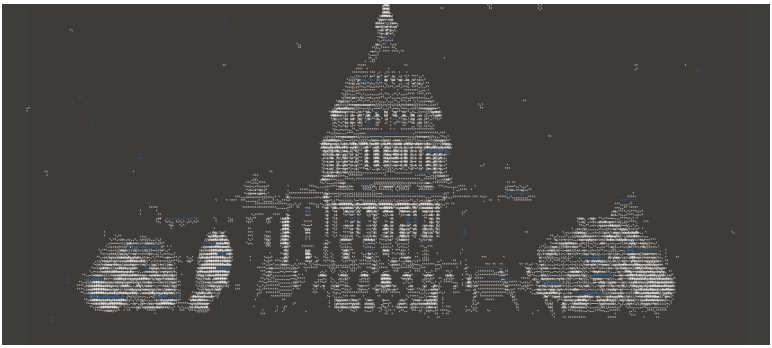
DATA AND DEMOCRACY



How (Not) to Write a Privacy Law

By Julie E. Cohen

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

In October 2020, the Knight First Amendment Institute at Columbia University convened a virtual symposium, titled "Data and Democracy," to investigate how technological advances relating to the collection, analysis, and manipulation of data are affecting democratic processes, and how the law must adapt to ensure the conditions for self-government. This symposium was organized by the Institute's 2019-2020 Senior Visiting Research Scholar, Yale Law Professor Amy Kapczynski, and co-sponsored by the Law and Political Economy Project at Yale Law School.

The essays in this series were originally presented and discussed at this two-day event. Written by scholars and experts in law, computer science, information studies, political science, and other disciplines, the essays focus on three areas that are both central to democratic governance and directly affected by advancing technologies and ever-increasing data collection: 1) public opinion formation and access to information; 2) the formation and exercise of public power; and 3) the political economy of data.

The symposium was conceptualized by Knight Institute staff, including Jameel Jaffer, Executive Director; Katy Glenn Bass, Research Director; Amy Kapczynski, Senior Visiting Research Scholar; Alex Abdo, Litigation Director; and Larry Siems, Chief of Staff. The essay series was edited by Glenn Bass with additional support from Lorraine Kenny, Communications Director; A. Adam Glenn, Writer/Editor; and Madeline Wood, Communications and Research Coordinator.

The full series is available at knightcolumbia.org/research/

INTRODUCTION

AFTER MANY YEARS OF FAILED STARTS, proposed information privacy legislation has begun moving forward in both houses of Congress. The docket in the recently ended 116th Congress was crowded, with a number of different proposals jostling for attention and no agreement on which deserved to be the front runner. Even so, as the 117th Congress begins, there is growing inside-the-Beltway consensus on the list of features that a successful bill will need to include. This paper critically assesses those zones of emerging consensus.

Many of the shared features of proposed privacy legislation embody fundamentally backward-looking approaches that cannot hope to constrain the activities they attempt to address. To varying extents but across the board, the current crop of proposals reflects what behavioral psychologist Abraham Maslow identified as the tendency to conform tasks to preexisting tools rather than vice versa.[1] Encapsulated in the saying that "if all you have is a hammer, everything looks like a nail," Maslow's insight is not really about hammers or nails but rather about the way human beings conceptualize approaches to new problems, and it contains an important lesson for would-be privacy reformers. The rote, brute-force application of laws

designed around the governance challenges of a prior era will not resolve the governance dilemmas created by today's surveillance-based business models. But all is not lost; the key lies in recognizing that governance too can be a site of innovation.

Part I discusses the zone of emerging consensus surrounding the definition and assertion of individual information privacy rights. Current approaches to crafting privacy legislation are heavily influenced by the antiquated private law ideal of bottom-up governance via assertion of individual rights, and that approach, in turn, systematically undermines prospects for effective governance of networked processes that operate at scale. Part II turns to the question of public governance. Many of the proposed bills designate public governance structures, but they also import antiquated public law mechanisms that operate without due regard for the topography of networked, data-driven processes. Effective privacy governance requires a model organized around problems of design, networked flow, and scale. I identify some essential components of such a model and a few more specific strategies for lawmakers and regulators to consider. Part III evaluates proposals for enforcement of newly recognized rights and obligations. Here there is less unanimity—some propose to create private rights of action while others would authorize only public enforcement litigation—but all parties seem to agree on the menu of choices, and none of those choices promises efficacy. The debate about private versus public enforcement litigation has been an unproductive distraction from the task of crafting more effective public enforcement mechanisms, of which I identify three.

RIGHTS-BASED GOVERNANCE: LEGISLATING IN THE SHADOW OF THE CATHEDRAL

Both existing information privacy laws and the recent crop of legislative proposals are pervasively informed by a governance paradigm that is deeply embedded in the U.S. legal tradition and that relies on individual assertion of rights to achieve social goals. To be clear, none of the bills recently before Congress purports, in so many words, to recognize *property* rights in personal data. Even so, almost all adopt a

basic structure that is indebted to property thinking. Within that structure, individual control rights function as the primary mechanism for governing the collection and processing of personal data, with no or only residual provision for ongoing governance at the collective level. Atomistic, post hoc assertions of individual control rights, however, cannot meaningfully discipline networked processes that operate at scale. Nor can they reshape earlier decisions about the design of algorithms and user interfaces.

Most of the bills introduced in the 116th Congress begin by assigning sets of control rights to consumers. Consumers may then consent to collection and processing, effectively waiving their purported control rights. Some proposals would require consumers to opt in to data collection and processing, as in the case of the Online Privacy Act of 2019, sponsored by Rep. Anna Eshoo (D-CA), and the Privacy Bill of Rights Act, sponsored by Sen. Edward Markey (D-MA).[2] One such bill, Sen. Maria Cantwell's (D-WA) Consumer Online Privacy Rights Act, additionally defines more general duties that covered information processing entities owe to consumers and permits consumers to sue when they believe those duties have been violated.[3] Others would require consumers to opt out of data collection and processing, as in the case of the Mind Your Own Business Act of 2019, sponsored by Sen. Ron Wyden (D-OR), and the Balancing the Rights of Web Surfers Equally and Responsibly Act of 2019, sponsored by Sen. Marsha Blackburn (R-TN).[4]

The precise mechanisms for opting in or out vary—some bills specify detailed mechanisms while others would require agency rulemaking—but everyone seems to agree that such mechanisms are important. The two laws repeatedly held up as models for a new wave of stricter privacy protection at the state level, the Illinois Biometric Information Privacy Act (BIPA) and the California Consumer Protection Act (CCPA), also adopt a control-rights-plus-opt-in-or-out approach, with BIPA adopting opt-in requirements for biometric data and CCPA establishing an opt-out mechanism for personal data more generally.[5]

The continuing optimism about consent-based approaches to privacy governance is mystifying, because the deficiencies of such approaches are well known and relatively intractable. Many of the bills do attempt to impose new procedural requirements, and some, such as Sen. Wyden's Mind Your Own Business Act and the Do Not Track Act of 2019, sponsored by Sen.

