27

FROM PROCEDURAL RIGHTS TO POLITICAL ECONOMY

New Horizons for Regulating Online Privacy

Daniel Susser

PENNSYLVANIA STATE UNIVERSITY, USA

Introduction

The 2010s were a golden age of information privacy research, but its policy accomplishments tell a mixed story. On one hand, promising new theoretical approaches were developed. At the decade's start, for example, contextual integrity theory lent analytical precision and normative force to intuitions that privacy is deeply social and context-specific (Nissenbaum, 2010).[1] At its end, theories of "informational" and "surveillance" capitalism began to lay bare privacy's political economy (Cohen, 2019; Zuboff, 2019).

At the same time, a series of revelations and scandals brought the full extent and concrete significance of digital surveillance to public consciousness, motivating renewed enthusiasm amongst policy makers for efforts to strengthen privacy. In 2013, Edward Snowden exposed the breadth and depth of government digital surveillance (especially by intelligence, national security, and law enforcement agencies), and the insinuation of national governments and their surveillance apparatuses into networks owned and operated by private companies (Greenwald, 2014). Beginning in 2016, the Facebook/Cambridge Analytica scandal[2] focused attention more squarely on private sector data practices, making plain the contours of a digital economy built on targeted advertising and dramatizing the harms it threatens (*The Cambridge Analytica Files*, n.d.). Meanwhile, the rise of China's "social credit system" and the role of digital surveillance in the repression of its minority Uyghur population raised urgent questions about privacy and surveillance outside the West (Buckley & Mozur, 2019; Dai, 2018).

Yet despite significant progress on the development of privacy theory and compelling demonstrations of the need for privacy in practice, real achievements in privacy law and policy have been, at best, uneven. On one hand, there have been meaningful developments in the European Union. Adoption of the General Data Protection Regulation (GDPR) in 2016, and its enactment in 2018, signaled the possibility of a new era in privacy and data protection law – regulation finally catching up to technology after decades of passivity (Satariano, 2018). In the US, on the other hand, there has been a massive failure to act. While several states have enacted privacy legislation, and in spite of broad consensus that action at the federal level is needed, the prospect of new comprehensive privacy protections appears dim (Kerry, 2021).

Of course, social media has been at the center of these stories. Online privacy was fraught prior to the emergence of Facebook, Twitter, Snapchat, and TikTok – from the earliest moments of the commercial internet researchers and activists have raised the alarm about data collection by

DOI: 10.4324/9781003244677-32

governments and private firms, and about the use of information collected online to monitor, sort, and manage people (Agre, 1994; Gandy, 1996). But the rise of social media platforms brought a sea change, as more people started spending more time online, and as digital technologies began to mediate more of our social, economic, and political lives. Facebook (and parent company Meta) is now one of the world's largest data collectors, gathering information about its nearly 3 billion users and their activity on its platform, as well as information about the activities of non-Facebook-users on the internet and through the physical world via web trackers and smartphone sensors (Wagner, 2018). Twitter is more than a message board for clever one-liners; it is a major gatekeeper of news and information, the primary medium through which many businesses, government agencies, politicians, and public figures communicate with their constituents. The privacy challenges we face are therefore deeper and more urgent than ever, but also more complex, involving a wide range of normative tradeoffs and implicating increasingly powerful interests.

In what follows, I describe three broad shifts in the way privacy scholars (and, to some degree, privacy advocates and policy makers) are approaching social media. First, whereas privacy was once primarily understood as an individual interest, and the role of privacy policy as strengthening each individual's ability to realize it, there is now increasing emphasis on the social and relational nature of privacy, and – concomitantly – on structural approaches to privacy policy. Second, while public and private actors have both been understood to pose threats to privacy, the center of gravity in privacy discussions has moved from worries about government surveillance to worries about data collection by private firms, and the frame for conceptualizing these problems has expanded from a predominantly rights-based model to one that includes an important political economy perspective. Third, at the beginning of the social media era, these technologies were largely understood as tools for facilitating interpersonal communication and privacy questions were cast in those terms. Today, there is growing recognition that social media platforms have become part of society's basic communications infrastructure – a kind of "digital public sphere" – and that social media regulation needs to reflect this larger social and political context.

