THE CASE FOR DATA PRIVACY RIGHTS (OR, PLEASE, A LITTLE OPTIMISM)

*Margot E. Kaminski**

Oh, the tragicomedy of privacy law: just as lawmakers in the United States have started to establish basic data privacy rights recognized the world over, the bulk of privacy law scholarship has conceded that these rights, or their close analogues, are useless.[1]

---

* Associate Professor of Law, Colorado Law; Director, Privacy Initiative, Silicon Flatirons Center; Affiliated Fellow, Information Society Project at Yale Law School. Thanks to: Meg Leta Jones, Harry Surden, Woodrow Hartzog, Neil Richards, and many others for influencing my work. Mistakes and obstinance are my own.

1 *See, e.g.*, Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1930 (2013) [hereinafter Cohen, *What Privacy is For*] ("[T]he new privacy governance is particularly ill-equipped to respond effectively to emerging practices of modulation. Its emphasis on privatized regulation and control of information flows via notice and choice reinforces precisely those aspects of modulation that are most troubling and most intractable."); Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV. (Mar. 23, 2021) [hereinafter Cohen, *How (Not) to Write a Privacy Law*], https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/DY8J-JH44] ("Atomistic, post hoc assertions of individual control rights, however, cannot meaningfully discipline networked processes that operate at scale."); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 425 (2018) ("The idealisation of control in modern data protection regimes . . . creates a pursuit that is actively harmful and adversarial to safe and sustainable data practices. It deludes us about the efficacy of rules and dooms future regulatory proposals to walk down the same, misguided path."); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1660 (1999) ("[T]he critical problem with the model of privacy-as-control is that it has not proved capable of generating the kinds of public, quasi-public, and private spaces necessary to promote democratic self-rule."); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) ("[P]rivacy self-management is certainly a laudable and necessary component of any regulatory regime, I contend that it is being tasked with doing work beyond its capabilities. Privacy self-management does not provide people with meaningful control over their data."); Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. (forthcoming 2022) (manuscript at 5) ("One set of weaknesses stems from the laws' individual rights approach, which is not only based on faulty assumptions, but also entrenches performances that are inherently mismatched against the structural harms of informational capitalism. The performative nature of individual rights in privacy law, which has habituated us into

Rights of notice, access, correction, even opt out—people won't know they have these rights and certainly won't often use them. Companies that must operationalize these rights will operationalize the weakest versions. Grounding data privacy law in individual rights fatally ignores the social scale of data privacy harms.[2] Grounding data privacy law in individual rights relies on malleable, manipulable, cognitively overloaded individuals to do the heavy work of regulating. Grounding data privacy law in individual rights will fail.

This Essay makes the case, nonetheless, for including individual rights in data privacy laws. Individual rights are not sufficient by themselves, but they are necessary for data privacy. These rights reflect common and historic understandings of data privacy and why it matters to many. They instantiate the dignitary and autonomy theories of privacy that form the basis of privacy rights around the world. They may help insulate data privacy laws from First Amendment challenges. And they also serve an overlooked role as a component of governance—a necessary aspect of institutional design. That is, the version of data privacy law that drops individual rights entirely and focuses only on centralized, often *ex ante* governance will encounter predictable problems that individual rights can in fact help resolve. We give up on individual rights at our peril. It's not clear data privacy laws will be enacted, or succeed at regulating, without them.

First, some background for the uninitiated. Most data privacy laws—in contrast with, say, privacy torts or prohibitions on wiretapping—are built on a scaffolding of individual procedural rights known as the Fair Information Practices (FIPs).[3] These rights aim to establish a kind of data due process for individuals whose information is gathered, held, processed, and used by often powerful entities.[4] The

---

thinking managing our privacy is an individual's responsibility, has also allowed industry to weaponize our exercise of those rights to undermine our privacy."); Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19, 38 (2021) ("To the extent that second wave privacy laws offer individuals additional rights to access, correct, delete, and port information, they sit within a long tradition of privacy laws focused on atomistic personal autonomy and choice. Most scholars agree that this conception of privacy is outdated and incompatible with today's information ecosystem.").

2 *See* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573 (2021).

3 *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS xxiii (1973) [hereinafter HEW REPORT]; *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/6YQN-933W]; *see also Fair Information Practice Principles*, IAPP, https://iapp.org/resources/article/fair-information-practices/ [https://perma.cc/N8FT-FJ5P].

