Kevin Sanson (Oakland: University of California Press, 2016), 254–66.

[31] Ibid., p. 256.

[32] In addition to Perlman (2016) and Lentz and Perlman (2016) see also Becky Lentz, "The Media Policy Tower of Babble: A Case for 'Policy Literacy Pedagogy,'" *Critical Studies in Media Communication* 31 (2, 2014): 134–40; Chon A. Noriega, *Shot in America: Television, the State, and the Rise of Chicano Cinema* (Minneapolis: University of Minnesota Press, 2000).

[33] We have identified most interviewees by their name, organization, and position held at the time of our interviews. Some have been anonymized due to the sensitive nature of their work.

[34] National Hispanic Media Coalition (NHMC), November 13, 2018, http://www.nhmc.org/nhmc-joins-33-consumer-civil-rights-advocates-public-interest-principles-privacy-legislation/.

[35] See Brian Fung and Craig Timberg, "The FCC Just Passed Sweeping New Rules to Protect Your Online Privacy," *Washington Post*, October 27, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/10/27/the-fcc-just-passed-sweeping-new-rules-to-protect-your-online-privacy/.

[36] In general, there is critical concern among scholars and others about frequent use of non-disclosure agreements (NDAs) by Big Tech companies, as these contracts are used to lay claim to restrict the flow of technical information. Such information is needed for scholars, advocates, and others to be able to determine whether technologies are violating privacy and other rights.

[37] These are government subpoenas issued to gather intelligence related to national security, but they are limited in their scope and do not require a judge's approval. Their use has been heavily contentious, particularly since the introduction of the PATRIOT Act.

[38] See Center for Democracy & Technology's (CDT) financials, which elaborates on the US$6,378,835 in revenue they received in 2018, https://cdt.org/financials/.

[39] See "Sources of Funding for Public Knowledge" on their website https://www.publicknowledge.org/about-us/ and their latest annual report: https://www.publicknowledge.org/documents/public-knowledge-annual-report-2017/.

[40] Perlman, "The Precarity and Politics of Media Advocacy Work," 264.

[41] Rob Pegoraro, "Tech Companies Are Quietly Phasing Out a Major Privacy Safeguard," *The Atlantic*, September 19, 2019, https://www.theatlantic.com/technology/archive/2019/09/what-happened-transparency-reports/599035/.

[42] See, for example, the latest reports from Google: https://cloud.google.com/blog/products/identity-security/google-clouds-semi-annual-transparency-report-now-available and Twitter: https://transparency.twitter.com/en.html.

[43] Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, MA: MIT Press, 2015).

[44] This includes the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international human rights instruments. See Ranking Digital Rights: Privacy on the RDR website: https://rankingdigitalrights.org/index2017/categories/privacy/.

Bibliography

Andrejevic, Mark. *iSpy: Surveillance and Power in the Interactive Era*. Lawrence: University of Kansas Press, 2007.

Bamberger, Kenneth, and Deirdre Mulligan. *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. Cambridge, MA: MIT Press, 2015.

Banks, Miranda, Bridget Conor, and Vicki Mayer, eds. *Production Studies, The Sequel!* New York: Routledge, 2015.

Benkler, Yochai, Robert Harris, and Hal Roberts. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press, 2018.

Cohen, Julie. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press, 2019.

Curtin, Michael, and Kevin Sanson, eds. *Precarious Creativity*. Oakland: University of California Press, 2016.

Curtin, Michael, and Kevin Sanson, eds. *Voices of Labor*. Oakland: University of California Press, 2017.

Gandy, Oscar. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview Press, 1993.

Gates, Kelly. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: New York University Press, 2011.

Gillespie, Tarleton. "The Politics of Platforms." *New Media & Society* 12, no. 3 (2010): 347–64.

Hartzog, Woodrow. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, MA: Harvard University Press, 2018.

Holt, Jennifer. "Regulating the Cloud and Defining Digital Markets." *Media Fields* 10 (2015): 1–13.