Josh Hawley (R-MO), would empower regulators to create a system that records consumers' expressed preferences.[6] For reasons ably explained by many talented privacy scholars and advocates, however, such provisions are unlikely to result in real control in any meaningful sense. In brief: The issues that users must navigate to understand the significance of consent are too complex and the conditions surrounding consent too easy to manipulate.[7] Most formulations of user control rights don't clearly include information derived from user behavior, thereby opening the way for gamesmanship by tech firms around the synthetic data that lie at the core of advertising-based business models.[8] Additionally, it's not clear what the right to revoke consent means in the context of machine-learning-based models trained on a large corpus that includes the to-be-withdrawn data.[9]

The problem I want to highlight here concerns the *aggregate* efficacy of such consent mechanisms: Organizing a regulatory regime around individual control rights imports a governance structure that is atomistic and post hoc. Individual users asserting preferences over predefined options on modular dashboards have neither the authority nor the ability to alter the invisible, predesigned webs of technical and economic arrangements under which their data travels among multiple parties. Nor can they prevent participants in those webs from drawing inferences about them—even when the inferences substitute for the very same data that they have opted out of having collected.

The assumption that bottom-up governance driven by self-interested rights assertion will actually work derives from long-held, nearly automatic ways of thinking about property rights as mechanisms for collective ordering. The property tradition holds that property rights internalize governance incentives and minimize governance costs by situating authority over resource access and use where it can be exercised most wisely and effectively.[10] Contemporary property thinkers do recognize that such an approach can undervalue certain types of collective harms. Even so, they argue that because collective governance is costly, property rights should be the default arrangement in most situations, and if rights to access and use a resource need to be transferred or aggregated, property owners can negotiate the arrangement that they all prefer. Within this way of thinking about the relationship between individual control and governance, externally

imposed regulatory requirements are the exception—and this is a feature, not a bug.[11] By analogy, one might think that individual control rights (and presumed self-regulatory incentives flowing from assertion of those rights) offer the most effective and appropriate way of channeling data collection and processing activities to achieve other regulatory goals. And, to be fair, reliance on disaggregated, bottom-up governance flowing from assertion of individual control rights makes some sense in one-on-one negotiations over such matters as the conditions of access to real property or consent to medical treatment. But such reliance has also failed repeatedly and spectacularly as a mechanism for ensuring effective governance of collective interests in land use and in medical research ethics.[12] It makes no sense whatsoever where networked, large-scale processes are involved.

It's worth noting, moreover, that property thinking extends beyond the rights that the proposed privacy bills purport to define, shaping important underlying exceptions in ways that frustrate the accountability the bills profess to guarantee. In many legal systems—most notably, those in European Union member states—disclosure of personal information for law enforcement or national security purposes doesn't eliminate the need to comply with data protection obligations, although it does change their form and content. Under the U.S. approach, law enforcement and national security exceptions tend to move the activity beyond the reach of data protection obligations altogether. So, for example, in Fourth Amendment jurisprudence, courts generally understand themselves to be navigating a universe of control rights that is divided into two parts. Data acquisition may be subject to heightened procedural requirements, but once data has been lawfully acquired, it passes into government control.[13] Statutes governing information collection beyond the Fourth Amendment's reach tend to follow the same pattern, saying little about what happens to data once it has been properly acquired.[14] National security legislation has become a partial exception to this rule, incorporating concepts like minimization that are familiar to data protection lawyers.[15] Yet the veil of secrecy surrounding national security data practices also frustrates the capacity for collective governance and precludes the post hoc forms of accountability to individual citizens that, for example, European human rights courts have required.[16] None of the privacy bills proposed in the 116th Congress addresses accountability for government data practices. (None,

therefore, would cure the defects identified by the European Court of Justice in invalidating the EU-U.S. Privacy Shield agreement, which was intended to enable transfer of European citizens' data to the U.S. for processing in the context of commercial activities.[17])

Some argue that user-governed data cooperatives might enable scaling consent for the era of data-driven, networked processes in a way that enables users to retake control of privacy dashboards and command adherence to their preferred sets of terms.[18] There are no extant examples of such arrangements, however, and confident predictions of their eventual emergence seem ill-informed for two reasons. First, to the extent that such arguments rely on theoretical work by economists on collective mechanisms for governing common resources, they tend to ignore important qualifications that affect the ability of common-governance arrangements to scale. Such arrangements are most effective in smaller, more homogeneous communities attempting to govern resources whose boundaries can be demarcated relatively clearly; they become less effective as the communities grow in size and heterogeneity and as the boundaries of the resource pool become less easy to control.[19] Second, power differentials within communities also shape the scaling-up process. So, for example, open-source licensing scaled relatively well during the two or so decades when the community of internet developers consisted primarily of hobbyists and research scientists, and much less well after conflicts with the interests of large, for-profit technology firms began to mature, and the Creative Commons licensing system never scaled to encompass the activities of large, for-profit content interests at all.[20]

To be clear, consent provisions do invite some kinds of collective entrepreneurship around governance of personal information flows; it just isn't the sort of entrepreneurship likely to produce greater control or greater privacy for individuals. Instead, reliance on consent as the principal governance mechanism for personal data has invited forms of entrepreneurship that follow the "contracting into liability rules" model used by collective rights organizations for managing intellectual property rights.[21] That model is well-suited for scaling up licensing processes over large numbers of low-value transactions. It produces a type of governance arrangement designed to operate at scale, but it does so—necessarily—by standardizing the options presented to users in ways that interpose additional barriers to meaningful

consent on a more granular level. So, for example, because European data protection laws require affirmative consent from individuals for many kinds of processing, smaller entities unable to internalize the resulting compliance costs have begun affiliating to offer "automated consent management panels" through which users can signal their choices to all of the member entities.[22] Within such arrangements, consent becomes a fig leaf deployed to achieve compliance with a regime that requires symbols of atomistic accountability. Users remain unable to demand or specify changes in the basic conditions of information processing or the design of networked services. Should the U.S. adopt consent requirements similar to those that now obtain in Europe, one imagines that industry adoption of automated consent management panels would quickly follow.

In short, both faith in the efficacy of disaggregated governance and hopes for the possibility of collective governance are best understood as reflecting backward-looking, conceptually entrenched commitments to private ordering rather than anything resembling evidence-based reasoning. Both arguments for bottom-up governance flowing from assertion of individual rights and arguments for commons-based cooperative governance of personal data collection and processing overlook the structural and temporal effects of *design* operating at *scale*. Effective governance of such activities requires public oversight—and, as we are about to see, it also requires new thinking about how to structure and conduct such oversight.

