12

Doughnut Privacy

A Preliminary Thought Experiment

Julie E. Cohen

Previous chapters in the book have highlighted the ways that data-driven technologies are altering the human experience in the digital world. In this chapter, I explore the implications of the "doughnut" model of sustainable economic development for efforts to strike the appropriate balance between data-driven surveillance and privacy. I conclude that the model offers a useful corrective for policymakers seeking to ensure that the development of digital technologies serves human priorities and purposes.

Among environmental economists and some city planners, Kate Raworth's (2017) theory of "doughnut economics" is all the rage. Raworth argues that, in an era when human wellbeing depends on sustainable development rather than on unlimited growth, economics as a discipline can no longer embrace models of welfare oriented exclusively toward the latter. As an alternative model to the classic upward-trending growth curve, she offers the doughnut: an inner ring consisting of the minimum requirements for human wellbeing, a middle band consisting of the safe and just space for human existence, and an ecological ceiling above which continued growth produces planetary disaster.[1]

I will argue, first, that a similarly doughnut-shaped model can advance conceptualization of the appropriate balance(s) between surveillance and privacy and, second, that taking the doughnut model seriously suggests important questions about the uses, forms, and modalities of legitimate surveillance. Foregrounding these questions can help policymakers centre the needs and priorities of humans living in digitally mediated spaces.

A note on definitions: By "surveillance" I mean to refer to sets of sociotechnical conditions (and their associated organizational and institutional practices) that involve the purposeful, routine, systematic, and focused collection, storage, processing, and use of personal information (Murakami Wood 2006). By "privacy" I mean

My thanks to participants in the eQuality Project research workshop "On Being Human in the Digital World" and the 2022 Privacy Law Scholars Conference for their helpful comments, and to Rasheed Evelyn, Conor Kane, and Sherry Tseng for research assistance.

[1] You can see Raworth's (2017) doughnut diagram at www.kateraworth.com/doughnut/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

to refer to sets of sociotechnical conditions (and their associated organizational and institutional practices) that involve forbearance from information collection, storage, processing, and use, thereby creating "...(degrees of) spatial, informational, and epistemological open-endedness" (Cohen 2019b, 13). Although conditions of surveillance and privacy are inversely related, they are neither absolute nor mutually exclusive – for example, one can have surveillance of body temperatures without collection of other identifying information or surveillance of only those financial transactions that exceed a threshold amount – and they are capable of great variation in both granularity and persistence across contexts.

12.1 FROM FRAMING EFFECTS TO MENTAL MAPS: DEFINING POLICY LANDSCAPES

The animating insight behind the doughnut model concerns the importance of mental maps in structuring shared understandings of the feasible horizons for economic and social policymaking. Frames and models create mental maps that foreclose some options and lend added weight to others (van Hulst and Yanow 2016). For that reason, if one wishes to contest existing policy choices, it will generally be insufficient simply to name the framing effects that produced them. Displacing framing effects requires different mental maps.

Specifically, the doughnut model of sustainable development represents an effort to displace an imagined policy landscape organized around the familiar figure of the upward-trending growth curve. The curve depicts (or so it is thought) the relationship between economic growth and social welfare: more is better. That philosophy resonates strongly with the logics of datafication and data extractive capitalism. Unsurprisingly, the imagined topography of policy interventions relating to surveillance is also organized around an upward-trending growth curve, which reflects (or so it is thought) the relationship between growth in data-driven "innovation" and social welfare: here too, more is better. The doughnut model visually reorders policy priorities, producing imagined policy landscapes that feature other human values – sustainability and privacy – more prominently.

12.1.1 *Sustainability and the Economic Growth Curve*

In economic modelling, the classic upward-trending growth curve links increased growth with increased social welfare. The curve tells us that more economic growth produces more social welfare and, conversely, that increasing social welfare requires continuing economic growth (Raworth 2017). The resulting mental map of feasible and desired policy interventions has produced decades of discussions about economic policy that take for granted the primacy of growth and then revolve narrowly around the twin problems of how to incentivize it and, equally important, how to avoid disincentivizing it.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

Although sustainability has emerged over the last half century as a key determinant of social welfare – indeed, an existentially important one – it has no clear place within that imagined landscape. This has become increasingly evident in recent decades. Concerns about long-term sustainability and species survival have fueled increasingly urgent challenges to production and consumption practices that treat resources as infinite and disposable. Those concerns have inspired new approaches to modeling production and consumption as circular flows of resources (Friant et al. 2020). In the abstract, however, circular-economy models have trouble escaping the gravitational pull of a policy landscape dominated by the upward-trending growth curve. In many circular-economy narratives, recycling-driven approaches to production and consumption are valuable, and deserving of inclusion in the policy landscape, precisely because they fuel continuing growth (Corvallec et al. 2022).

The doughnut model is premised on a more foundational critique of growth-driven reasoning. It deploys ecological and systems thinking to model policy frontiers – outer bounds on growth that it is perilous to transgress. And it represents those boundaries using a crisp, simple visual depiction, offering policymakers a new imagined landscape for their recommendations and interventions (Raworth 2017, 38–45). It compels attention to sustainability considerations precisely because it forces us to look at them – and it demands that ostensibly more precise mathematical models and forecasts organized around growth be dismantled and reorganized around development ceilings calibrated to preserve safe and just space for human existence (Luukkanen et al. 2021).

12.1.2 *Privacy and the Surveillance Innovation Curve*

Imagined policy landscapes also do important work shaping policy outcomes in debates about surveillance and privacy. Most often, that landscape is dominated by a close relative of the economist's upward-trending growth curve, which models data-driven "innovation" versus social welfare. Like the upward-trending growth curve in economics, the upward-trending surveillance innovation curve suggests that, generally speaking, new ventures in data collection and processing will increase social welfare – and, conversely, that continuing increases in social welfare demand continuing growth in data harvesting and data processing capacities (e.g. Thierer 2014).