4 *See generally* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014); Kate Crawford & Jason Schultz, *Big Data*

FIPs' origin story is debatable; they appear to have originated in parallel in several countries around the same time.[5] But their impact is unmistakable. Nearly every country around the world with a data privacy law—and there are a lot of them—has structured that law at its core around the FIPs.[6]

In the United States, the FIPs were conceived of as a solution to a tough theoretical problem. U.S. privacy law largely did not recognize an expectation of privacy in information once an individual voluntarily shared it.[7] But data processing as a practice raised concerns even if information was initially obtained with permission.[8] Information could be used out of context. It could be erroneous or out of date. It could be used in ways that fail to comport with social values. It could trap people within stigmatized identities not of their own making. It could enable manipulation and even violence. Data processing raised concerns in the 1970s about power imbalances, opacity, and accountability that sound on the whole very much like the policy conversations of today.[9]

The proposed solution, back in 1973, was to rebalance the power ledger through a focus on procedural fairness.[10] If companies and government agencies would not negotiate the terms of data use with individuals, then individuals would have to be affirmatively afforded certain rights. Thus, the FIPs were born (at least, one version was born) on this side of the Atlantic: a right to be notified of data collection and processing, a right of access to one's data, and a right of individual participation that could include correction, deletion, and even opt out. There were affirmative obligations for companies, too, like obligations to identify what the data would be used for, minimize data collection, store data securely, and keep data accurate and up to date. But the core of the FIPs are its individual data privacy process

---

and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B.C. L. REV. 93 (2014); Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI*, 121 COLUM. L. REV. 1957 (2021).

5 *See* Frederik Johannes Zuiderveen Borgesius, Improving Privacy Protection in the Area of Behavioural Targeting 134–35 (Dec. 17, 2014) (Ph.D. dissertation, University of Amsterdam) (UvA-DARE).

6 For example, Article 5 of the General Data Protection Regulation (GDPR) lays out its version of the FIPs principles, which are furthered elsewhere in the GDPR. Council Regulation 2016/679, art. 5, 2016 O.J. (L 119) 35–36 (EU) [hereinafter GDPR]; *see also* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 128 (2017); Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771 (2019).

7 *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979).

8 *See* Kaminski & Urban, *supra* note 4, at 1994–97; HEW REPORT, *supra* note 3, at 167–68.

9 *See* Kaminski & Urban, *supra* note 4, at 1970, 1994–96; HEW REPORT, *supra* note 3, at 167–68.

10 *See* Kaminski & Urban, *supra* note 4, at 1994–96; HEW REPORT, *supra* note 3, at xxiv–xxv.

rights: notice and access, coupled with a (limited) opportunity to be heard.[11]

The FIPs are about fairness. They are not about protecting against the gathering and circulation of substantively sensitive data. They are thus complimentary to, not replacements for, a more substantive privacy tort regime. They are frustratingly vague, and readily made hollow.[12] They also get to the individual core of data privacy, its focus on dignity and autonomy in the face of vast power disparities. Lose the FIPs, and we lose the thread that has tied the data privacy project together. We lose, in short, what motivates many to call for data privacy law.

A number of sectoral U.S. laws operationalize the FIPs.[13] So do data protection laws (data privacy laws) around the world.[14] But until only very recently, the United States lacked a general comprehensive data privacy law. Only in the past few years have several U.S. states begun enacting comprehensive data privacy laws structured around the FIPs' individual rights.[15] Several of these laws, while enacted, have yet to even go into effect. They are far from equivalent to EU data protection law, and certainly have significant shortcomings. Yet here we are, with data privacy rights now squarely within the Overton Window and a host of privacy scholars claiming that they cannot and will not ever work.

How did we get here?

Largely, we got to this place through the mess that is U.S. privacy law. The United States has long relied on a watered-down version of data privacy rights known as "notice and choice."[16] Notice and choice is precisely not what it sounds like. Individuals are given little notice,

11 *See* Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 97–99 (2020).

12 *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 964–77 (2017).

13 *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033–34 (1996); 15 U.S.C. §§ 6501–02 (2018); 16 C.F.R. § 312.2, 312.3 (2016) ("Children's Online Privacy Protection Act" or "COPPA"); 15 U.S.C. § 1681b (2018) ("Fair Credit Reporting Act" or "FCRA"); Hartzog, *supra* note 12, at 953–54; Jones & Kaminski, *supra* note 11, at 99 ("While the FIPs are no panacea, they form the backbone of data protection laws, or data privacy laws, both within the United States and around the world.").