It is worth emphasizing at the outset that these are not brand-new ideas only recently emerging in the literature. Scholars have to some degree or other recognized and wrestled with them for decades. My aim is to highlight trends – shifts in the relative attention and significance given to alternative frames. They point to rich conceptual and normative resources, the tools to find our way toward privacy in a digital world.

Shift 1: The Structural Turn

Traditionally, privacy was understood as a right of individuals against unwanted attention or trespass – the "right to be let alone," in Samuel Warren and Louis Brandeis's formulation (1890). Throughout the last century, as technology furnished new ways to observe people and invade their private spaces, what it means to be "let alone" evolved. There are many strands to this evolutionary story, familiar from privacy studies (Sloot & Groot, 2018). Relevant for present purposes is the application – or, perhaps, the adaptation – of privacy rights to information technology. Beginning in the 1960s, especially with the publication of Alan Westin's (1967) *Privacy and Freedom*, privacy in the digital context became equated with an individual's (or group's) right to control information about themselves – so-called "personal information." To be "let alone" meant to only have information about oneself captured, stored, and analyzed according to one's own wishes, and – eventually – with one's consent (Gellman, 2017; Susser, 2019).

The idea that digital privacy is control over personal information was formalized in the US Fair Information Practices (FIPs) in 1973, codified in the US Privacy Act of 1974, exported to Europe as the Organization for Economic Cooperation and Development (OECD) privacy principles in 1980, and enshrined in European law in the form of the 1995 EU Data Protection Directive (Gellman,

2017). According to the Fair Information Practices, data collectors are responsible for notifying data subjects that information about them is going to be collected and processed, and soliciting their consent for it.[3] It is for this reason that websites and apps present "clickwrap" privacy agreements when users first log in, asking for confirmation that one has read the privacy policy and consents to its terms and conditions. Daniel Solove famously described this as "privacy self-management" – each individual left to contemplate the data practices of each data collector and to decide for themselves whether or not to participate (Solove, 2013).

This approach was contested from the start, both for its theoretical understanding of privacy and as a policy framework for managing increasingly data-driven societies. Scholars put forward competing theories – some argue privacy is more about access to people than control over such access (Gavison, 1980), others that control theories misunderstand the relationship between privacy and intimacy (Rachels, 1975; Reiman, 1976) or the connection between privacy and trust (Waldman, 2018), or that controlling information is one dimension of privacy but not its entirety (Nissenbaum, 2010; Susser, 2016). Practically, many pointed out that privacy self-management simply doesn't work: Privacy policies are too long and difficult to read. They can't be negotiated and fail to offer real choices. And even if they could be and did, there are too many data collectors for each person to manage (see Susser, 2019 for an overview).

More fundamentally, critics of privacy-as-control pointed out that this approach misapprehends the interests privacy rights protect. Privacy is not simply an individual right protecting individual interests; it is a social value, emerging from long-standing social norms and practices, and cherished for its effects on society as a whole (Nissenbaum, 2010). Without privacy, for example, citizens cannot formulate and voice the critical perspectives necessary for democratic self-government (Cohen, 2013). It is a "public," "common," and "collective" value, to use Priscilla Regan's terms (Regan, 2009).

Understanding privacy as a social value has immediate implications for policy. If we value privacy not only for its benefits to individuals but also for its impacts on society, then it makes little sense to place decisions about privacy in individual hands. Privacy self-management is a non-starter – we do not ask individuals to self-manage air quality or street traffic, and asking them to self-manage data is equally unrealistic in a data-driven world. What is needed is a *structural* approach, and the last decade has seen both deepening appreciation for and significant developments of this perspective. Through a structural lens, the primary goal of privacy law and policy is not to strengthen each person's ability to control information about themselves (though it may aim for that too), but to ensure information flows in ways that are conducive to privacy's individual and social ends.