COVERAGE AND OVERSIGHT: MASLOW'S HAMMER STRIKES AGAIN … AND AGAIN AND AGAIN

ASSUMING LEGISLATION DRAFTED to prioritize effective governance rather than atomized, post hoc assertions of control rights, how should privacy governance work? To varying extents but across the board, the bills introduced in the 116th Congress exemplify Maslow's hammer in action. All lean heavily on the set of existing public governance tools in ways that drastically reduce the likelihood of effective intervention.

An initial choice concerns where to situate oversight authority. Most recent proposals would vest authority in the Federal Trade Commission (FTC) or, for proposals aimed at voter privacy, the Federal Election Commission (FEC). The choice of regulator is enormously consequential because it tends to bake in preexisting jurisdictional limitations that weren't designed with the networked information economy in mind. So, for example, the FTC lacks jurisdiction over common carrier functions of information businesses, which in turn means that any grant to the FTC effectively gives the Federal Communications Commission (FCC), which does have that jurisdiction, some power to limit the extent of the FTC's authority. Only some of the proposed bills would expressly transfer authority to oversee the personal data practices of common carriers to the FTC.[23] The FTC also has more limited rulemaking and enforcement powers than other independent agencies, for reasons that have always been political and that reflect ingrained reluctance to give consumer protection regulators authority to meddle with market activity, and it has very limited resources. Proposed bills that designate the FTC as privacy regulator without removing the preexisting limits should be understood as subscribing to those choices, whether or not their sponsors acknowledge it.[24] For its part, the FEC has authority only over "electioneering communications" and only in certain ways. Even if the relevant definitions were amended to treat digital advertising the same way as broadcast advertising, the most potent and toxic flows of data-driven, networked misinformation and disinformation would not qualify as electioneering communications.[25] Sponsors of bills confidently promising to counter election manipulation by bringing greater transparency to digital electioneering typically do not seem to understand this.

Even proposals to create wholly new privacy agencies, however, aren't immune to the temptations posed by Maslow's hammer. Consider two different, increasingly popular ways of framing delegations of regulatory authority:

The first approach appropriates and repurposes trust-based concepts first developed in fiduciary and corporate law. It exists in two principal strands, one arguing for articulation of duties of confidentiality, care, and loyalty that mirror fiduciary duties, and the other arguing more generally for obligations of trustworthiness.[26] Both arguments rest to varying extents on

analogies to other sorts of arrangements that have been thought to trigger fiduciary obligations. Because the practices that generate personal data for processing and targeted advertising are relational—users enter into long-term arrangements with many different providers of platform-based services—the idea of relationships extending throughout time and across different contexts might (in theory) support imposing obligations based on the idea that such relationships create heightened duties. One important critique of this approach points out that the concept of heightened duties has tended to scale poorly in the corporate context, where managerial self-interest and perceived short-term obligations to shareholders tend to prevent internalization of more public-regarding sensibilities.[27] One might, of course, seek to constrain self-interest and short-termism by specifying duties of care and loyalty clearly and precisely.[28]

But the problem of how to foster *trust* in networked digital economies is even more complicated than debates about the relevance of fiduciary analogies within corporate settings tend to assume. The mere fact of an ongoing service relationship signifies relatively little in an era when relationships have been redefined as mass-market products and are mediated by standardized interfaces designed for large-scale, networked interconnection.[29] In the era of relationship-as-mass-market-product, it is worth remembering that our legal and regulatory traditions surrounding product safety have evolved in ways that are different and more exacting. One might of course describe the web of obligations and standards that exists in the realm of product design using the language of trust; so, for example, when I sit in the desk chair in my office, I trust that it won't collapse. Yet I suspect most modern lawyers would understand that formulation as too general to be helpful. When accidents inevitably occur, it is far more useful to be able to speak concretely about such matters as material tolerances and manufacturing specifications—and to be able to invoke corresponding tort and regulatory frameworks—than it is to talk in airy generalities about the nature of my relationship to the chair manufacturer.

This point about the necessary relationship between *design* and regulatory oversight extends beyond the manufacture of consumer goods to a vast range of complex, information-intensive products and services that are, in fact, comprehensively regulated. We might posit that pharmaceutical companies should have duties of care, loyalty, and scientific integrity toward

those who ingest their drugs; that insurance companies should have duties of care, loyalty, and actuarial integrity toward their policyholders; and that banks should have duties of care, loyalty, and solvency toward their depositors. But traditions of public governance of all three groups of actors are sufficiently robust that most would understand such formulations as adding very little to debates about how those relationships-as-products ought to be governed.

A second approach to framing delegations of regulatory authority involves using ideas of *market domination* derived from antitrust law to structure oversight regimes. So, for example, some of the proposed bills include special disclosure and reporting mandates that would apply only to covered information businesses of a certain size.[30] Conceptually, such proposals map to—but also represent a partial retreat from—arguments for mandating breakups and reorganizations of the very largest tech giants. (Breakups and other antitrust interventions may also be on the table in the 117th Congress.[31]) But antitrust-based approaches do not align well with surveillance abuses. Antitrust law has long grappled with the question of how to reconcile intangible intellectual property rights with competition mandates; addressing market domination within networked information ecosystems requires confronting similar questions about the appropriate extent of control over networked data flows structured by technical and legal protocols.[32] In order for proposals targeting dominant actors to produce meaningful restructuring of surveillance-based business models, they would need to disrupt not only corporate ownership and control structures but also licensed flows of data. In particular, the software developer kits supplied to app developers by dominant platform providers embed data collection and transmission protocols in ways that developers themselves often do not understand.[33] Privacy legislation designed to disrupt dominance must speak clearly to the ways that data flows are designed, embedded, layered, concealed, and propagated via networks of relationships that include multiple actors. And antitrust interventions designed to extend data flows *outside* the licensing ecosystems of dominant entities will only make privacy problems worse if they are not paired with other, privacy-focused interventions.

More generally, the dysfunctions of the networked information economy reflect underlying problems of *networked flow* and *scale* that are distinct from existing patterns of market domination. Regulation of information-economy

phenomena confronts what Paul Ohm has characterized as an "order of magnitude problem": networked flows of information produce effects that manifest at scale.[34] Market domination plays an important role in that process, and the self-serving actions of dominant legal actors can exacerbate order of magnitude harms, but networked phenomena generate scalar effects even when a dominant legal entity is not present. Marginal actors in networked information ecosystems have become adept at leveraging both the services of dominant platforms and the underlying attributes of information networks that connect human populations. New and established media companies, disinformation farms, and extremist brokers of hate and ethnic supremacy all employ strategies for collecting, processing, and exploiting personal data, and those strategies rely on accumulated learning about how to optimize content for networked, social circulation across multiple platforms and applications.[35] To be effective at all, regimes for privacy governance need to target order of magnitude problems in ways that enable oversight and enforcement to scale up and out commensurately.