14 *See* Schwartz, *supra* note 6, at 772–75.

15 Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1767 (2021) ("[T]he CCPA is not modeled on the GDPR, though both share similarities founded in the long-established Fair Information Practice Principles.").

16 *See* Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy* Homo Economicus, 49 WAKE FOREST L. REV. 261, 261–62 (2014).

and next to no choice.[17] Anybody who has ever visited a website without reading the privacy policy, or contemplated quitting a social network but found themselves pulled back in by the vortex of their peers, can tell you how well notice and choice has been working. Not well. The individual at the center of U.S. privacy law failed us because she wasn't actually given real rights to begin with.

It has also become common to recognize our very human foibles. Even if we were given real control, it would fail. Humans have limited time and attention spans and known cognitive biases.[18] We drown in choice overload. We are misled by choice architecture. The very core of us is malleable, and companies and political campaigns knowingly exploit that.[19] To hang our hat on individual rights or individual consent would serve not as privacy protection but as "privacy washing." Companies would be able to pretty much keep doing what they have always done, but now they could argue that they were doing it with our permission.[20]

So why not focus, instead, on setting substantive rules for data uses?[21] Talk about the trust we place in information intermediaries, and the corresponding duties we are owed.[22] Mandate certain elements of technological design and prohibit others.[23] Recognize that the much-touted individual is not the only unit of analysis that matters—that population-level impacts should be our focus, and

17 NEIL RICHARDS, WHY PRIVACY MATTERS 174, 176 (2022) (describing the "pathological 'notice and choice' regime governing data practices" and observing that "the American regime of 'privacy self-management' . . . puts the legal responsibility squarely on 'users' of services to make 'choices' about their privacy after 'notice' from the company in the form of a privacy policy, many of which pull off the impressive linguistic feat of being both vague and dense at the same time, saying a lot without really saying anything at all").

18 *See* Hartzog, *supra* note 12, at 969–70; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1488–89 (2019).

19 *See* Cohen, *What Privacy Is For*, *supra* note 1, at 1917.

20 Cohen, *How (Not) to Write a Privacy Law*, *supra* note 1 ("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.").

21 *See id.* (noting that enforcement "efforts do not reliably produce lasting behavioral change unless they are paired with more specific mandates," and referring to the "hole at the center where substantive standards ought to be").

22 *See, e.g.*, Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021); Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34 (2020); Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV. 1897 (2021). *But see* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019).

23 *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 57–58 (2018).

democratic governance our aim.[24] It's not that all of this is wrong—it's not! It's largely right!—but somehow it has been framed in opposition to the individual rights that made data privacy appealing in the first place.

The remainder of this Essay makes the case for why individual data privacy rights are necessary. It admits that data privacy rights are not sufficient by themselves. But if we are going to shift to a more regulatory approach to data privacy, we need to be mindful of what is lost if we give up on individual rights. The loss would be a matter of rhetoric, a matter of motivation, a matter of rights balancing, and perhaps most overlooked, a matter of institutional design. This Essay offers an important counterfactual—not the data privacy laws of our dreams, for sure, but what current state data privacy laws would look like if we gave up on individual rights.

First: individual rights reflect what most people think of when they think of privacy. When somebody signs onto a social network, they aren't thinking "Gee, I really trust these guys."[25] They're not thinking, "Gee, I hope this site has been cleared of dark patterns."[26] They're thinking "Gee, I hope they're not watching me when I do *that*." Or "Gee, I wish I could stop them from sharing this information with my employer, or my girlfriend." Or "Gee, I wish I knew what they were collecting and doing with all that information."

Privacy has historically and theoretically centered on the individual self. The autonomy version of privacy focuses on freedom, choice, and control.[27] The dignitary version of privacy focuses on preventing objectification and preserving personhood.[28] There are flaws in each of these characterizations, to be sure, but they each have

24 Viljoen, *supra* note 2, at 650; Cohen, *How (Not) to Write a Privacy Law*, *supra* note 1 ("[B]ecause 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.").

25 *See supra* note 22.

26 *See generally* Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43 (2021).