Imagined policy landscapes dominated by the upward-trending surveillance innovation curve have proved deeply inhospitable to efforts to rehabilitate privacy as an important social value. Richly textured accounts of privacy's importance abound in the privacy literature. Some scholars (e.g. Cohen 2012, 2013; Richards 2021; Roessler 2005; Steeves 2009) focus on articulating privacy's normative values; others (e.g. Nissenbaum 2009) on defining norms of appropriate flow; and others (e.g. Post 1989; Solove 2008) on mapping privacy's embeddedness within a variety of social and cultural practices. But the imagined policy landscape generated by the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

upward-trending surveillance innovation curve locates "innovation" and its hypothesized ability to solve a wide variety of economic and social problems solidly at centre stage.

As in the case of sustainable development, the doughnut model is an effective visual device for directing attention toward the negative effects of excess surveillance and, therefore, toward the difficult but necessary task of specifying surveillance ceilings. Additionally, theoretical accounts of privacy directed primarily toward rehabilitating it as a value worth preserving typically do not offer enough guidance on how to identify necessary surveillance floors. Claims about appropriate versus inappropriate flow (Nissenbaum 2009) tend to be most open to contestation at times of rapid sociotechnical change, when norms of contextual integrity are unsettled. My own account of post-liberal privacy as an inherently interstitial and structural construct devotes some attention to the technical and operational requirements for implementing privacy safeguards (Cohen 2012, 2013, 2019b) but does not consider how to distinguish between pro-social and anti-social surveillance implementations. The doughnut model productively engages and frames questions about how to identify and manage both kinds of surveillance/privacy frontiers.

12.2 FROM MENTAL MAPS TO POLICY HORIZONS: MAPPING SURVEILLANCE/PRIVACY INTERFACES

The doughnut model for privacy policymaking defines two distinct "surfaces" over which balance needs to be achieved. The outer perimeter of the doughnut includes sectors representing different threats to safe and just human existence flowing from excesses of surveillance. Conversely, as in the case of the sustainability doughnut, the hole at the centre represents insufficient levels of data-driven surveillance – or privacy afforded to a degree that undermines the social foundation for human wellbeing.

12.2.1 *The Sustainability Ceiling: Antisocial Surveillance (and Prosocial Privacy)*

The growing and increasingly interconnected literatures in surveillance studies, information studies, and law have developed detailed accounts of the ways that excesses of surveillance undermine prospects for a safe and just human existence. Just as the outer perimeter of Raworth's (2017) doughnut is divided into sectors representing different kinds of planetary threats, so we can divide the privacy doughnut's outer perimeter into sectors representing the different kinds of threats to human wellbeing that scholars have identified. Because the literatures on these issues are extensive, I will summarize them only briefly.

Some sectors of the privacy doughnut's outer perimeter involve surveillance practices that undermine the capacity for self-development. Dominant platform

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

companies such as Google, Meta, Amazon, TikTok, and Twitter, and many other providers of networked applications and information services use browsing, reading, listening, and viewing data to impose pattern-driven personalization, tailoring the information environment for each user to what is already known about that user or inferred based on the behaviours and preferences of similar users. Pattern-driven personalization privileges habit and convenience over more open-ended processes of exploration, experimentation, and play (Cohen 2012, 2013; Richards 2021; Steeves 2009). It also facilitates the continual delivery of nudges designed to instill more predictable and more easily monetizable patterns of behavior (Zuboff 2019).

Other sectors involve surveillance practices that destabilize democratic institutions and practices. In particular, providers of online search and social media services use data about user behaviours and preferences to target and/or uprank flows of information, including both user-generated content and promoted content. Patterns of affinity-based information flow deepen political polarization, and this in turn affords more fertile ground for misinformation to take root and disinformation campaigns to flourish (e.g. Cohen 2019a; Nadler et al. 2018). The persistent optimization and re-optimization of online environments around commercial and narrowly tribal priorities and interests undermines trust in democratic institutions and erodes the collective capacity to define and advance more broadly public-regarding priorities and interests (Farrell and Schneier 2018; Viljoen 2021; see also Chapter 2, by Murakami Wood).

Other sectors involve surveillance practices that reinforce economic power and widen distributive gaps. Many employers use surveillance technologies to monitor employee behavior both in and, increasingly, outside workplaces (Ajunwa et al. 2017). Persistent work-related surveillance magnifies power disparities between employers and workers and raises the barriers to collective organization by workers that might mitigate those disparities (Rogers 2023). The same persistent surveillance of user behaviors and preferences that enables pattern-driven personalization of the information environment also facilitates personalization of prices and non-price terms for consumer goods and services, imposing hierarchical logics within consumer markets (e.g. Cohen 2019a; Fourcade and Healy 2017; Zuboff 2019).

Other sectors involve surveillance practices that compound pre-existing patterns of racialized and/or gendered inequality (e.g. Benjamin 2019; Citron 2022; Richardson and Kak 2022; see also Chapter 9, by Akbari). Scholars who focus on race, poverty, and their intersections show that privacy tends to be afforded differently to different groups, in ways that reinforced racialized abuses of power and that subjugate the poor while framing poverty's pathologies as failures of personal responsibility (Bridges 2017; Eubanks 2018; Gilliom 2001; Gilman 2012). Data extractive capitalism reinforces and widens these patterns and strengthens linkages between market-based and carceral processes of labeling and sorting (Benjamin 2019; Browne 2017; see also Chapter 5, by Lyon).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

Seen through a global prism, many extractive surveillance implementations reinforce pre-existing histories of colonialist exploitation and resource extraction (Couldry and Mejias 2019; see also Chapter 9, by Akbari). Recognition of the resulting threats to self-governance and self-determination has fueled a growing movement by scholars and activists in the Global South to assert control of the arc of technological development under the banner of a new "non-aligned technologies movement" (Couldry and Mejias 2023).