For some European observers, the cardinal sin of U.S. legislative proposals for privacy governance is their failure to implement a third approach: a suite of European-style *data protection* obligations that would apply to all entities regardless of their size or market position and that would map to data stewardship issues more straightforwardly and comprehensively than fiduciary principles do. In particular, data protection incorporates duties of minimization and purpose limitation that, some argue, would make a difference in the ways information-centric business models operate.[36] Policymakers in the U.S. have largely acquiesced in the narrative advanced by tech firms and their advocates that innovation requires broad leeway to repurpose collected data and so, unsurprisingly, most of the bills recently before Congress don't take the idea of purpose limitation seriously.[37]

A more fundamental problem with the data protection approach is that, to the extent that it relies on prudential obligations rather than on more concrete specifications for structural limits on data collection and use, it invites death by a thousand cuts. Data protection law was originally conceived as a suite of requirements for enabling information collection and transfer with appropriate safeguards for data subjects. And data protection in practice can reduce to an exercise in managerial box-checking.[38] The European General

Data Protection Regulation (GDPR) imposes a substantive duty of data protection by design and default, but it does not specify the sorts of design practices that such a duty might require. There is a hole at the center where substantive standards ought to be—and precisely for that reason, data protection regulators often rely on alleged disclosure violations as vehicles for their enforcement actions, reflexively reaching back for atomistic governance via user control rights as the path of least resistance.[39]

In short, while problems of trust and market domination each undeniably contribute to the dysfunctions that surveillance-based business models create, responding adequately to those dysfunctions requires moving beyond reactive conceptions of data protection toward a governance model organized around problems of design, networked flow, and scale, and framed in terms of concrete requirements that must be satisfied by firms collecting, processing, and exchanging personal information.

How, though, are regulators to develop and exercise the sort of authority that I have just described? Here Maslow's hammer makes a third appearance. Legislators framing delegations of regulatory authority tend to assume—in the face of mounting evidence to the contrary—that regulators will be able to pursue the goals they have defined using a preexisting tool set consisting largely of century-old techniques for economic regulation.

In legislative drafting, questions about regulatory tool sets tend to be afterthoughts. Legislators and their staff seem to understand the universe of available tools as a fixed and relatively static category. So, if one wants to gain regulatory traction on a new problem—or, conversely, if one wants to appear reformist while moving the needle only very slightly—one confers authority to make rules and bring enforcement actions, and then one waits to reap the predicted beneficial results. Many of the proposed bills follow this well-worn formula, ignoring that it has already broken down. Even informal rulemaking has proved wholly unsuited to the task of constraining networked, highly informationalized processes because both the processes and available learning about how to govern them evolve so quickly.[40] For its part, enforcement practice has largely devolved into standard-form consent decree practice, creating processes of legal endogeneity that simultaneously internalize and dilute substantive mandates.[41] Other parts of the regulatory landscape do offer more diverse suites of oversight tools—in particular,

contemporary approaches to financial regulation, which have themselves undergone rapid change over the last quarter century, suggest a variety of strategies that privacy regulators might appropriate and repurpose—but the need to operate within preexisting regulatory silos prevents beneficial experimentation with such tools.

Empowering a regulator to conduct *effective* privacy governance requires three kinds of disruption to business as usual so that regulatory innovation can proceed. First and most basically, effective privacy governance requires a suite of modern oversight authorities and staff with the ability to develop and execute them. Tools for privacy regulators might include design requirements borrowed in concept from consumer finance regulation; operating requirements for auditing, benchmarking, and stress testing borrowed in concept from bank regulation; monitoring requirements borrowed in concept from a range of regulatory fields; and more.[42] Equally important, it might include other types of tools developed in consultation with experts on matters ranging from dark patterns to algorithmic bias to network threat modeling.[43]

Second, implementing the new tools requires disruptions to entrenched patterns of privatized oversight that too often stand in for true public-private cooperation in regulatory matters. Across a wide and growing number of economic sectors, regulatory authorities have become more heavily reliant on third-party auditors, technology vendors, and other professional intermediaries to evaluate regulatory compliance.[44] As Margot Kaminski explains, the emerging system of "binary governance" of privacy reflects the same trends; as Ari Waldman shows, the result is a system of increasingly widespread but increasingly performative compliance.[45] Although third-party intermediaries may have valuable roles to play in scaling up governance mechanisms, regulatory design for the networked information era must also include mechanisms for rendering such intermediaries accountable to public regulatory authorities. Put another way, there is a difference between delegating authority to entities that are also self-interested actors and deputizing those actors to conduct oversight activities on the public's behalf.

Finally, a regime of privacy governance needs to impose *public* transparency obligations on both the actors in networked information ecosystems and the regulators who oversee their operations. To do so effectively, legislation and implementing regulation need to specify those obligations in ways that

anticipate the continuing gravitational pull of property thinking. A principal transparency tool used today, the Federal Freedom of Information Act, is riddled with exemptions that reinforce the de facto property logics that Part I described. Some shield national security and law enforcement operations from scrutiny, reinforcing the proposition that transfers of information into those domains effect a surrender of control. Others protect claimed trade secrets and more generally "confidential information" embodied in information-processing tools supplied by private contractors, reinforcing de facto rights to exclude that are understood to operate even against government users.[46] Emerging conventions for "binary governance" of personal data processing often repeat these errors, stopping short of requiring public-facing transparency about information-handling practices.[47] Honoring the public's right to know requires a less deferential approach to the secrecy claims that have become endemic in the networked information era.

Only two of the bills introduced in the 116th Congress—Rep. Eshoo's (D-CA) Online Privacy Act and the Data Protection Act sponsored by Sen. Kirsten Gillibrand (D-NY)—come anywhere near this approach to privacy governance, and both also have fatal flaws. The Eshoo bill would create an independent digital privacy agency and give it robust enforcement powers, but would orient the agency's rulemaking powers largely toward violations of a dramatically expanded array of individual control rights. The Gillibrand bill would create an independent data protection agency to oversee a range of "high-risk data practices," including both profiling and processing of biometric data and other sensitive data, but would limit the agency's rulemaking and enforcement powers by imposing conditions similar to those that currently constrain the FTC.[48] One bill that remained on the drawing board during the 116th Congress—Sen. Sherrod Brown's (D-OH) Data Accountability and Transparency Act—begins to reenvision public governance of personal data processing more thoroughly. It forbids certain operations using personal data, prohibits various forms of data-driven discrimination, and proposes an independent data protection agency with authority to enforce the prohibitions and to supervise the testing of automated decision systems.[49] Brown's DATA Act also retains a suite of control rights and includes language curtailing federal enforcement authority that is modeled on the FTC Act. Its more innovative provisions, however, could form the kernel of a viable privacy governance regime for the networked information era. They merit genuine and sustained consideration.