27 *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

28 *See, e.g.*, Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES L. 83, 121 (2019) ("[O]ur incomputability is in part protected by a practical and actionable right to reject computation and/or to be computed in alternative ways, underlining the indeterminate nature of each and every individual person and the 'equal respect and concern' that our governments owe each of them."); Lee A. Bygrave, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUT. L. & SEC. REP. 17, 18 (2001); Meg Leta Jones, *The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood*, 47 SOC. STUD. SCI. 216, 231 (2017); Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1016–17 (2017); Martha C. Nussbaum, *Objectification*, 24 PHIL. & PUB. AFFS. 249, 256–57 (1995) (arguing that there are seven forms of objectification).

a long lineage both here and abroad. And they each resonate through the metaphors policymakers love to use and scholars love to hate: privacy as data ownership, and privacy as individual control.[29]

There are a host of significant problems with characterizing data as property.[30] A perfect right to exclude leads to tragedies of the commons, while alienation results in a one-time shot at control that would give up on individual rights that "follow the data." If we gave people data property rights, it's likely we'd end up precisely back where we are: individuals selling their data for pennies, not thinking of future risks, and vulnerable minorities exploited and surveilled. This Essay is certainly not arguing that data rights should be characterized as property rights, nor that the relationship between individuals and their personal data is "ownership" in the conventional sense.

But the now common trope of "data ownership" indicates important things about how many people understand data privacy. When laypeople talk of data "ownership," they are not speaking of establishing monetary incentives to produce a good. They are referencing an Americanized version of dignity, tracing "ownership" back to Lockean desert: I deserve to "own" my data because it came out of my body, my personhood, off my back. Data would be *personal property* in the sense Margaret Radin means it: as closely tied to one's personhood as a wedding ring, home, or diary; not fungible and readily alienated.[31] Data as property invokes, too, the centrality of individual control. If I own my car, I have the right to exclude you from it. If I own my data, I (ideally) control the terms of its sale and use.

When people talk of "control," another term privacy scholars now love to hate, it's often just a shorthand for autonomy. Control is an instantiation of freedom, liberty, choice. Of *course* we don't actually control the distribution of our data. Of *course* we don't have the

29 RICHARDS, *supra* note 17, at 90 ("Privacy as Control runs deep in our legal and cultural understandings of privacy."); Cohen, *How (Not) to Write a Privacy Law*, *supra* note 1 ("[N]one 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."); Jacob M. Victor, Commentary, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 518–19 (2013).

30 *See, e.g.*, Cohen, *How (Not) to Write a Privacy Law*, *supra* note 1 ("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. Contemporary property thinkers do recognize that such an approach can undervalue certain types of collective harms."); Mark A. Lemley, Comment, *Private Property*, 52 STAN. L. REV. 1545, 1547 (2000); Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125, 1151–70 (2000); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2076–94 (2004).

31 *See* Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 959–61 (1982).

capacity in reality, temporally or cognitively, to rationally monitor and choose every way our data will be used. Of *course* companies set the framing and the terms, which often sets the outcomes; in the words of the late Ian Kerr, "the devil is in the defaults."[32] But the rhetoric of autonomy, of control, reflects some very true realities of what privacy, for many, feels like. It's the *choice* of which face to wear for which audience.[33] It's the *choice*, for those privileged enough to be able exercise it, to form our identities.[34] It's the *choice* of how to modify your behavior, or not, depending on who you know will be watching.[35] This explains the centrality of notice to most of our privacy laws, from data privacy laws to wiretapping laws to Fourth Amendment jurisprudence. Notice, ideally, enables adjustment.[36] We manage our boundaries well only if we know the circumstances in which we set them.[37] Or it's the *lack of choice*, the way a lack of privacy freezes us, rendering us vulnerable, even persecuted, embarrassed, exposed.[38]

This capacity for boundary management—this constant dance of a dialectic over how much to reveal and how much to conceal—in reality does not have a liberal self at the core.[39] We are constructed as much as we do the constructing, and we are intermediated and modulated and all of the things. But as Julie Cohen has identified, a central paradox and project of data privacy law is to establish the circumstances where that liberal self could better exist, even as we

32 Ian Kerr, *The Devil Is in the Defaults*, 4 CRITICAL ANALYSIS L. 91 (2017).

33 *See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 1–16 (1973).

34 RICHARDS, *supra* note 17, at 6 ("Privacy rules can promote *identity* formation because privacy can help us to figure out who we are and what we believe, by ourselves and with our intimates and confidants.").