In the realm of privacy theory, these developments can be seen in a range of new approaches that took shape in recent years. Neil Richards argues a "structural turn" was inaugurated in the US context in the early work of the "Information Privacy Law Project" – a loose confederation of legal scholars in the late 1990s and early 2000s who carved out and established the field of information privacy law (Richards, 2006). For these scholars, it was clear that digital privacy required a macro-perspective, focusing less on individuals and individual rights and more on the power relationships between data collectors and data subjects (Solove, 2004). Which is to say, shifting attention from traditional worries about each particular "invasion" of privacy to the systemic conditions created by society-wide architectures of digital surveillance and data processing (Richards, 2006, p. 1095).

Yet only recently were conceptual tools introduced that fully realized this structural perspective. First, Helen Nissenbaum's "contextual integrity" theory provided a new lens through which to understand both the source and normative content of demands for information privacy, and located each in the midst of social life. Privacy as a value emerges, Nissenbaum argues, in relation to particular social contexts – e.g., the home, the workplace, or the doctor's office – to ensure that information flows in ways conducive to their ends, goals, and purposes (Nissenbaum, 2010). And what privacy demands is specific to each context: the rules for how information should flow are

different at home and at work. One reason social media complicates privacy is it tends to "collapse" these different contexts (Marwick & boyd, 2010). Second (and in much the same spirit), a number of scholars have argued that privacy law and policy should train their sights on relationships of trust, such as fiduciary relationships, and work to ensure that data collection and use practices build and justify that trust. Rather than focusing on people's individual privacy preferences, these approaches would orient privacy law and policy toward relational values, like duties of loyalty and care (Balkin, 2021; Richards & Hartzog, 2020; Waldman, 2018). Third, in the last decade, it has become increasingly clear that the real stakes of data collection – its costs and its benefits – lie not in any specific pieces of information, but rather in the pooling together and analysis of data at scale. Appreciating this requires a structural vantage point. Thus, new approaches are emerging that take aggregated data as their starting point and ask how collective, democratic values can guide discussions about privacy and surveillance (Viljoen, 2021).

This theoretical shift is also starting to materialize in new policy, most importantly the European GDPR. Enacted in 2016 and made effective two years later, GDPR is "the most consequential regulatory development in information policy in a generation," though its concrete requirements are still being articulated and the full scope of its effects is yet to be felt (Hoofnagle et al., 2019, p. 66). At a basic level GDPR takes a FIPs-based approach takes a FIPs-based approach, meaning it focuses primarily on procedural rather than substantive safeguards, designed to give individuals control over personal information and to ensure that data is accurate and secure.[4] But it reflects lessons learned about the need for structural intervention. For example, while individual consent plays a role in GDPR it is not "core" to its protections (Leta Jones & Kaminski, 2021, p. 108). Data processing is presumed unlawful in advance, consent is only one of several mechanisms for legitimating it, and consenting to data collection and processing does not waive other protections, such as accuracy and data minimization requirements (Hoofnagle et al., 2019; Leta Jones & Kaminski, 2021).

The structural turn is also having an impact in the US, though policy makers there have been much slower to act. At the federal level, lawmakers have introduced dozens of data- and privacy-related bills targeting everything from "individual rights and business obligations, to special protections for sensitive information and access to records by law enforcement, to emerging technologies such as facial recognition and artificial intelligence" (International Association of Privacy Professionals, 2021). As of this writing, however, none has been adopted. By contrast, more than half the states have introduced new privacy legislation, and in recent years online privacy laws have passed in California, Colorado, Maine, Nevada, and Virginia (International Association of Privacy Professionals, 2022). While many of these efforts aim to strengthen the FIPs there is growing recognition that systemic change is needed, one sign of which is renewed enthusiasm for using competition policy to rein in the power of Silicon Valley's biggest firms. A growing chorus of academics and regulators – most visibly, the legal scholar and current Chairperson of the Federal Trade Commission, Lina Khan – have taken aim at the largest data collectors and seek to strengthen privacy indirectly, not by giving individuals more control over information flows, but by using antitrust law to undo the massive concentration of information (and the power it confers) in relatively few hands (Kolhatkar, 2021).[5]