REMEDIES AND ENFORCEMENT: THE (FALSE) CHOICE BETWEEN BAD AND WORSE

A THIRD IMPORTANT AREA of emerging consensus about the structure of privacy legislation involves enforcement mechanisms. Notwithstanding deep disagreement about whether to authorize private rights of action for violations, all parties seem to be working from the same unquestioned assumptions about what the universe of enforcement mechanisms includes. According to the conventional wisdom, there are two principal strategies available for pursuing information privacy violations: private remedial litigation initiated by affected individuals and public enforcement action initiated by agencies.[50] Proposals to double down on one or both of those strategies tend to overlook the inconvenient truth that ex post, litigation-centered approaches have not proved especially effective at constraining Big Tech's excesses. They also tend to overlook or downplay other possibilities that might prove more effective because they are better tailored to the scaled-up risks and harms that networked information flows create.

To be clear, both private remedial litigation and agency enforcement proceedings can serve important expressive and normative functions. Public enforcement proceedings against those who flagrantly violate public mandates reassert the importance of the values those mandates express. In theory at least, affording adequate scope for such proceedings can demonstrate a public commitment to holding powerful, for-profit entities accountable to the citizens whose interests the laws were enacted to protect.[51] Affording individuals the ability to vindicate statutorily conferred rights in private litigation can also demonstrate such a commitment—at minimum, by compelling the defendant to provide an account of its actions. Additionally, depending on how they are structured, enforcement proceedings have the potential to validate important dignitary interests.[52]

At the same time, though, discussions about both the relative and absolute efficacy of litigation-centered enforcement mechanisms reflect magical thinking about litigation's upsides. In recent decades, sustained assaults on standing to sue and on class-action eligibility and scope have drastically narrowed the feasibility horizon for litigation asserting harm to individual interests.[53] Efforts to recognize new information privacy rights eligible for

vindication by private litigants largely pretend this is not the case. Public enforcement litigation, meanwhile, is chronically underfunded, and in recent decades, public agencies have largely acquiesced in the emergence of conventions for structuring consent decrees that delegate most oversight to private auditors and in-house compliance officers.[54]

Returning to the themes developed in Part I, the surprisingly unanimous faith in enforcement litigation—private or public—as a remedial lever reflects the cathedral's lingering shadow, in two complementary ways. First, because enforcement litigation is predominantly atomistic in its identification and valuation of harms, it cannot effectively discipline networked phenomena that produce widely distributed, collective harms manifesting at scale. The mismatch is most obvious for private remedial litigation, which takes individual injury as the proper frame of reference even when claims are aggregated using class-action devices or processed together using newer multidistrict litigation mechanisms.[55] Public enforcement, however, is scarcely better. Agency enforcement staff operating under significant resource constraints consider their targets carefully and select them for maximum impact, but an approach that singles out selected bad actors tends to validate the mainstream of current conduct rather than meaningfully shifting its center of gravity. To the extent that the prevailing approach identifies smaller actors outside the mainstream as enforcement targets, moreover, those actors simply have insufficient authority to catalyze upstream redesign of the networked processes, protocols, and interfaces within which they operate.

Second, enforcement litigation tends to express the same bottom-up approach to governance of resources that characterizes property thinking generally, and so it has little to say about *how* violations ought to be remedied. Recall that according to property thinking, forcing cost internalization incentivizes property owners to do the right thing while leaving them appropriate discretion as to which inward-facing governance mechanisms to implement. As a practical matter, though, such efforts do not reliably produce lasting behavioral change unless they are paired with more specific mandates. To the contrary, and especially when the challenged behavior is both highly profitable and relatively opaque to outside observers, it empowers violators to treat the costs of occasional enforcement actions as operating expenses. Taken cumulatively, the results of the FTC's privacy enforcement

proceedings—including even the widely publicized contempt order against Facebook following the Cambridge Analytica disclosures—are consistent with that pattern. Over the past two decades, tech industry reliance on surveillance-based business models has only grown more entrenched.[56]

The balance of this section briefly describes three mechanisms that might enable enforcement interventions to attain more lasting and far-reaching impact. There may be others; the point is not to develop an exclusive list but rather to challenge entrenched habits of thinking and encourage experimentation with strategies designed to target the design of networked processes, protocols, and interfaces and to scale up commensurately with the conduct at issue. Each of the suggestions described below has appeared in at least one proposed privacy bill, where it prompted inside-the-Beltway reactions ranging from derision to embarrassed silence. Not coincidentally, such proposals—paired with a more active approach to privacy governance along the lines described in Part II—likely represent the only realistic prospects for moving the needle on enforcement.

An essential strategy for scaling enforcement authority involves leveraging gatekeeper power to demand and guarantee adherence to the design, operational, and monitoring requirements that public oversight processes have defined. For information businesses that qualify as online service providers, that would entail near-complete reversal of prevailing thinking about the appropriate extent of responsibility for the acts of third parties. As Rory Van Loo demonstrates, however, from a regulatory perspective, that approach is an anomaly; in many other industries, deputizing intermediaries to enforce appropriate standards of corporate behavior is vital and accepted.[57] By analogy, it is entirely rational to suggest deputizing online intermediaries to discipline smaller actors operating within information ecosystems that they have created and that generate enormous profits. Moreover, the presence of intermediary-based regimes in other fields gives the lie to the well-rehearsed contention that such regimes necessarily collapse into "censorship." We have already seen some examples of how such a system might work. For example, it might prescribe standards for the data collection and exchange functions built into software developer kits, and it might set outer limits on optimization for networked, social spread of content via recommendation feeds.

To be fully effective, scaled-up enforcement authority must be paired with strategies for scaling up sanctions against violators. The difficulties associated with crafting such strategies are well known and extend far beyond privacy. The very largest technology companies, however, have shown by their repeated, passive-aggressive flouting of enforcement decrees both in the U.S. and elsewhere that they may be uniquely immune to the incentives thought to be afforded by monetary fines on a conventional scale. The contempt sanctions levied against Facebook following the Cambridge Analytica disclosures are a case in point—the $5 billion fine, although by far the largest the FTC had ever imposed, represented only a month's worth of earnings for the tech giant.[58] As Paul Ohm has proposed, violations that produce order of magnitude effects require a commensurate response.[59]

One often overlooked element of the public enforcement tool kit, with the potential to scale in a way rarely matched by ordinary civil fines, is disgorgement of the profits accruing from unlawful activity. The Supreme Court recently confirmed that federal courts have inherent equitable authority to order disgorgement even absent more specific authority.[60] And several existing agencies, including both the FTC and the Securities and Exchange Commission, have disgorgement authority in certain kinds of cases.[61] Only two of the privacy bills proposed in the 116th Congress prescribe a disgorgement remedy.[62] Current approaches to conceptualizing disgorgement, however, too often return reflexively to the atomistic and transactional approach to governance described in Part I. Activating either the inherent judicial disgorgement authority or existing agency disgorgement authority tends to require a standard of traceable economic injury that many complaints alleging information privacy harms cannot meet. To be most effective in the privacy context, disgorgement authority should be tied to violation of publicly defined design, operational, and monitoring requirements. Privacy legislation should clearly prescribe disgorgement as a remedy for such violations, and it should empower regulators to define—and justify to the public—mechanisms for attributing profits to lawbreaking and for calibrating recovery based on order of magnitude effects.[63] Last and importantly, rather than dissipating the benefits of disgorgement awards by distributing a few dollars to each affected consumer, it should specify that at least part of the amount recovered will be used to fund public oversight operations.