35 *See* Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1132–35 (2015) (building on the work of social psychologist Irwin Altman in defining privacy in physical spaces); *see generally* IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR (1975); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980) ("Our interest in privacy . . . is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.").

36 *See* Kaminski, *supra* note 35, at 1136 ("Requiring notice allows the surveillance subject to recalculate her mechanisms for maintaining an optimized balance of openness and closedness in a given environment. Notice and consent are thus an important aspect of many information capture statutes.").

37 *See* Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 205 (2017) ("[I]f a person has notice of the recording, whether actual or constructive, she will be able to recalibrate her behavior accordingly, with the knowledge that it will be seen or heard by a wider audience. Many recording laws thus have notice requirements; they ban surreptitious recording but allow recording with notice.").

38 *See* Kaminski, *supra* note 35, at 1133, 1137–38.

39 *See* Cohen, *What Privacy Is For*, *supra* note 1, at 1905.

acknowledge it foundationally as myth.[40] That liberal self is at the center not just of so many peoples' conceptions of selfhood but also of the beautiful twisted fiction of American democracy that has driven both our policymaking and our jurisprudence in this space—and drives it still.

Privacy has thus repeatedly, despite scholars' best efforts, been characterized as individualized data "ownership" or individualized control. It has been connected, historically and doctrinally, to the individual body, to individual shame, to self-construction.[41] At the core of privacy, ultimately, is the self. That self may well be a fiction, but it's a fiction that goes down so deep that to root it out is to be left with serious shambles, both legal and theoretical. Data privacy is in some ways crucially different from what has historically been characterized as privacy, but what links the two concepts for the layperson is the ability to know about and intervene in information flows about one's self.[42]

The recent move away from the self in privacy scholarship is understandable. Scholars have long acknowledged that privacy violations produce society-wide harms. Individual privacy harms add up to the potential death of democracy. Can we rely on individual decisions to forge a good society? (No.) Salomé Viljoen's recent contribution on relational surveillance is brilliant: my decision to stay on social media affects how online advertisers someday will profile you.[43] We are all connected in this economy, so to conceive of data privacy only as a series of atomized hierarchical relationships between the watched and the watcher is to neglect the ways in which my choices impact yours. Group privacy, too, is underprotected by atomistic privacy rights; so is privacy in neighborhoods, and in communities historically targeted and surveilled.

The FIPs admittedly don't capture these relationships. They don't capture or protect "group privacy," whether we mean the population-

40 *Id.* at 1918 ("Like the liberal self, liberal democracy has always been an ideal to be pursued and approximated. A polity's ability to approximate liberal democracy has both institutional and material preconditions.").

41 *See* AB 375, 2017–2018 Assemb., Reg. Sess. § 2(f) (Cal. 2018) (enacting The California Consumer Privacy Act of 2018) ("The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."); *see also* Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1875 (2019).

42 *See* RICHARDS, *supra* note 17, at 22 (offering the following working definition of privacy: "Privacy is the degree to which human information is neither known nor used"(emphasis omitted)). For a discussion of the differences between U.S. and EU conceptions of privacy, see *id.* at 17–18; Jones & Kaminski, *supra* note 11, at 97–101.

43 *See* Viljoen, *supra* note 2, at 606.

level effects of demographically based surveillance and data use, or the awfully common scenario of cameras trained primarily on predominantly Black communities.[44] Individual privacy can be a tool of antisubordination.[45] But it also leads to complicated tradeoffs and is not the only nor necessarily the best way to accomplish antisubordination goals.

So. None of this is to say that we shouldn't regulate the bad acts we know about—that we shouldn't make companies design less invasive technologies and prohibit population-level discrimination and the exploitation of particularly vulnerable or historically marginalized groups. We should do all those things! To an individual, data privacy harms may feel deeply individual. But to a company, an individual is a data widget, among many data widgets: a set of eyeballs and a wallet and some demographic traits. If we're going to be treated and manipulated and manufactured like widgets, companies should be regulated like widget-makers, for sure.