Last, but hardly least, the surveillance economy also imposes planetary costs. These include both chemical pollution caused by extraction of rare earth metals used in digital devices and air pollution, ozone depletion and other climate effects produced by immense data centres (Crawford 2021). These problems also link back to Raworth's (2017) original doughnut diagram; the surveillance economy is both socially and ecologically unsustainable.

12.2.2 *The Hole at the Centre: Prosocial Surveillance (and Antisocial Privacy)*

If the doughnut analogy is to hold, the hole at the doughnut's centre must represent too much privacy – privacy afforded to a degree that impedes human flourishing by undermining the social foundation for collective, sustainable governance. Diverse strands of scholarship in law and political theory have long argued that excesses of privacy can be socially destructive. The doughnut model reinforces some of those claims and suggests skepticism toward others. But the privacy doughnut's 'hole' also includes other, more specific surveillance deficits. I will develop this argument by way of two examples, one involving public health and the other involving the public fisc.

Liberal and feminist scholars have long argued that certain understandings of privacy reinforce conditions of political privation and patriarchal social control. The most well-known liberal critique of excess privacy is Hannah Arendt's (1958) description of the privation of a life lived only in home spaces segregated from the public life of the engaged citizen. Building on (and also critiquing) Arendt's account of privacy and privation, feminist privacy scholars (e.g. Allen 2003; Citron 2022; Roessler 2005) have explored the ways that invocations of privacy also function as a modality of patriarchal social control. It is useful to distinguish these arguments from those advanced by communitarian scholars about the ways that privacy undermines social wellbeing (e.g. Etzioni 2000). Theorists in the latter group have difficulty interrogating communally asserted power and identifying any residual domain for privacy. The communitarian mode of theorizing about privacy therefore tends to reinforce the imagined policy landscape generated by the upward-trending surveillance innovation curve. In different ways and to different extents, liberal and feminist critiques of excess privacy are concerned with the nature of the balance struck between "public" and "private" spheres of authority

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

and with the ways in which excesses of privacy can impede full inclusion in civil society and reinforce maldistributions of power.

Moving beyond these important but fairly general objections, excess privacy can also impede human flourishing in more context-specific ways. Here are two examples:

The events of the past years have illustrated that competent and humane public health surveillance is essential for human flourishing even when it overrides privacy claims that might warrant dispositive weight in other contexts (Rozenshtein 2021; see also Chapter 5, by Lyon). A competent system of public health surveillance needs to detect and trace the spread of both infections and viral mutations quickly and capably (Grubaugh et al. 2021). A humane system of public health surveillance must identify and care for those who are sick or subject to preventive quarantine. At the same time, however, such a system must safeguard collected personal information so it cannot be repurposed in ways that undermine public trust, and it must take special care to protect vulnerable populations (Hendl et al. 2020). Competent and humane public health surveillance therefore necessitates both authority to collect and share information and clearly delineated limits on information collection and flow.

Some public health surveillance operations clearly cross the doughnut's outer perimeter. From the Western legal perspective, obvious candidates might include the Chinese regime of mandatory punitive lockdowns (e.g., Chang et al. 2022) and (at one point) testing via anal swabs (Wang et al. 2021). But having avoided these particular implementations does not automatically make a system of public health surveillance competent and humane. In the United States and the United Kingdom, for example, information collected for pandemic-related public health care functions has flowed in relatively unconstrained ways to contractors deeply embedded in systems of law enforcement and immigration surveillance, fueling public distrust and fear (No Tech for Tyrants and Privacy International 2020).

Particularly in the current neoliberal climate, however, it has been less widely acknowledged that other kinds of public health surveillance interventions fail the threshold-conditions criterion. The US regime of public health surveillance during the coronavirus pandemic operated mostly inside the doughnut's hole, relying on patchy, haphazard, and often privatized networks of protocols for testing and tracing backstopped by an equally patchy, haphazard, and often privatized network of other protective and social support measures (Jackson and Ahmed 2022). Some nations, meanwhile, constructed systems of public health surveillance designed to operate within the doughnut. One example is the Danish regime combining free public testing and centralized contact tracing with a public passport system designed to encourage vaccination and facilitate resumption of public and communal social life (Anderssen et al. 2021; see also Ada Lovelace Institute 2020). Additionally, although a responsible and prosocial system of public health surveillance must

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

balance the importance of bodily control claims in ways that respect individual dignity, it should not permit overbroad privacy claims to stymie legitimate and necessary public health efforts (Rozenshtein 2021). Refusal to participate in testing and tracing operations, to comply with humanely designed isolation and masking protocols, and to enroll in regimens for vaccination and related status reporting can fatally undermine efforts to restore the threshold conditions necessary for human flourishing – that is, to return society more generally to the zone of democratic sustainability defined by the doughnut.

As a second example of necessary, public-regarding surveillance, consider mechanisms for financial surveillance. The legal and policy debates surrounding financial and communications surveillance arguably present a puzzle. If, as any competent US-trained lawyer would tell you, speech and money are sometimes (always?) interchangeable, we ought to be as concerned about rules allowing government investigators access to people's bank statements as we are about rules allowing the same investigators access to people's communication records. Yet far more public and scholarly attention attaches to the latter. In part, this is because the financial surveillance rules are complex and arcane and the entities that wield them are obscure. In part, however, it is because it is far more widely acknowledged that systemic financial oversight – including some financial surveillance – implicates undeniably prosocial goals.

Financial surveillance authority underpins the ability to enforce tax liabilities without which important public services necessary for human wellbeing could not be provided (Swire 1999). Such services include everything from roads, clean water, and sewage removal to public education, housing assistance, and more. By this I don't mean to endorse current mechanisms for providing such assistance or the narratives that surround them, but only to claim that such services need to be provided and need to be funded.