Shift 2: Privacy's Political Economy

Demands for privacy have always tracked the shifting landscape of surveillance (Igo, 2018), and from the early days of the commercial internet some prescient observers warned of the need to update our privacy "threat model" (to borrow a security term), as intrusive surveillance was beginning to originate as much from data collection by private firms as it did from governments (Agre, 1994; Gandy, 1996). But this argument has only gotten real purchase in the public imaginary more recently, in the wake of major scandals like the Facebook/Cambridge Analytica affair. For the first

time, there is widespread concern about Big Tech's core business model – collecting, analyzing, and selling personal information (Pew Research Center, 2019; Radu, 2020). The targeted advertisements it makes possible are increasingly seen as creepy (Tene & Polonetsky, 2013; Dobber, this volume) and manipulative (Susser et al., 2019), rather than useful and convenient (as Silicon Valley has long contended) (Zuckerberg, 2019). And so, discussions about strengthening digital privacy are focusing more and more on regulating the surveillance economy.

Doing so requires, first, understanding the specific nature of Big Tech firms – especially social media companies – which is to say, it requires a theory of *platforms*. A kind of digital intermediary, platforms are the infrastructures that make possible all manner of online interaction and commerce (Cohen, 2019; Gillespie, 2010; Srnicek, 2017). Unlike other firms, which produce and distribute goods or services, platforms exist to facilitate connection. eCommerce platforms, like Amazon, connect buyers to sellers. Gig economy platforms, like Uber and Lyft, connect service providers (e.g., drivers) to customers. Social media platforms, like Facebook and Twitter, connect advertisers to eyeballs. In the process of facilitating these connections, platforms collect, analyze, and monetize data about them. And this data collection is not incidental: surveillance is the lifeblood of digital firms. As Julie Cohen writes, platforms are designed, fundamentally, for "data-based surplus extraction" (2019, p. 40).

Business models centered on surveillance and the selling of personal information tend toward specific economic dynamics – most importantly, market concentration and high barriers to exit (Haucap & Heimeshoff, 2014). Platforms are governed by network effects: the more people choose to use a particular platform the more attractive it becomes to other users. As Nick Srnicek writes:

> [T]his generates a cycle whereby more users beget more users, which leads to platforms having a natural tendency toward monopolisation. It also lends platforms a dynamic of ever-increasing access to more activities, and therefore to more data. Moreover, the ability to rapidly scale many platform businesses by relying on pre-existing infrastructure and cheap marginal costs means that there are few natural limits to growth.
>
> *(Srnicek, 2017, pp. 30–31)*

In addition, as Cohen argues, platforms are designed to make leaving for a competitor's alternative as difficult as possible. They are configured, she writes, "with the goal of making clusters of transactions and relationships stickier – sticky enough to adhere to the platform despite participants' theoretical ability to exit and look elsewhere for other intermediation options" (Cohen, 2019, p. 41). For example, most major platforms are intentionally non-interoperable. If someone gets fed up with Facebook, there is no easy way to move their data to another social media platform. Posts, photographs, chat histories – sometimes many years' worth – are stuck where they are.

These economic tendencies help explain the growth and consolidation of digital firms and also indicate obstacles to governing them (Brennan-Marquez and Susser, 2022). For privacy advocates, the question is how to bring surveillance under control when digital platforms, designed for and premised on the limitless expansion of data collection, sit at the center of global economies (the largest are currently some of the most valuable corporations in the world). Shoshana Zuboff argues that the dominance of companies such as Google and Facebook/Meta has inaugurated a new economic era – "surveillance capitalism" – in which people are treated not as consumers (to be served and satisfied), but rather as "objects from which raw materials are extracted and expropriated" (Zuboff, 2019, p. 94). Google and Facebook want data about us in order to predict and manipulate our beliefs, desires, and behavior with targeted advertisements. "Surveillance capitalism's products and services are not the objects of a value exchange," Zuboff writes, "They do not establish constructive producer-consumer reciprocities. Instead they are 'hooks' that lure users into their

extractive operations in which our personal experiences are scraped and packaged as the means to others' ends" (Zuboff, 2019).