Another underused element of the public enforcement tool kit is personal liability for senior executives and board members who thwart or undermine effective public privacy governance. As one option, privacy legislation might empower public authorities to pursue criminal sanctions against individual executives who deliberately violate applicable rules designed to preserve the integrity of important collective processes.[64] As a practical matter, though, establishing the intent required for criminal culpability can be difficult within corporate contexts—in no small part because the same processes of legal endogeneity that undermine real reform also work to negate criminal intent when violations arise.[65] A more promising approach to personal liability would borrow and adapt veil-piercing mechanisms from the corporate enforcement tool kit. Particularly where corporate privacy violators have adopted dual-tier ownership structures to preserve disproportionate voting power for founding "innovators" and venture capitalists—as is the case with most of the tech companies that are now household names[66]—it makes doubly good sense to adopt penalties that target personal wealth accruing from participation in surveillance abuses, even when knowledge or intent regarding specific violations cannot be proved.

CONCLUSION: LESSONS FOR LEGISLATORS

POLICYMAKERS PRIZE CONSENSUS, but at times of great economic and technological transformation, consensus can be a double-edged sword. The emerging inside-the-Beltway consensus on the shape of information privacy legislation is a case in point; it purports to map the road forward but promises only to excuse business as usual and further entrench systemic surveillance abuses. Drafting *effective* privacy legislation requires a starkly different approach. At this critical juncture in governance of networked information processes, it is urgently important to avoid the temptation to takethe easy road. Governance institutions and techniques also can—and should—be sites of innovation. I have sketched an approach to designing public governance institutions capable of constraining networked processes that operate at scale, and have identified additional resources that interested legislators can consult. The 117th Congress has an opportunity to begin that process in earnest.

NOTES

1 Abraham H. Maslow, The Psychology of Science: A Reconnaissance 15–16 (1966).

2 Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019). Others that require opt-in consent are: Social Media Privacy Protection and Consumer Rights Act of 2019, S. 189, 116th Cong. (2019) (sponsored by Sen. Amy Klobuchar [D-MN]); Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) (sponsored by Sen. Maria Cantwell [D-WA]); Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020) (sponsored by Sen. Jerry Moran [R-KS]); Information Transparency & Personal Data Control Act, H.R. 2013, 116th Cong. (2019) (sponsored by Rep. Suzan K. DelBene [D-WA]).

3 Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) (sponsored by Sen. Maria Cantwell [D-WA]). I discuss the ways that regulatory oversight might lend substance to general duties in Part II.

4 Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (2019) (requiring creation of a "Do Not Track" data sharing opt-out website); Balancing the Rights of Web Surfers Equally and Responsibly Act of 2019, S. 116, 116th Cong. (2019) (proposing opt-in approval for sensitive user information and opt-out approval for non-sensitive user information).

5 *See* California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.120(a) (2018) (outlining a consumer right to opt-out). *See also* Illinois Biometric Information Privacy Act (BIPA), 740 Ill. Comp. Stat. 14/15 (2008).

6 *See, e.g.*, Do Not Track Act, S. 1578, 116th Cong. (2019) (empowering the FTC to establish and enforce a national Do Not Track system); Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (2019) (same).

7 Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. Econ. Literature 442 (2016); Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (2018); Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, 21 New Media & Soc'y (2019), https://doi.org/10.1177/1461444819833331 [https://perma.cc/J8B4-K3ES].

8 *See, e.g.*, Lillian Edwards & Michael Veale, *Enslaving the algorithm: From a 'right to an explanation' to a 'right to better decisions'?* 16 IEEE Sec. and Priv. 46–54 (2018); Michael Veale, Reuben Binns, & Max Van Kleek, *Some HCI Priorities for GDPR-Compliant Machine Learning*, CHI-GDPR (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143705 [https://perma.cc/R36K-D7Q7]; Lillian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to Explanation' is Probably Not the Remedy You Are Looking For*, 16 Duke L. & Tech. Rev. 18, 68–72 (2017). *See also* Joe McNamee, *Is Privacy Still Relevant in a World of Bastard Data?*, EDRi Ed., (March 9, 2016), https://edri.org/enditorial-is-privacy-still-relevant-in-a-world-of-bastard-data [https://perma.cc/UE6Q-YCH7].

9 *See, e.g.*, Edwards & Veale, *supra* note 8, at 33-35.

10 *See, e.g.*, Henry E. Smith, *Exclusion Versus Governance: Two Strategies for Delineating Property Rights*, 31 J. Legal Stud. S453 (2002); Henry E. Smith & Thomas W. Merrill, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 Yale L. J. 1 (2000).

11 For a good explanation, see Henry E. Smith, *Mind the Gap: The Indirect Relation between Ends and Means in American Property Law*, 94 Cornell L. Rev. 959, 964-69 (2009) (characterizing the default to private ordering as a "rebuttable presumption" and acknowledging its outer limits).

12 *See generally* Lee Anne Fennell, *The Problem of Resource Access*, 126 Harv. L. Rev. 1471 (2013); Carl H. Coleman, *Rationalizing Risk Assessment in Human Subjects Research*, 46 Ariz. L. Rev. 1 (2004). Many of the most spectacular failures have involved the interests of marginalized and/or low-income communities. *See generally* Thomas W. Mitchell, *From Reconstruction to Deconstruction: Undermining Black Landownership, Political Independence, and Community through Partition Sales of Tenancies in Common*, 95 Nw. U. L. Rev. 505 (2001); Vernellia R. Randall, *Slavery, Segregation and Racism: Trusting the Health Care System Ain't Always Easy—An African American Perspective on Bioethics*, 15 St. Louis U. Pub. L. Rev. 191 (1995). Privacy failures also follow that pattern. *See generally* Ruha Benjamin, Race

After Technology: Abolitionist Tools for the New Jim Code (2019); Nancy S. Kim, Consentability: Consent and Its Limits (2019); Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism (2018).

13 On heightened process requirements for data acquisition, see Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373 (2014); United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

14 *See* 18 U.S.C. § 2518 (Wiretap Act); 18 U.S.C. § 2703 (Stored Communications Act).

15 *See* 50 U.S.C. § 1806(a) ("Information acquired from an electronic surveillance … may be used and disclosed … only in accordance with minimization procedures."). *See also* 50 U.S.C. § 1801(h) (defining "minimization procedures"); *see generally* Daphna Renan, *The FISC's Stealth Administrative Law, in* Global Intelligence Oversight: Governing Security in the Twenty-First Century 121 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016).