Relatedly, financial surveillance authority enables investigation of complex financial crimes, including not only the usual poster children in contemporary securitized debates about surveillance (organized crime, narcotrafficking, and global terrorism) (Swire 1999), but also and equally importantly the kleptocratic escapades of governing elites and oligarchies. A wide and growing assortment of recent scandals – involving everything from assets offshored in tax havens (ICIJ 2021) to diverted pandemic aid (AFREF et al. 2021; Podkul 2021) to real estate and other assets maintained in capitalist playgrounds by oligarchs and the uber-rich (Kendzior 2020; Kumar and de Bel 2021) – underscore the extent to which gaps in financial oversight systems threaten social wellbeing. Effective, transnational financial surveillance is an essential piece (though only one piece) of an effective response.

The inability to perform any of these financial surveillance functions would jeopardize the minimum requisite conditions for human flourishing. And, to be clear, this argument does not depend on the continued existence of nation states in their current form and with their current geopolitical and colonial legacies.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

If current nation states ceased to exist tomorrow, other entities would need to provide, for example, roads, clean water, and sewage removal, and other entities would need to develop the capacity to support and protect the least powerful.[2]

12.3 INSIDE THE DOUGHNUT:ABOLITION V./OR/AND GOVERNANCE

To (over)simplify a bit, so far, I may seem to have argued that one can have too much surveillance or not enough. Broadly speaking, that is a familiar problem within the privacy literature, so at this point it may appear that I have not said that much after all. And equally important, I have not specifically addressed the characteristic orientations and effects of surveillance models in our particular, late capitalist, insistently racialized society. In practice, surveillance implementations have tended to entrench and intensify extractive, colonialist, and racialized pathologies (Benjamin 2019; Browne 2017; Couldry and Mejias 2023; see also Chapter 9, by Akbari), and awareness of that dynamic now underwrites a rapidly growing movement for surveillance abolition whose claims lie in tension with some of my own claims about the doughnut's inner ring.

12.3.1 *An Existential Dilemma*

Surveillance abolition thinking rejects thinking about the possibility of reorienting surveillance technologies toward prosocial and equality-furthering goals as pernicious and wrongheaded. Although beneficial uses are hypothetically possible, the track record of abuse is established and far more compelling. There is no 'right kind' of surveillance because all kinds of surveillance – including those framed as luxuries for the well-to-do – will invariably present a very different face to the least fortunate (Gilliard 2020, 2022). Drawing an explicit parallel to the campaign for abolition of policing more generally (e.g. McLeod 2019; Morgan 2022), surveillance abolition thinking calls upon its practitioners to imagine and work to create a world in which control over data and its uses is radically reimagined (Milner and Traub 2021). Abolitionist thinkers and activists tend to view proposals for incremental and/or procedural privacy reforms as working only to entrench surveillance-oriented practices and their disparate impacts more solidly.

As one example of the case for surveillance abolition, consider evolving uses of biometric technologies. Facial recognition technology has been developed and tested with brutal disregard for its differential impacts on different skin tones and genders (Buolamwini and Gebru 2018) and deployed for a wide and growing variety of extractive and carceral purposes (Garvie et al. 2016; Hill 2020). At the same time, it has been normalized as a mechanism for casual, everyday authentication of access to

[2] The implications of these arguments for current experiments in cryptocurrency-based disintermediation of fiat currency are evident but beyond the scope of this paper.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

consumer devices in a manner that creates profound data security threats (Rowe 2020). India's Aadhaar system of biometric authentication, which relies on digitalized fingerprinting, was justified as a public welfare measure, but works least well for the least fortunate – for example, manual laborers whose fingerprints may have been worn away or damaged (Singh and Jackson 2017). At the same time, the privatization of the "India stack" has created a point of entry for various commercial and extractive ventures (Hicks 2020).

As a second example of the case for surveillance abolition, consider credit scoring. In the United States, there are deep historical links between credit reporting and racial discrimination (Hoffman 2021), and that relationship extends solidly into the present, creating self-reinforcing circuits that operate to prevent access to a wide variety of basic needs, including housing (Leiwant 2022; Poon 2009; Smith and Vogell 2022) and employment (Traub 2014). In municipal and state systems nationwide, unpaid fines for low-level offenses routinely become justifications for arrest and imprisonment, creating new data streams that feed back into the credit reporting system (Bannon et al. 2010).

The other half of the existential dilemma to which this section's title refers, however, is that governing complex societies requires techniques for governing at scale. Some functions of good governance relate to due process in enforcement. I do not mean this to refer to policing but rather and more generally to the ability to afford process and redress to those harmed by private or government actors. For some time now, atomistic paradigms of procedural due process have been buckling under the strain of large numbers. The data protection notion of a "human in the loop" is no panacea for the defects embedded in current pattern-driven processes (e.g. Crootof et al. 2023; Green 2022), but, even if it were, it simply isn't possible to afford every type of complaint that a human being might lodge within a bureaucratic system the type of process to which we might aspire.

Other functions of good governance are ameliorative. Governments can and do (and must) provide a variety of important public benefits, and surveillance implementations intersect with these in at least three ways. First, surveillance can be used (and misused) to address problems of inclusion. Failure to afford inclusion creates what Gilman and Green (2018) term "surveillance gaps" in welfare and public health systems. Second, distributing government benefits without some method of accounting for them invites fraud – not by needy beneficiaries too often demonized in narratives about responsibility and advantage-taking, but rather by powerful actors and garden-variety scammers seeking to enrich themselves at the public's expense (AFREF et al. 2021; Podkul 2021). Third, mechanisms for levying and collecting tax revenues to fund public benefits and other public works invite evasion by wealthy and well-connected individuals and organizations (Global Alliance for Tax Justice 2021; Guyton et al. 2021; ICIJ 2021). In a world of large numbers, the possibilities for scams multiply. Surveillance has a useful role to play in combating fraud and tax evasion. For example, the Internal Revenue Service, which is chronically under-

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

resourced, spends an outsize portion of the enforcement resources that it does have pursuing (real or hypothesized) tax cheats at the lower end of the socioeconomic scale (Kiel 2019), but training artificial intelligence for fraud detection at the upper end of that scale, where tax evasion is also more highly concentrated (Alstadsaeter et al. 2019), could produce real public benefit.