Complicating things further, recent scholarship demonstrates that law itself has been instrumental to the development of the surveillance economy. Contrary to standard narratives of privacy laws simply failing to "keep up" with the break-neck pace of technological innovation, exploring these issues through a law and political economy lens reveals the "facilitative role" law has played in turning personal information into the kind of commodity technology firms can own, sell, and profit from (Cohen, 2019, p. 8).[6] Much like law facilitated the "enclosure" of land and related practices of ownership and control that marked the transition from an agrarian economy to industrial capitalism in the 18th and 19th centuries, law has been constitutive of the transition currently underway, to surveillance or "informational" capitalism.[7] In particular, as Amy Kapczynski argues (following Cohen), without changes in intellectual property law – especially trade secrecy and contract law – "platform power could not have evolved as it has" (Kapczynski, 2020, p. 1503).

So what is to be done? While research in this area is only in its early stages, certain lessons are already in view: First, an analysis of the political economy of privacy lends support to the "structural turn" described in the previous section. Standard regulatory tools for ensuring fair consumer-business relationships, such as procedural rules that make business practices more transparent and solicit consumer consent, are obviously ill-suited for this world. It is difficult to imagine, for example, any set of FIPs-like requirements mitigating the harms platforms threaten, no matter how carefully enforced. If platforms derive their power, in part, from network effects (that tend toward market concentration) and specific technological affordances (that make it difficult to exit, and thus, for competitors to emerge), then there is little reason to believe individual users, each in their own relationships with firms, can act as a meaningful counterbalance. Importantly, this does not mean law and policy should ignore these relationships – even if structural changes are achieved, individuals will need support as they continue to manage information about themselves, and transparency still brings some benefits (Susser 2017; Susser, 2019). Structural interventions and individual protections are each necessary (but not sufficient), and privacy advocates and policy makers will need to think holistically about how they can be integrated (Kaminski, 2019).

Second, if the very harm regulation aims to prevent – surveillance – is the source of Big Tech's profits, then structural change must take a particular form: remaking the industry's dominant business model. If we are serious about privacy in the digital world, technology firms (especially social media companies) will have to find new ways to make money. Various proposals already exist for setting this transformation in motion. The "new antitrust" movement, discussed in the previous section, offers one approach. Though it is not obvious why competition amongst surveillance firms should lead to less surveillance overall (Balkin, 2021; Cohen, 2021). Tackling the problem more directly, a number of advocacy organizations, policy makers, and regulators have called for a ban on behavioral or "surveillance-based" advertising outright (Forbrukerrådet, 2021; Vinocur, 2021). That does not mean prohibiting advertising altogether, but rather returning to a status quo ante where ads were positioned using contextual information (such as the content of the website where the ad appears) instead of detailed personal profiles. Whatever tools we choose to use, the future of digital privacy requires ending the surveillance business.

Shift 3: The Digital Public Sphere

Finally, discussions about online privacy cannot be divorced from the larger context in which social media has become, in the last decade, more than a means of connecting people to one another (or connecting them to advertisers, depending on your perspective). For better or worse, it has become an integral part of society's communications infrastructure – a "digital public sphere" (Balkin, 2021). This fact is evident everywhere, from the complex interchange between social media and popular

culture, to its use for government communications and political messaging, to the role it plays in generating and disseminating news. While much of the debate around regulation and the digital public sphere focuses on questions about free speech, privacy is centrally important too.

As Jack Balkin argues, a "healthy and vibrant" public sphere promotes *democratic participation* (the two-way flow of information and opinion from the public to government and back again), *democratic culture* (influence from a wide spectrum of people and communities on ideas that shape individual and social identity), and *the growth and spread of knowledge* (Balkin, 2021, pp. 77–78), and the aim of regulating the organizations, technologies, and practices that facilitate the public sphere should be to ensure they help realize these values. Social media companies, Balkin writes, "have already constructed a digital public sphere in which they are the most important players" (Balkin, 2021, p. 96). Thus, law and policy should design rules and incentives to encourage, amongst other things (such as a diversity of media sources, governed by professional and public-regarding norms) that social media platforms act as "trusted and trustworthy intermediate institutions" (Ibid.).