It's this duality of personal data—widget in the one sense, selfhood in another (and if we really want to get complicated, speech antecedent in a third, but more on that in a moment)—that makes regulating it so complex. And it's the duality of personal data that we may be able to harness to get the kinds of privacy laws scholars now call for. Because people care about their selves. Widget making is less interesting. What motivates the enactment of data privacy laws—what's motivating the enactment of data privacy laws *right now*—is an individual's experience of feeling like her personal information is out of her control.[46] That is, the California Consumer Privacy Act (CCPA) isn't about widgets and widget makers and capital or even

---

44 *See, e.g.*, Chaz Arnett, *Race, Surveillance, Resistance*, 81 OHIO STATE L.J. 1103, 1110 (2020); Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J. L. & TECH. 425, 429 (2017) (observing the harms of group surveillance).

45 Scott Skinner-Thompson, *Agonistic Privacy & Equitable Democracy*, 131 YALE L.J.F. 454, 457 (2021) ("[W]hile privacy scholars have underscored privacy's ability to enable participation, members of marginalized groups have used privacy itself to create agonist, participatory friction."); *see also* SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS 103 (2021) (discussing surveillance as a tool of subordination).

46 *See* AB 375, 2017–2018 Assemb., Reg. Sess. § 2(g)–(h) (Cal. 2018) (enacting The California Consumer Privacy Act of 2018):

> (g) In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened.
>
> (h) People desire privacy and more control over their information. California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information.

discrimination—it's about *inalienable rights.*[47] And inalienable rights, for better or for worse, belong to individuals.[48]

Perhaps one reason U.S. scholars feel so ready to shift away from the individual rights framework is that we haven't constitutionalized data privacy on this side of the Atlantic. If we only had a federal constitutional right to data privacy that applied to both governmental and nongovernmental actors! In Europe, data privacy is a human right.[49] It's in the EU Charter.[50] It has been read into the European Convention on Human Rights.[51] It's muddled, and fuzzy, and intertwined with other conceptions of privacy, and involves balancing tests that are confusing to most Americans, to be sure. But the core of the data privacy right is a fundamental human right that belongs to an individual. To get rid of this core is to get rid of the foundation for the whole apparatus, including the detailed widget regulation.

While we may not have a federal constitutional right to data privacy, we now for the first time have state laws that instantiate similar rights through legislation. And these laws draw a through-line from state constitutional privacy rights to these newly legislated data privacy rights. Both the CCPA and the Colorado Privacy Act are framed by preambles touting the existence of a privacy right in each respective state constitution. Each law's preamble explains that now is the time to update those rights to address privacy harms in the data analytics age.[52]

Whether they're constitutional rights or not, data privacy rights sound in fundamental rights rhetoric. They also do more than that, even here in the United States. Data privacy rights offer a potentially powerful defense on the battleground of constitutional analysis. Because as most know, the First Amendment as currently interpreted poses a significant threat to data privacy laws. Characterizing data privacy as an individual right can, as a number of us have now noted,

---

47 *See id.* § 2(a) ("In 1972, California voters amended the California Constitution to include the right of privacy among the 'inalienable' rights of all people. . . . Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.").

48 *See* Colorado Privacy Act, COLO. REV. STAT. § 6-1-1302(a)(I) (2021) ("The people of Colorado regard their privacy as a fundamental right and an essential element of their individual freedom.").

49 *See* Jones & Kaminski, *supra* note 11 at 103.

50 Charter of Fundamental Rights of the European Union arts. 7–8, Dec. 12, 2000, 2000 O.J. (C 364) 10.

51 European Convention on Human Rights art. 8, Nov. 4, 1950, E.T.S. No. 5; *see also* Gloria González Fuster & Serge Gutwirth, *Opening Up Personal Data Protection: A Conceptual Controversy*, 29 COMPUT. L. & SEC. REV. 531, 536 (2013).

52 *See* Colorado Privacy Act, COLO. REV. STAT. § 6-1-1302(a)(II) (2021) ("Colorado's constitution explicitly provides the right to privacy under section 7 of article II, and fundamental privacy rights have long been, and continue to be, integral to protecting Coloradans and to safeguarding our democratic republic[.]"); COLO. CONST. art. II, § 7.

place First Amendment interests on both sides of the equation.[53] Unchecked surveillance causes chilling effects (on individuals). It leads to the depletion of minority views (held by individuals). It causes individuals to avoid reading controversial material, to avoid participating in democracy. If we drop the individual cast of data privacy law, we maybe win the battle over getting more substantive regulation into legislation. (A big maybe). But we do so at the cost of potentially losing the First Amendment war.