In short, a basic function of good government is to prevent the powerful from taking advantage of the powerless, and this requires rethinking both what constitutes legitimate surveillance and what constitutes legitimate governance. Current surveillance dysfunctions and injustices suggest powerfully that the root problem to be confronted involves re-learning how to govern, and for whose benefit, before re-learning how to surveil.

The doughnut model is not a cure-all for pathologies of exclusion and exploitation that have deep historical roots, but it does more than simply position privacy problems as matters of degree. It suggests, critically, that one can have too much of the wrong kind of surveillance, and/or not enough of the right kind, and that "wrong" and "right" relate to power and its abuses in ways that have very specific valences. We may make some headway simply by asking more precise questions about the types of surveillance that a just society *must* employ or *should never* permit. But not enough. Surveillance implementations are always already situated relative to particular contexts in which power and resources are distributed unequally and, unless very good care is taken, they will tend to reinforce and widen pre-existing patterns of privilege and disempowerment. Even for processes that (are claimed to) occur within the doughnut's interior, the details matter.

12.3.2 *Policymaking inside the Doughnut:Five Legitimacy Constraints*

Engaging the abolitionist critique together with the need to govern at scale suggests (at least) five additional constraints that ostensibly prosocial surveillance implementations must satisfy. The first two constraints, *sectoral fidelity* and *data parsimony*, are necessary to counteract surveillance mission creep. Policymakers must ask more precise questions about the particular sustainability function to which a proposed implementation relates and must insist on regimes that advance that function and no others. And the formal commitment to sectoral fidelity must be supported by a mandate for parsimonious design that, wherever possible and to the greatest extent possible, prevents collected data from migrating into new surveillance implementations. The third constraint is *distributive justice*. Policymakers must interrogate existing and proposed surveillance implementations through an equity lens and, as necessary, abandon or radically modify those that reinforce or increase pre-existing inequities. The fourth and fifth constraints, *openness to revision* and *design for countervailing* power, work against epistemic closure of narratives embraced to justify surveillance in the first place. Policymakers should create oversight mechanisms that facilitate revisiting and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

revising policies and practices and should require design for countervailing power in ways that reinforce such mechanisms.

One of privacy law's most difficult challenges has involved building in appropriate leeway for evolution in data collection and use while still minimizing the risk of surveillance mission creep. The data minimization and purpose limitation principles that underpin European-style data protection regimes represent one articulation of this challenge, but those principles date back to the era of standalone databases and present interpretive difficulties in an era of interconnected, dynamic information systems. Their touchstones – respectively, collection that is "limited to what is necessary in relation to" the stated purpose and further processing that is "compatible" with the original stated purpose[3] – seem to invite continual erosion. In particular, they have been continually undermined by prevailing design practices that create repositories of data seemingly begging to be repurposed for new uses. Nissenbaum's (2009) theory of privacy as contextual integrity represents an attempt to situate the construct of purpose limitation within a more dynamic frame; sometimes, changes in data flow threaten important moral values, but not always. Exactly for that reason, however, the theory of contextual integrity does not adequately safeguard the public against moral hazard and self-dealing by those who implement and benefit from surveillance systems.

Together, the constraints of sectoral fidelity and data parsimony offer a more reliable pathway to maintaining prosocial surveillance implementations while resisting certain predictable and predictably harmful forms of mission creep. To begin, a sectoral fidelity constraint enshrined in law (and reaffirmed with adequate and effective public oversight) would represent a much stronger public commitment to limiting surveillance in the interest of social sustainability. So, for example, such a constraint would allow reuse of data collected for public health purposes for new or evolving public health purposes, but it would forbid mission creep from one sector to another – for example, from health to security – even when data are repurposed for a security-related use that otherwise would fall inside the doughnut. Instances of mission creep in which data collected for public health purposes flow out the back door to be used for national security purposes jeopardize the public trust on which public health surveillance needs to rely. Systems of national security surveillance are necessary in complex societies, but they require separate justification and separate forms of process.

Absent reinforcement by a corresponding design constraint, however, a commitment to sectoral fidelity that is expressed purely as a legal prohibition, seems predestined to fail. Because surveillance implementations express, and cannot ever

[3] Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. (L 119) 1, art. 5(1)(b)–(c).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

fully avoid expressing, power differentials, they inevitably present temptations to abuse. Where surveillance is necessary for social sustainability, a requirement of design for data parsimony can work to limit mission creep in ways that legal restrictions alone cannot. So, for example, large-grain surveillance proxies that use hashed, locally stored data for credentialing and authentication might facilitate essential governance functions in privacy protective ways, ensuring access to public services and facilitating access to transit systems without persistent behavioural tracking.