Surveillance and manipulation are antithetical to these goals, as recent history has demonstrated: as public awareness about surveillance capitalism has grown trust in social media platforms has declined, and for good reason (Social Media and Cybersecurity, 2021). Privacy is an antidote. It guarantees (as much as possible) that people feel safe communicating – capable of authentically expressing their beliefs and opinions, and open to encountering alternative perspectives – necessary for democratic participation (Cohen, 2013). Privacy creates space for the creativity and experimentation critical for the development of a robust democratic culture (Ibid.). And privacy fosters trust, essential for the spread of knowledge and for combating the paranoia in which mis- and dis-information thrive. Though it might sound paradoxical, privacy is at the heart of a well-functioning public sphere.

Understanding social media and privacy through this lens complements developments described in the previous sections, offering further reasons to incorporate structural perspectives into privacy discussions and strengthening the case against surveillance-based business models that undermine public trust. Moreover, the normative guideposts it recommends point toward additional concrete governance strategies: If social media is critical infrastructure, we could regulate it as a public utility (Rahman, 2018). If the dominant platforms can't fathom alternatives to existing surveillance-based business models, we could publicly fund alternatives. Perhaps, as Ethan Zuckerman and others have argued, the digital public sphere demands "digital public infrastructure": Wikipedia could serve as a model (Zuckerman, 2020), or the BBC in the UK and PBS in the US (Coatney, 2019). Or we could simply forbid social media companies from treating users as objects of surveillance and manipulation by imposing fiduciary obligations – duties of loyalty, confidentiality, and care (Balkin, 2020).

Conclusion

The shifts in perspective and approach outlined above point toward new horizons for privacy theory and practice. They offer invaluable resources for remaking social media, and the digital world more broadly, into technosystems that respect privacy and serve individual, social, and democratic ends. The next decade will decide whether we heed these lessons or remain in thrall to the frameworks and strategies that got us where we are. Of course, none of this occurs in a vacuum – privacy's prospects are inextricably connected with the deeper social, economic, and political conditions we face. Understanding what new laws are needed, for example, is not the same as marshaling the power to enact them, and skepticism about our capacity for progress on these fronts is not unreasonable. But there is, perhaps, also reason for optimism. A defining feature of the advances discussed throughout this chapter is, precisely, an ever-expanding theoretical aperture – greater attention to and appreciation for privacy's complex relationship with social contexts, economic systems, and political values. We have many of the tools we need, the question is whether we will use them.

At the same time, important questions remain unresolved. To close, consider three issues in need of attention from privacy and social media scholars moving forward: First, while the structural approaches to privacy, discussed above, are essential, they ought to be viewed as complements to (rather than replacements for) approaches that focus on individual rights. Yet few have tried to explain how to reconcile or integrate them. Successfully regulating social media privacy means enabling individuals to advance their informational interests while recognizing that those interests are interwoven – *networked* – with the interests of others, and that there are social and political interests to account for too. Second, work on the political economy of information has raised devastating moral and political objections to the surveillance-based business models social media companies rely on, but we have only begun to glimpse plausible alternatives. Indicting surveillance capitalism is not enough; we must conjure a future beyond it (Susser 2022). Finally, there remains the challenge of translating these theoretical insights into practice, using them to shape concrete legislation. As we've seen, privacy is a complex value and social media is a complicated enterprise. To meet this challenge scholars, policy makers, activists, and advocates must think and work together to chart the course ahead.

Notes

1 Nissenbaum elaborated this theory comprehensively in her (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, though she had already sketched the main ideas in earlier work (Nissenbaum, 2004). It is in the decade since *Privacy in Context* was published, however, that its approach to conceptualizing privacy problems has become a dominant force shaping the field.
2 Facebook (the company) has rebranded as Meta, a container organization for various social media platforms, including – in addition to Facebook – Facebook Messenger, Instagram, and WhatsApp. In this chapter, I am mostly interested in Facebook as a social media platform (rather than in its corporate form), so I refer to Facebook rather than Meta.
3 There are many iterations of the FIPs, which enumerate a range of principles, including rights of access, participation, data minimization, and security. But notice (or "transparency") and consent (or "choice") are the dominant focus in both privacy theory and privacy practice. For a detailed history, see (Gellman, 2017).
4 Hoofnagle et al. call GDPR "FIPs on steroids" (2019, p. 78). Richards and Hartzog describe it as "the strongest implementation of the FIPs to date" (2020, p. 1).
5 For an overview of what some have called the "new Brandeisian" approach to antitrust, see (Khan, 2020). On potential limitations of this approach, see (Balkin, 2021; Cohen, 2021).
6 "Own" is a complicated story. See (Kapczynski, 2020, p. 1502) on the "indicia of ownership."
7 Cohen prefers "informational capitalism" (following Manuel Castells) to "surveillance capitalism," because it focuses attention on "the underlying transformative importance of the sociotechnical shift to informationalism as a mode of development" (Cohen, 2019, p. 6).