16 Case C-311/18, Schrems and Facebook Ireland v. Data Protection Commissioner (2020), http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en#Footnote* ¶45 ("While individuals, including EU data subjects, therefore have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g., E.O. 12333) are not covered. Moreover, even where judicial redress possibilities in principle do exist for non-U.S. persons … claims brought by individuals … will be declared inadmissible where they cannot show 'standing.'"); Case C-362/14, Schrems v. Data Protection Commissioner (2015) ¶90 (concluding that the U.S. government's use of personal information went "beyond what was strictly necessary and proportionate to the protection of national security" and "that the data subjects had no administrative or judicial means of redress.").

17 Case C-311/18, Schrems and Facebook Ireland v. Data Protection Commissioner (2020).

18 *See generally* Eric A. Posner & E. Glen Weyl, Radical Markets: Uprooting Capitalism and Democracy for a Just Society (2018). *But see* Elettra Bietti, *Locked-in Data Production: User Dignity and Capture in the Platform Economy* (Oct. 14, 2019), https://ssrn.com/abstract=3469819 [https://perma.cc/AB4V-J9LF] (arguing a market-based approach to give individuals rights for their data contributions perpetuates harm).

19 *See generally* Elinor Ostrom, Governing the Commons: The Evolution of Institutions for Collective Action (1990); Brett Frischmann, Michael J. Madison, & Katherine J. Strandburg, eds., Governing Knowledge Commons (2014).

20 *See* Julie E. Cohen, *Property and the Construction of the Information Economy: A Neo-Polanyian Ontology, in* Handbook of Digital Media and Communication 333-49 (Leah Lievrouw & Brian Loader, eds., 2020).

21 Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 Calif. L. Rev. 1293 (1996).

22 Midas Nouwens, *Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating their Influence*, CHI'20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems 1 (April 2020), https://dl.acm.org/doi/pdf/10.1145/3313831.3376321.

23 *See, e.g.*, Information Transparency and Personal Data Control Act, H.R. 2013, 116th Cong., 1st Sess. (2019) (sponsored by Rep. Suzan Delbene, D-WA); Social Media Privacy Protection and Consumer Rights Act, S. 189, 116th Cong., 1st Sess. (2019) (sponsored by Sen. Amy Klobuchar, D-MN); Digital Accountability and Transparency to Advance Privacy Act, S. 583, 116th Cong., 1st Sess. (2019) (sponsored by Sen. Catherine Cortez Masto, D-NV).

24 Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy 55-56, 333-35 (2016); *see, e.g.*, Social Media Privacy Protection and Consumer Rights Act of 2019, S. 189, 116th Cong. (2019); Balancing the Rights of Web Surfers Equally and Responsibly Act of 2019, S. 116, 116th Cong. (2019); Application Privacy, Protection, and Security Act of 2020, H.R. 6677, 116th Cong. (2020); Do Not Track Act, S. 1578, 116th Cong. (2019).

25 *See* Richard L. Hasen, Cheap Speech: Saving American Elections in the Disinformation Era (forthcoming, Yale Univ. Press 2021) (manuscript on file with author); *see also* Julie E. Cohen, *Tailoring*

Election Regulation: The Platform Is the Frame, 4 Geo. L. Tech. Rev. 641, 649-53 (2020).

26 Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 Harv. L. Rev. Forum 11 (2020); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183 (2016); Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law* (July 3, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217 [https://perma.cc/QS5R-JY2R].

27 David E. Pozen & Lina M. Khan, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497 (2019).

28 *See* Richards & Hartzog, *supra* note 26; Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 Harv. L. Rev. 34 (2020); Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 Wash. U. L. Rev. (forthcoming in 2021).

29 *See generally* Shmuel I. Becker & Sara Dadush, *Relationship as Product: Transacting in the Age of Loneliness*, 2021 U. Ill. L. Rev. (forthcoming in 2021).

30 *See, e.g.*, Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020) (enhanced management requirements for larger businesses and reduced consumer access rights vis-à-vis smaller businesses); Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (2019) (enhanced reporting and user-facing accountability requirements for larger businesses).

31 *See* Staff of Subcomm. on Antitrust, Com. and Admin. L. Comm. on Judiciary, 116th Cong., Investigation of Competition in Digital Markets (2020).

32 *See* Nikolas Guggenberger, *Essential Platforms* (Sept. 30, 2020), Stan. Tech. L. Rev. (forthcoming in 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3703361 [https://perma.cc/5LJC-LZ5S]; Philip J. Weiser, *Law and Information Platforms*, 1 J. Telecomm. & High Tech. L.1 (2002).

33 *See* Aaron Sankin & Surya Mattu, *The High Privacy Cost of a "Free" Website*, The Markup (Sept. 22, 2020), https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites [https://perma.cc/6S2P-9LEG].

34 Paul Ohm, *Regulating at Scale*, 2 Geo. L. Tech. Rev. 546 (2018).

35 *See* Anthony Nadler, Matthew Crain & Joan Donovan, *Weaponizing the Digital Influence Machine: The Political Perils of Online Adtech*, Data & Soc'y (2018), https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf [https://perma.cc/5RHD-2E5J]; Caitlin Petre, *The Traffic Factories: Metrics at Chartbeat, Gawker Media, and The New York Times*, Tow Ctr. for Dig. Journalism (2015), https://doi.org/10.7916/D80293W1 [https://perma.cc/4L4V-5GLU].

36 Regulation 2016/679 of the European Parliament and of the Council of 27 April 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, May 4, 2016, 2016 O.J. (L 119), art. 5(1)(b)-(c).

37 On the innovation narrative, see Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 71-72, 89-106 (2019).

38 *See* Przemyslaw Palka, *Data Management Law for the 2020s: The Lost Origins and New Needs*, 68 Buff. L. Rev. 559 (2020).

39 *See* Margot Kaminski & Meg Leta Jones, *An American's Guide to the GDPR*, 98 Denver L. Rev. (forthcoming in 2021); *Palka*, supra note 38.

40 *See, e.g.*, Chris Brummer, *Disruptive Technology and Securities Regulation*, 84 Fordham L. Rev. 977 (2015): 977-1052; Henry T.C. Hu, *Disclosure Universes and Modes of Regulation: Banks, Innovation, and Divergent Regulatory Quests*, 31 Yale J. Reg. 565 (2014); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010); Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C. Davis. L. Rev. 529 (2009).

41 *See* Cohen, *supra* note 37, at 160-63, 188-89; Ari Ezra Waldman, *Privacy Law's False Promise*, 97 Wash. U. L. Rev. 773 (2020). On legal endogeneity, *see generally* Lauren Edelman, Working Law: Courts, Corporations, and Symbolic Civil Rights (2016).