Neither the sectoral fidelity principle nor the data parsimony principle, however, speaks directly to surveillance-based practices that have powerful differential impacts on privileged and unprivileged groups of people living in the digital age. A legitimacy constraint capable of counteracting the extractive drift of such systems needs to be framed in terms of equity and anti-subordination (cf. Viljoen 2021). Some kinds of scoring are inequitable because they entrench patterns of lesser-than treatment, and some kinds of goods ought to be distributed in ways that do not involve scoring at all. For example, as Foohey and Greene (2022) document, tweaks designed to make the consumer credit scoring system more accurate simply entrench its systemic role as a mechanism for perpetuating distributional inequity. Piecemeal prohibitions targeting particular types or uses of data are overwhelmingly likely to inspire workarounds that violate the spirit of the prohibitions and reinforce existing practices – for example, "ban the box" laws prohibiting inquiry about employment applicants' criminal records have engendered other profiling efforts that disparately burden young men of color (Strahilevitz 2008). Under such circumstances, the question for policymakers should be how to restrict both the nature and the overall extent of reliance on scoring and sorting as mechanisms for allocation and pricing. The background presumption of inherent rationality that has attached to credit scoring should give way to comprehensive oversight designed to restore and widen semantic gaps; mandate use of data-parsimonious certifications of eligibility; and encourage creation of alternative allocation mechanisms. Where state-driven surveillance implementations must be deployed to address problems of inclusion, equity should be understood as a non-negotiable first principle constraining every aspect of their design.

The fourth and fifth legitimacy constraints – openness to revision and design for countervailing power – follow from the principle of equity. Training surveillance implementations away from the path of least resistance – that is, away from policies and practices that reinforce historic patterns of injustice and inequity – demands institutional and technical design to resist epistemic closure. Too often, proposed regulatory oversight models for surveillance implementations amount to little more than minor tweaks that, implicitly, take the general contours of those implementations as givens. That sort of epistemic closure is both unwarranted (because it cedes the opportunity to contest the validity of data-driven decisions) and self-defeating (because it disables public-regarding governance from achieving (what ought to be)

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

its purposes). More specifically, since failure modes for surveillance are likely to have data-extractive, racialized, and carceral orientations, accountability mechanisms directed toward rejection of epistemic closure need to be designed with those failure modes in mind.

Like strategies for avoiding surveillance mission creep, strategies for embedding a revisionist and equity-regarding ethic of public accountability within surveillance implementations are both legal and technological. On one hand, honoring the principle of openness to revision requires major reforms to legal regimes that privilege trade secrecy and expert capture of policy processes (Kapczynski 2022; Morten 2023). But surveillance power benefits from technical opacity as well as from secrecy (Burrell 2016), and merely rolling back legal protections for entities that create and operate surveillance implementations still risks naturalizing opaque practices of algorithmic manipulation that ought themselves to be open to question and challenge. An oversight regime designed to resist epistemic closure should mobilize technological capability to create countervailing power wherever surveillance implementations are used. As a relatively simple example, algorithmic processes (that also satisfy the other legitimacy constraints) might be designed to incorporate tamper-proof audit mechanisms designed to open their operation to public oversight. A more complicated example is Mireille Hildebrandt's (2019) proposal for agonistic machine learning – that is, machine learning processes that are designed to interrogate their own assumptions and test alternate scenarios.

12.4 CONCLUSION

The doughnut model for privacy suggests important questions about the appropriate boundaries between surveillance and privacy and about the forms and modalities of legitimate data-driven governance that should inform future research and prescriptive work. Living within the doughnut requires appropriate safeguards against forms of data-driven surveillance that cross the outer perimeter, and it also requires data-driven governance implementations necessary to attain the minimum requirements for human wellbeing. In particular, automated, data-driven processes have important roles to play in the governance of large, complex societies. Ensuring that any particular surveillance implementation remains within the space defined by the doughnut rather than drifting inexorably across the outer perimeter requires subjecting it to additional legitimacy constraints, of which I have offered five – sectoral fidelity, data parsimony, equity, openness to revision, and design for countervailing power. Strategies for bending the arc of surveillance toward the safe and just space for human wellbeing must include both legal and technical components – such as, for example, reliance on surveillance proxies such as credentialing and authentication to facilitate essential governance and allocation functions in data-parsimonious ways. Ultimately, governing complex societies in ways that are sustainable, democratically accountable, and appropriately respectful of human rights and human

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

dignity requires techniques that are appropriately cabined in their scope and ambition, equitable in their impacts, and subject to critical, iterative interrogation and revision by the publics whose futures they influence.

REFERENCES

Ada Lovelace Institute. "International Monitor: Vaccine Passports and COVID Status Apps." *Ada Lovelace Institute*. May 1, 2020. www.adalovelaceinstitute.org/project/international-monitor-vaccine-passports-covid-status-apps/.

Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. "Limitless Worker Surveillance." *California Law Review* 105 (2017): 735–776.

Allen, Anita. *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*. Lanham, MD: Rowman & Littlefield, 2003.

Alstadsaeter, Annette, Niels Johannesen, and Gabriel Zucman. "Tax Evasion and Inequality." *American Economic Review* 109, no. 6 (2019): 2073–2103.

Americans for Financial Reform, Anti-Corruption Data Collective and Public Citizen. "Report: Public Money for Private Equity: Pandemic Relief Went to Companies Backed by Private Equity Titans." *Americans for Financial Reform*, September 15, 2021. https://ourfinancialsecurity.org/2021/09/report-public-money-for-private-equity-cares-act.

Anderssen, Pernille Tangaard, Natasa Loncarevic, Maria B. Damgaard, Mette W. Jacobsen, Farida Bassioni-Stamenic, and Leena E. Karlsson. "Public Health, Surveillance Policies and Actions to Prevent Community Spread of COVID-19 in Denmark, Serbia, and Sweden." *Scandinavian Journal of Public Health* 50, no. 6 (2021): 711–729. https://doi.org/10.1177%2F1403494821056215.

Arendt, Hannah. *The Human Condition*. Chicago: University of Chicago Press, 1958.

Bannon, Alicia, Mitali Nagrecha, and Rebekah Diller. *Criminal Justice Debt: A Barrier to Reentry*. New York: Brennan Center for Justice at New York University School of Law, 2010.

Benjamin, Ruha. *Race after Technology: Abolitionist Tools for the New Jim Code*. New York: Polity Press, 2019.