References

Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, *10*(2), 101–127. https://doi.org/10.1080/01972243.1994.9960162
Balkin, J. M. (2020). The fiduciary model of privacy. *Harvard Law Review*, *134*, 11–33.
Balkin, J. M. (2021). How to regulate (and not regulate) social media. *Journal of Free Speech Law*, *1*, 71–96.
Brennan-Marquez, K., & Susser, D. (2022). Privacy, Autonomy, and the Dissolution of Markets. *Knight First Amendment Institute*. https://knightcolumbia.org/content/privacy-autonomy-and-the-dissolution-of-markets
Buckley, C., & Mozur, P. (2019, May 22). How China Uses High-Tech Surveillance to Subdue Minorities. *The New York Times*. https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html
Coatney, M. (2019, September 24). We Need a PBS for Social Media. *The New York Times*. https://www.nytimes.com/2019/09/24/opinion/public-broadcasting-facebook.html
Cohen, J. E. (2013). What privacy is for. *Harvard Law Review*, *126*, 1904–1933.
Cohen, J. E. (2019). *Between truth and power: the legal constructions of informational capitalism*. Oxford University Press.

Cohen, J. E. (2021). How (not) to write a privacy law. *Knight First Amendment Institute*. https://knightcolumbia.org/content/how-not-to-write-a-privacy-law

Dai, X. (2018). Toward a reputation state: the social credit system project of China. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3193577

Forbrukerrådet. (2021). *Time to Ban Surveillance Advertising: The Case Against Commercial Surveillance Online*. https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf.

Gandy, O. (1996). Coming to terms with the panoptic sort. In D. Lyon & E. Zureik (Eds.), *Computers, surveillance, and privacy*. University of Minnesota Press.

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, *89*(3), 421–471.

Gellman, R. (2017). Fair information practices: A basic history. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.2415020

Gillespie, T. (2010). The politics of "platforms." *New Media & Society*, *12*(3), 347–364. https://doi.org/10.1177/146144480934273

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US Surveillance State*. Macmillan.

Haucap, J., & Heimeshoff, U. (2014). Google, Facebook, Amazon, eBay is the Internet driving competition or market monopolization. *International Economics and Economic Policy*, 11(1), 49–61.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Igo, S. E. (2018). *The known citizen: A history of privacy in modern America*. Harvard University Press.

International Association of Privacy Professionals. (2021). *US Federal Privacy Legislation Tracker*. https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/

International Association of Privacy Professionals. (2022). *US State Privacy Legislation Tracker*. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Kaminski, M. E. (2019). Binary governance: Lessons from the GDPR's approach to algorithmic accountability. *Southern California Law Review*. https://doi.org/10.2139/ssrn.3351404

Kapczynski, A. (2020). The law of informational capitalism. *Yale Law Journal*, *129*, 1460–1515.

Kerry, C. (2021, August 16). One Year After Schrems Ii, the World Is Still Waiting for U.s. Privacy Legislation. *Brookings*. https://www.brookings.edu/blog/techtank/2021/08/16/one-year-after-schrems-ii-the-world-is-still-waiting-for-u-s-privacy-legislation/

Khan, L. (2020). The end of antitrust history revisited. *Harvard Law Review*, *133*, 1655–1682.

Kolhatkar, S. (2021, November 29). Lina Khan's Battle to Rein in Big Tech. *The New Yorker*. https://www.newyorker.com/magazine/2021/12/06/lina-khans-battle-to-rein-in-big-tech

Leta Jones, M., & Kaminski, M. (2021). An American's guide to the GDPR. *Denver Law Review*, *98*, 93–128.