This Essay closes with what might at first feel like a detour: an analysis of privacy regulation through the lens of institutional design. It turns out that even if individuals are faulty decisionmakers, and even if individual rights are rarely exercised, and even if we all agree that the right unit of analysis for data privacy law is social or the group, individual rights can still do things that government regulation alone cannot. That is, individual rights can be complimentary to regulation. This is a lesson as old as administrative law.[54]

In a perfect world, what does *regulatory* data privacy law look like? That is, data privacy law that isn't centered on the individual. (To be clear, a full answer to this is well beyond the scope of this Essay.) It probably starts with some bans: you can't gather x types of info, can't conduct info-gathering under y circumstances, or can't use data in z ways. So, legislators or regulators come up with some bans, which aim to protect particular practices (like communications), relationships (like doctor-patient), spaces (like homes), information (like sexual information), or vulnerable parties (like children). (We'll leave aside for now the potential First Amendment implications of any of this.)

Then they come up with exceptions to the bans. Then they mandate some design elements (like prominent visceral notice and clear consent streams), while prohibiting others (like dark patterns). Maybe they institute licensing requirements: you can't process or use personal data without approval of your practices by a regulator.[55] Your license is conditional: you can only process and use data under certain circumstances. It must be reviewed and renewed every few years. And it's revocable: you have to stop processing data if you exceed your license or do something wrong. An enforcing agency probably

53 *See, e.g.*, Kaminski, *supra* note 37, at 203 ("[T]he Supreme Court has recognized that protecting this kind of privacy is itself often protective of free expression. First Amendment interests, in other words, arise on both sides."); Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 466–67 (2015); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 393–407 (2008).

54 *See, e.g.*, Douglas A. Kysar, *The Public Life of Private Law: Tort Law as a Risk Regulation Mechanism*, 9 EUR. J. RISK REG. 48 (2018).

55 *See* Frank Pasquale, *Licensure as Data Governance*, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV. (Sept. 28, 2021), https://knightcolumbia.org/content/licensure-as-data-governance [https://perma.cc/PR4A-JDDN].

conducts rulemaking to get public input into clarifying everything (the bans, the exceptions, the design requirements, the licensing standards), and maybe issues ongoing cyclical guidance in consultation with a variety of stakeholders. Then they build up a huge, costly, expert enforcement apparatus, monitor the market for wrongdoings, and impose big sanctions when they happen. What's so wrong with this plan?

Well, first, it won't happen. If we look at the *other* aspect of recent data privacy laws, the part that regulates rather than relies on individual rights, we see that the counterfactual isn't this (to some) ideal. The counterfactual, even in Europe, is impact assessments: internal enterprise risk management constructed around vague and contestable standards.[56] Not clearly articulated bans (or, at least, not many of them).[57] Not licensing. Don't get me wrong: done well, there's lots to like about impact assessments and risk mitigation backed by substantive design standards and human rights.[58] I want companies to be forced to think about a technology's impact on human rights before they deploy it. I want them to have to build things differently and take the public good into account. I'd love them to get audited and monitored and have reporting requirements. All of that would be leaps and bounds above the current state of play in the United States, including in new data privacy laws.[59] But it's not the data privacy

56 *See* Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1604–05 (2019) (discussing impact assessments in the GDPR); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301 to 1313 (2021); Consumer Data Privacy Act, VA. CODE ANN. §§ 59.1-571 to 581 (2021); Cohen, *How (Not) to Write a Privacy Law*, *supra* note 1.

57 An exception is a proposed law in the state of Washington, as discussed in Margot E. Kaminski, Regulating the Risks of AI (Feb. 14, 2022) (working paper) (on file with author); *see also* SB 5116, 2022 Leg., Reg. Sess. (Wash. 2022).

58 *See* Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 HARV. J.L. & TECH. 117 (2021); Margot E Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations*, 11 INT'L DATA PRIV. L. 125 (2021); Jacob Metcalf, Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh & Madeleine Clare Elish, *Algorithmic Impact Assessments and Accountability: The Co-Construction of Impacts*, *in* ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 735 (2021); Emanuel Moss, Elizabeth Anne Watkins, Jacob Metcalf & Madeleine Clare Elish, *Governing with Algorithmic Impact Assessments: Six Observations*, *in* AAAI/ACM Conference on AI, Ethics, and Society 1010 (2021); EMANUEL MOSS, ELIZABETH ANNE WATKINS, RANJIT SINGH, MADELEINE CLAIRE ELISH & JACOB METCALF, DATA & SOC'Y, ASSEMBLING ACCOUNTABILITY: ALGORITHMIC IMPACT ASSESSMENTS FOR THE PUBLIC INTEREST (2021).