Bridges, Khiara. *The Poverty of Privacy Rights*. Redwood City, CA: Stanford University Press, 2017.

Browne, Simone. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press, 2017.

Buolamwini, Joy, and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research* 81 (2018): 1–15.

Burrell, Jenna. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." *Big Data & Society* 3, no. 1 (2016): 1–12.

Chang, Agnes, Amy Qin, Isabelle Qian, and Amy C. Chien. "Under Lockdown in China." *The New York Times*, April 29, 2022. www.nytimes.com/interactive/2022/04/29/world/asia/shanghai-lockdown.html.

Citron, Danielle Keats. *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*. New York: W. W. Norton, 2022.

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

Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. New Haven, CT: Yale University Press, 2012.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

"Turning Privacy Inside Out." *Theoretical Inquiries in Law* 20, no. 1 (2019b): 1–21.
"What Privacy Is For." *Harvard Law Review* 126 (2013): 1904–1933.
Corvallec, Herve, Alison F. Stowell, and Nils Johansson. "Critiques of the Circular Economy." *Journal of Industrial Ecology* 26, no. 3 (2022): 421–432.
Couldry, Nick, and Ulises A. Mejias. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television & New Media* 20, no. 4 (2019): 336–349.
"The Decolonial Turn in Data and Technology Research: What Is at Stake and Where Is It Heading?" *Information, Communication & Society* 26, no. 3 (2023): 786–802.
Crawford, Kate. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven, CT: Yale University Press, 2021.
Crootof, Rebecca, Margot E. Kaminski, and W. Nicholson Price. "Humans in the Loop." *Vanderbilt Law Review* 76 (2023): 429–510.
Etzioni, Amitai. *The Limits of Privacy*. New York: Basic Books, 2000.
Eubanks, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: Macmillan, 2018.
Farrell, Henry, and Bruce Schneier. "Research Publication No. 2018-7: Common-Knowledge Attacks on Democracy." Berkman Klein Center for Internet & Society at Harvard University. November 17, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273111.
Foohey, Pamela, and Sara S. Greene. "Credit Scoring Duality." *Law and Contemporary Problems* 85, no. 3 (2022): 101–122.
Fourcade, Marian, and Kieran Healy. "Seeing Like a Market." *Socio-Economic Review* 15 (2017): 9–29.
Friant, Martin Callisto, Walter J. V. Vermeulen, and Roberta Salomone. "A Typology of Circular Economy Discourses: Navigating the Diverse Versions of a Contested Paradigm." *Resources, Conservation and Recycling* 161 (2020): 1–19.
Garvie, Clare, Alvaro Bedoya, and Jonathan Frankle. "The Perpetual Lineup: Unregulated Police Face Recognition in America." *Georgetown Center on Privacy & Technology*, 2016. www.perpetuallineup.org/.
Gilliard, Chris. "The Rise of 'Luxury Surveillance.'" *The Atlantic*, October 18, 2022. www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772/.
"The Two Faces of the Smart City." *Fast Company*, January 20, 2020. www.fastcompany.com/90453305/the-two-faces-of-the-smart-city.
Gilliom, John. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press, 2001.
Gilman, Michele E. "The Class Differential in Privacy Law." *Brooklyn Law Review* 77, no. 4 (2012): 1389–1445.
Gilman, Michele E., and Rebecca Green. "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization." *New York University Review of Law & Social Change* 42 (2018): 253–307.
Global Alliance for Tax Justice. "The State of Tax Justice 2021." *Tax Justice Network*. November 16, 2021. https://taxjustice.net/reports/the-state-of-tax-justice-2021/.
Green, Ben. "The Flaws of Policies Requiring Human Oversight of Government Algorithms." *Computer & Security Review* 45 (2022): 1–22. https://doi.org/10.1016/j.clsr.2022.105681.
Grubaugh, Nathan D., Emma B. Hodcroft, Joseph R. Fauver, Alexandra L. Phelan, and Muge Cevik. "Public Health Actions to Control New SARS-CoV-2 variants." *Cell* 184, no. 5 (2021): 1127–1132.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

Guyton, John, Patrick Langetieg, Daniel Reck, Max Risch, and Gabriel Zucman. "Tax Evasion at the Top of the Income Distribution: Theory and Evidence." *National Bureau of Economic Research*, December 2021. www.nber.org/papers/w28542.

Hendl, Tereza, Ryoa Chung, and Verina Wild. "Pandemic Surveillance and Racialized Subpopulations: Mitigating Vulnerabilities in COVID-19 Apps." *Journal of Bioethical Inquiry* 17 (2020): 928–934.

Hicks, Jacqueline. "Digital ID Capitalism: How Emerging Economies Are Reinventing Digital Capitalism." *Contemporary Politics* 26, no. 3 (2020): 330–350.

Hildebrandt, Mireille. "Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning." *Theoretical Inquiries in Law* 20, no. 1 (2019): 83–121.

Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *The New York Times*, January 18, 2020. www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hoffman, Tamar. "Debt and Policing: The Case to Abolish Credit Surveillance." *Georgetown Journal of Poverty Law and Policy* 29, no. 1 (2021): 93–119.

van Hulst, Merlijn, and Dvora Yanow. "From Policy 'Frames' to 'Framing': Theorizing a More Dynamic Approach." *American Review of Public Administration* 46, no. 1 (2016): 92–112.

International Consortium of Investigative Journalists (ICIJ). "Offshore Havens and Hidden Riches of World Leaders and Billionaires Exposed in Unprecedented Leak." *International Consortium of Investigative Journalists*, October 3, 2021. www.icij.org/investigations/pandora-papers/global-investigation-tax-havens-offshore/.

Jackson, Jason, and Aziza Ahmed. "The Public/Private Distinction in Public Health: The Case of COVID-19." *Fordham Law Review* 90, no. 6 (2022): 2541–2559.