Marwick, A., & boyd, d. (2010). I tweet honestly, I tweet passionately: Twitter, users, context collapse, and the imagined audience. *New Media & Society*, 13(1), 114–133. https://doi.org/10.1177/1461444810365313

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*, 119–157.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Pew Research Center. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*.

Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, *4*(4), 323–333.

Radu, S. (2020, January 15). The World Wants More Tech Regulation. *U.S. News & World Report*. https://www.usnews.com/news/best-countries/articles/2020-01-15/the-world-wants-big-tech-companies-to-be-regulated

Rahman, K. S. (2018). Internet platforms as the new public. *Georgetown Law Technology Review*, *2*, 234–251.

Regan, P. M. (2009). *Legislating privacy: Technology, social values and public policy*. The Univ. of North Carolina Press.

Reiman, J. H. (1976). Privacy, intimacy, and personhood. *Philosophy & Public Affairs*, *6*(1), 26–44.

Richards, N. (2006). The information privacy law project. *The Georgetown Law Journal*, *94*, 1087–1140.

Richards, N., & Hartzog, W. (2020). A relational turn for data protection? *European Data Protection Law Review*, *6*(4), 492–497. https://doi.org/10.21552/edpl/2020/4/5

Satariano, A. (2018, May 24). G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog. *The New York Times*. https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html

Sloot, B. van der, & Groot, A. de (Eds.). (2018). *The handbook of privacy studies: an interdisciplinary introduction*. Amsterdam University Press.

Social Media and Cybersecurity. (2021, March 1). UNSW Online. https://studyonline.unsw.edu.au/blog/social-media-and-cyber-security-lp

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York University Press.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*, 1880–1903.

Srnicek, N. (2017). *Platform capitalism*. Polity Press.

Susser, D. (2016). Information privacy and social self-authorship: *Techné: Research in Philosophy and Technology*, *20*(3), 216–239. https://doi.org/10.5840/techne201671548

Susser, D. (2017). Transparent media and the development of digital habits. In Y. Van Den Eede, S. O'Neal Irwin, & G. Wellner (Eds.), *Phenomenology and media: Essays on human-media-world relations*. Lexington Books.

Susser, D. (2019). Notice after notice-and-consent: why privacy disclosures are valuable even if consent frameworks aren't. *Journal of Information Policy*, *9*, 148–173. https://doi.org/10.5325/jinfopoli.9.2019.0037

Susser, D. (2022). Data and the Good? *Surveillance & Society*. *20*(3), 297–301.

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review*, *4*, 1–45.

Tene, O., & Polonetsky, J. (2013). A theory of creepy: technology, privacy and shifting social norms. *Yale Journal of Law and Technology*, *16*, 59–102.

The Cambridge Analytica Files. (n.d.). The Guardian. https://www.theguardian.com/news/series/cambridge-analytica-files

Viljoen, S. (2021). A Relational Theory of Data Governance. *Yale Law Journal*, *131*, 573–654.

Vinocur, N. (2021, April 2). The Movement to End Targeted Internet Ads. *Politico*. https://www.politico.eu/article/targeted-advertising-tech-privacy/

Wagner, K. (2018, April 20). This Is How Facebook Collects Data on You Even If You Don't Have an Account. *Vox.Com*. https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg

Waldman, A. E. (2018). *Privacy as trust: Information privacy for an information age* (1st ed.). Cambridge University Press. https://doi.org/10.1017/9781316888667

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193. 10.2307/1321160

Westin, A. (1967). *Privacy and freedom*. Atheneum.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First edition). PublicAffairs.

Zuckerberg, M. (2019, January 25). The Facts About Facebook. *Wall Street Journal*. http://ezaccess.libraries.psu.edu/login?url=https://search-proquest-com.ezaccess.libraries.psu.edu/docview/2170828623?accountid=13158

Zuckerman, E. (2020). The Case for Digital Public Infrastructure. *Knight First Amendment Institute*. https://doi.org/10.7916/d8-chxd-jw34