59 Chander et al., *supra* note 15, at 1750 (pointing out that while most proposed U.S. privacy laws have some version of the FIPs, they lack the accountability and governance half of the GDPR). Newer laws like Colorado's and Virginia's, modeled after Washington's, lean in on a lite version of impact assessments, but again lack the GDPR's required structure; central regulator; history of regulation; backstop constitutional court; and many, many, many procedural and substantive details.

regime most scholars dream of. It's just the data privacy regime we are most likely to get.

Second, even if a more top-down version of regulatory privacy were enacted, it would still lack some of the benefits that individual rights could provide. It wouldn't let individuals make their own choices or opt out. It would be one-size-fits-most. It wouldn't compensate individuals for individual harms or correct those harms once they occur. It wouldn't provide civil recourse for individuals: a way for them to identify what's been done specifically to them and be listened to, acknowledged, and recognized. And it would miss out on potentially important policy feedback. That is, individual claims, whether made through litigation or otherwise, can afford opportunities to change policy going forward. Environmental regulatory standards came out of litigation;[60] so did safety standards for cars.[61] Because this is the thing about individual rights: they can be, in fact often are, complementary to regulation, not in opposition to it. If we can't get the institutions exactly right—can't force companies to consult impacted stakeholders, or get regulators to ignore a flood of industry input—then individual rights offer another way in.

Last, and far from least, individual data privacy rights with their emphasis on notice and access potentially offer us transparency onto patterns and practices we currently cannot see. That has regulatory value. It informs, even drives, new policymaking. It allows input by stakeholders who might otherwise not be at the table. It potentially holds companies publicly accountable and prevents or mitigates capture. This still matters even if we get command-and-control privacy regulation (which we won't). Because even if we get more top-down privacy law, there will still be delegation to companies. It's the nature of the beast. No technology-neutral omnibus law can get by with writing rules on absolutely everything. Maybe no law can, period. So unless we replace that source of oversight with something else (and there's little sign of appetite for, say, publicly releasing impact assessments[62]), we forego the not inconsiderable potential benefits of having more information. Information imbalances are power imbalances, right?

We may be able to design a version of regulatory privacy that gets us many of the touted but unrealized benefits of individual rights. I'm not confident that we could get it enacted. I'm not confident that if it were enacted, it wouldn't get watered down or even captured. I am confident that there is more to individual rights than we currently give them credit for, especially if they are well executed.

---

60 *See* Kysar, *supra* note 54, at 49.

61 *See* Bryan H. Choi, *Crashworthy Code*, 94 WASH L. REV. 39, 87 (2019).

62 *See* Kaminski, *supra* note 57.

Maybe it's not that individual rights will inevitably fail, but that we have not made them strong enough. Maybe we have not put enough thought into structuring incentives for people to use them. Maybe there is a reason that so much energy has gone into the détente over whether data privacy laws should be enforceable through a private right of action.[63] Maybe there is something to constitutionalizing, to talking in terms of *rights* and not economic *choice* or *consent*. And maybe, even if you don't agree with any of this, there is still value to thinking about how to design and implement the individual rights we now have so that they better work towards overall governance goals.

Just imagine if we could actually say no. Wait, Apple has: and a reported 96% of individuals opted out of targeted tracking.[64] Meta's stock dropped more than 25%.[65] So much for individual rights.

63 *See* Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639 (2022).

64 Samuel Axon, *96% of US Users Opt Out of App Tracking in iOS 14.5, Analytics Find*, ARS TECHNICA (May 7, 2021), https://arstechnica.com/gadgets/2021/05/96-of-us-users-opt-out-of-app-tracking-in-ios-14-5-analytics-find/ [https://perma.cc/D85E-8L3Q]. Thanks to Meg Jones for a conversation regarding this number.

65 Carly Olson, *Meta Rivalry with Apple Inflamed as Facebook Parent Company Share Price Plummets*, THE GUARDIAN (Feb. 4, 2022), https://www.theguardian.com/technology/2022/feb/04/meta-rivalry-apple-inflamed-facebook-parent-company-share-price-plummets [https://perma.cc/6BLQ-8MUF] (last visited Apr. 2, 2022).