Kapczynski, Amy. "The Public History of Trade Secrets." *U.C. Davis Law Review* 55 (2022): 1367–1443.

Kendzior, Sarah. *Hiding in Plain Sight: The Invention of Donald Trump and the Erosion of America*. New York: Flatiron Books, 2020.

Kiel, Paul. "It's Getting Worse: The IRS Now Audits Poor Americans at About the Same Rate as the Top 1%." *ProPublica*, 2019. www.propublica.org/article/irs-now-audits-poor-americans-at-about-the-same-rate-as-the-top-1-percent.

Kumar, Lakshmi, and Kaisa de Bel. "Acres of Money Laundering: Why US Real Estate Is a Kleptocrat's Dream." *Global Financial Integrity*, August 2021. https://gfintegrity.org/acres-of-money-laundering-2021/.

Leiwant, Matthew Harold. "Locked Out: How Algorithmic Tenant Screening Exacerbates the Housing Crisis in the United States." *Georgetown Law Technology Review* 6 (2022): 276–299.

Luukkanen, Jyrki, Jarmo Vehmas, and Jari Kaivo-oja. "Quantification of Doughnut Economy with the Sustainability Window Method: Analysis of Development in Thailand." *Sustainability* 13 (2021): 1–18. https://doi.org/10.3390/su13020847.

McLeod, Allegra. "Envisioning Abolition Democracy." *Harvard Law Review* 132 (2019): 1613–1649.

Milner, Yeshimabeit, and Amy Traub. *Data Capitalism + Algorithmic Racism*. Demos, 2021. www.demos.org/research/data-capitalism-and-algorithmic-racism.

Morgan, Jamelia. "Responding to Abolition Anxieties: A Roadmap for Legal Analysis." *Michigan Law Review* 120 (2022): 1199–1224.

Morten, Christopher J. "Publicizing Corporate Secrets." *University of Pennsylvania Law Review* 170 (2023): 1319–1404.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

Murakami Wood, David, ed. *A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network*. London: Mark Siddoway/Knowledge House, 2006. https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf.

Nadler, Anthony, Matthew Crain, and Joan Donovan. "Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech." *Data & Society*, October 17, 2018. https://datasociety.net/library/weaponizing-the-digital-influence-machine/.

Nissenbaum, Helen. *Privacy in Context*. Stanford: Stanford University Press, 2009.

No Tech for Tyrants and Privacy International. "All Roads Lead to Palantir: A Review of How the Data Analytics Company Has Embedded Itself Throughout the UK." *Privacy International*, October 29, 2020. https://privacyinternational.org/report/4271/all-roads-lead-palantir.

Podkul, Cezary. "How Unemployment Insurance Fraud Exploded during the Pandemic." *ProPublica*, 2021. www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic.

Poon, Martha. "From New Deal Institutions to Capital Markets: Commercial Consumer Risk Scores and the Making of Subprime Mortgage Finance." *Accounting, Organizations & Society* 34, no. 5 (2009): 654–674.

Post, Robert. "The Social Foundations of Privacy: Community and Self in the Common Law Tort." *California Law Review* 77 (1989): 957–1010.

Raworth, Kate. *Doughnut Economics: 7 Ways to Think Like a 21st Century Economist*. White River Junction, VT: Chelsea Green Publishing, 2017.

Richards, Neil. *Why Privacy Matters*. New York: Oxford University Press, 2021.

Richardson, Rashida, and Amba Kak. "Suspect Development Systems: Databasing Marginality and Enforcing Discipline." *University of Michigan Journal of Law Reform* 55, no. 4 (2022): 813–883.

Rogers, Brishen. *Rethinking the Future of Work: Law, Technology and Economic Citizenship*. Cambridge, MA: MIT Press, 2023.

Roessler, Beate. *The Value of Privacy*. Cambridge, MA: Polity Press, 2005.

Rowe, Elizabeth A. "Regulating Facial Recognition Technology in the Private Sector." *Stanford Technology Law Review* 24 (2020): 1–54.

Rozenshtein, Alan Z. "Digital Disease Surveillance." *American University Law Review* 70 (2021): 1511.

Singh, Ranjit, and Steven J. Jackson. "From Margins to Seams: Imbrication, Inclusion, and Torque in the Aadhaar Identification Project." In *Proceedings of the 2017 Conference on Human Factors in Computing Systems*, 4776–4824. New York: ACM, 2017. https://doi.org/10.1145/3025453.3025910.

Smith, Erin, and Heather Vogell. "How Your Shadow Credit Score Could Decide Whether You Get an Apartment." *ProPublica*, 2022. www.propublica.org/article/how-your-shadow-credit-score-could-decide-whether-you-get-an-apartment.

Solove, Daniel. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

Steeves, Valerie. "Reclaiming the Social Value of Privacy." In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock, 191–208. New York: Oxford University Press, 2009.

Strahilevitz, Lior J. "Privacy Versus Antidiscrimination." *University of Chicago Law Review* 75, no. 1 (2008): 363–381.

Swire, Peter P. "Financial Privacy and the Theory of High-Tech Government Surveillance." *Washington University Law Quarterly* 77 (1999): 461–512.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

Thierer, Adam. *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Arlington County, VA: Mercatus Center at George Mason University, 2014.

Traub, Amy. *Discredited: How Employment Credit Checks Keep Qualified Workers out of a Job*. Demos, 2014. www.demos.org/research/discredited-how-employment-credit-checks-keep-qualified-workers-out-job.

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

Wang, Yuliang, Xiaobo Chen, Feng Wang, Jie Geng, Bingxu Liu, and Feng Han. "Value of Anal Swabs for SARS-COV-2 Detection: A Literature Review." *International Journal of Medical Sciences* 18 (2021): 2389–2393.

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

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 17 Nov 2026 at 00:21:30, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009383851.015