Igo, Sarah. *The Known Citizen: A History of Privacy in Modern America*. Cambridge, MA: Harvard University Press, 2018.

Jameison, Kathleen Hall. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know*. Oxford: Oxford University Press, 2018.

Landau, Susan. *Listening In: Cybersecurity in an Insecure Age*. New Haven, CT: Yale University Press, 2017.

Lentz, Becky. "The Media Policy Tower of Babble: A Case for 'Policy Literacy Pedagogy'" *Critical Studies in Media Communication* 31, no. 2 (2014): 134–40.

Lentz, Becky, and Allison Perlman. "Net Neutrality: Working for Internet Freedoms: Network Neutrality in the United States and the Labors of Policy Advocacy—Introduction to Special Section." *International Journal of Communication* 10 (2016): 8. https://ijoc.org/index.php/ijoc/article/view/6522/1859.

Lyon, David, and Elia Zureik, eds. *Surveillance, Computers, and Privacy*. Minneapolis: University of Minnesota, 1996.

MacKinnon, Rebecca. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books, 2013.

Mak, Aaron. "How Much Facebook Has to Pay in Fines and Settlements this Year." *Slate.com*, October 8, 2019. https://slate.com/technology/2019/10/facebooks-2019-fines-and-settlements.html.

Maxwell, Richard. *The Routledge Companion to Labor and Media*. New York: Routledge, 2015.

Mayer, Vicki, Miranda Banks, and John Caldwell, eds. *Production Studies: Cultural Studies of Media Industries*. New York: Routledge, 2009.

Monahan, Torin. *Surveillance in the Time of Insecurity*. New Brunswick, NJ: Rutgers University Press, 2010.

Montgomery, Kathryn C. *Target: Prime Time*. New York: Oxford University Press, 1989.

National Hispanic Media Coalition (NHMC), November 13, 2018. http://www.nhmc.org/nhmc-joins-33-consumer-civil-rights-advocates-public-interest-principles-privacy-legislation/.

Newman, Russell. *The Paradoxes of Net Neutrality*. Cambridge, MA: MIT Press, 2019.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press, 2009.

Noriega, Chon A. *Shot in America: Television, the State, and the Rise of Chicano Cinema*. Minneapolis: University of Minnesota Press, 2000.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.

Pegoraro, Rob. "Tech Companies are Quietly Phasing out a Major Privacy Safeguard." *The Atlantic*, September 19, 2019. https://www.theatlantic.com/technology/archive/2019/09/what-happened-transparency-reports/599035/.

Perlman, Allison. *Public Interests*. New Brunswick, NJ: Rutgers University Press, 2016.

Pickard, Victor. *After Net Neutrality: A New Deal for the Digital Age*. New Haven, CT: Yale University Press, 2019.

Plantin, Jean-Christophe, Carl Lagoze, Paul N. Edwards, and Christian Sandvig. "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook." *New Media & Society* 20, no. 1 (2016): 293–310.

Szczepanik, Petr, and Patrick Vonderau, eds. *Behind the Screen*. New York: Palgrave Macmillan, 2013.

Solove, Daniel. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2010.

Tiku, Nitasha. "Most of the Google Walkout Organizers Have Left the Company." *Wired*, July 16, 2019. https://www.wired.com/story/most-google-walkout-organizers-left-company/.

Turow, Joseph. *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*. New Haven, CT: Yale University Press, 2017.

Van Dijck, José, Thomas Poell, and Martijn de Waal. *The Platform Society*. New York: Oxford University Press, 2018.

Vonderau, Patrick. "Beyond Piracy: Understanding Digital Markets." In *Connected Viewing: Selling, Streaming, & Sharing Media in the Digital Age*, edited by Jennifer Holt and Kevin Sanson, 99–123. New York: Routledge, 2014.

Wakabayashi, Daisuke, et al. "Google Walkout," *New York Times*, November 1, 2018. https://www.nytimes.com/2018/11/01/technology/google-walkout-sexual-harassment.html.

Zuboff, Shoshana. *Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.