42 *See, e.g.*, Mehrsa Baradaran, *Regulation by Hypothetical*, 67 Vand. L. Rev. 1247 (2014); Rory Van Loo, *The Missing Regulatory State: Monitoring Busi-*

nesses in an Age of Surveillance, 72 VAND. L. REV. 1563 (2019); Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 COLUM. L. REV. 369 (2019); Rory Van Loo, *Rise of the Digital Regulator*, 66 DUKE. L.J. 1267 (2017); Lauren E. Willis, *Performance-Based Consumer Regulation*, 82 U. CHI. L. REV. 1309 (2015).

43 *See, e.g.*, HARTZOG, *supra* note 7; David Freeman Engstrom, et al., *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies*, Report submitted to the Administrative Conference of the United States, Feb. 2020, https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf [https://perma.cc/LMM2-LRBK].

44 Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669 (2010); Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377 (2006); Waldman, *Privacy Law's False Promise*, *supra* note 41.

45 Margot Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529 (2019); ARI EZRA WALDMAN, INDUSTRY UNBOUND: PRIVACY, PRACTICE, AND CORPORATE POWER (forthcoming in 2021) (manuscript on file with author).

46 Sonia Katyal & Charles Tait Graves, From Trade Secrecy to Seclusion, 109 GEO. L.J. (forthcoming in 2021).

47 *See* Kaminski, *supra* note 45.

48 Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019); Data Protection Act of 2020, S. 3300, 116th Cong. (2020), §§7(b), 8(b).

49 Data Accountability and Transparency Act of 2020 Discussion Draft, 116th Cong., 2020 Session (2020), https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf [https://perma.cc/7JP7-LDG6].

50 For perhaps the clearest expression of this conventional wisdom, see Cameron F. Kerry, et al., *Bridging the Gaps: A Path Forward to Federal Privacy Legislation*, GOVERNANCE STUDIES AT BROOKINGS (June 2020).

51 *See, e.g.*, RICHARD H. MCADAMS, THE EXPRESSIVE POWERS OF LAW: THEORIES AND LIMITS, 193–94 (2015) (discussing the signaling function of civil enforcement); Cass R. Sunstein, *On the Expressive Function of Law* 144 U. PA. L. REV. 2021, 2032 (1996) (considering the expressive function of law with or without accompanying enforcement activity).

52 *Cf.* Rachel Bayefsky, *Remedies and Respect*, 109 GEO. L.J. (forthcoming in 2021).

53 *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEXAS L. REV. 738 (2018); Cindy A. Schipani & Terry Morehead Dworkin, *Class Litigation After Dukes: In Search of a Remedy for Gender Discrimination in Employment*, 46 U. MICH. J.L. REFORM 1249 (2013). *Cf.* Deborah R. Hensler, *Has the Fat Lady Sung? The Future of Mass Toxic Torts*, 26 REV. LITIG. 883, 892 (2007) ("[W]hat distinguishes mass toxic tort litigation procedurally from virtually all other forms of mass tort litigation … is that plaintiff and defense attorneys in mass toxic torts have not relied exclusively on class actions to aggregate cases.")

54 *See* COHEN, *supra* note 37, at 186-93; Waldman, *Privacy Law's False Promise*, *supra* note 41.

55 *See generally* Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535 (2017). (This, it should be said, is not the privacy class action bar's fault; they are simply following the path of least resistance.).

56 *See generally* COHEN, *supra* note 37; SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); Shoshana Zuboff, *The Coup We Are Not Talking About*, N.Y. TIMES (Jan. 31, 2021), https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html [https://perma.cc/Z4BH-LS9Y].

57 *See generally* Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467 (2020); *cf.* Lauren E. Willis, *Performance-Based Remedies: Ordering Firms to Eradicate Their Own Fraud*, 80 L. & CONTEMP. PROBS. 7 (2017).

58 Nilay Patel, *Facebook's $5 Billion FTC Fine Is an Embarrassing Joke*, THE VERGE (July 12, 2019), https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke.

59 Ohm, *supra* note 34, at 554-55.

60 Liu v. SEC, 140 S. Ct. 1936 (2020).

61 For now. *See* AMG Capital Mgmt. v. FTC, 910 F.3d 417 (9th Cir. 2018), *cert. granted*, 141 S. Ct. 194 (2020).

62 Data Protection Act of 2020, S. 3300, 116th Cong. (2020) (Relief available to be granted by a court or agency includes "rescission or reformation of contracts," "restitution," and "disgorgement or compensation for unjust enrichment."); Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019) (Relief available also includes "rescission or reformation of contracts," "restitution," and "disgorgement or compensation for unjust enrichment.").

63 *See* Ohm, *supra* note 34, at 554-55; *cf.* Samuel N. Liebmann, Note, *Dazed and Confused: Revamping the SEC's Unpredictable Calculation of Civil Penalties in the Technological Era*, 69 Duke L. J. 429 (2019).

64 *See, e.g.*, Mind Your Own Business Act of 2019, S. 2637, 116th Cong. §1352 (2019) (requiring that CEO and chief privacy officer certify annual data protection reports, and imposing criminal sanctions for certain violations).

65 *See, e.g.*, James M. Anderson & Ivan Waggoner, The Changing Role of Criminal Law in Controlling Corporate Behavior (2014); H. Nejat Seyhun, *The Effectiveness of the Insider-Trading Sanctions*, 35 J. L. & Econ. 149, 153, 157–58 (1992); *Developments in the Law: Corporate Crime: Regulating Corporate Behavior Through Criminal Sanctions*, 92 Harv. L. Rev. 1227, 1367–68 (1979).

66 Rani Molla, *More Tech Companies Are Selling Stocks that Keep Their Founders in Power*, Vox Recode (April 11, 2019), https://www.vox.com/2019/4/11/18302102/ipo-voting-multi-dual-stock-lyft-pinterest.

About the Author

Julie E. Cohen is the Mark Claster Mamolen Professor of Law and Technology at the Georgetown University Law Center. She teaches and writes about surveillance, privacy and data protection, intellectual property, information platforms, and the ways that networked information and communication technologies are reshaping legal institutions. She is the author of *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, 2019); *Configuring the Networked Self: Law, Code and the Play of Everyday Practice* (Yale University Press, 2012), which won the 2013 Association of Internet Researchers Book Award and was shortlisted for the Surveillance & Society Journal's 2013 Book Prize; and numerous journal articles and book chapters.

Acknowledgments

Thanks to Lindsey Barrett, Kiel Brennan-Marquez, Erin Carroll, Jeff Gary, Woodrow Hartzog, Paul Ohm, Rory Van Loo, Ari Waldman, and participants in the Knight First Amendment Institute-Law and Political Economy Project's Data and Democracy Symposium for their comments on earlier drafts, and to Dana Holmstrand, Sadev Parikh, and Christina Wing for their outstanding research assistance.

About the Knight First Amendment Institute

The Knight First Amendment Institute at Columbia University defends the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. It promotes a system of free expression that is open and inclusive, that broadens and elevates public discourse, and that fosters creativity, accountability, and effective self-government.

knightcolumbia.org

Design: Point Five
Illustration: ©Erik Carter

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY