Privacy, Practice, and Performance

Ari Ezra Waldman*

Privacy law is at a crossroads. In the last three years, U.S. policymakers have introduced more than fifty proposals for comprehensive privacy legislation, most of which look roughly the same: they all combine a series of individual rights with internal compliance. The conventional wisdom sees these proposals as groundbreaking progress in privacy law and explains their uniformity by looking to catalyzing precedent like the General Data Protection Regulation in Europe or the California Consumer Privacy Act.

This Article challenges that emerging consensus. Relying on contemporary sociological and critical studies scholarship, this Article analyzes recent privacy proposals in the United States through their social practices and argues that those practices are drawing boundaries that set the terms of privacy law from the ground up. In other words, privacy law's practices are descriptively and normatively performative: they have socially constructed what we think privacy law is and should be. We have not only become accustomed to conceptualizing privacy law in certain ways; we have come to see a model of individual rights and internal procedural compliance as the normal, ordinary, commonsense modality of privacy law. So constructed, privacy law is flawed, with substantial negative effects for individuals, society, equality, and justice.

DOI: https://doi.org/10.15779/Z38JD4PQ3D

* Professor of Law & Computer Science and Faculty Director, Center for Law, Information, and Creativity, Northeastern University. Ph.D., Columbia University; J.D., Harvard Law School. This project is the third in a series of projects about the social practices of privacy law, culminating in a book: *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*. This Article benefited from comments and suggestions from participants at faculty colloquia at Northeastern University School of Law, Northeastern University College of Social Sciences and Humanities, Georgetown University Law Center, the University of Colorado School of Law, Yale Law School, Washington University in St. Louis, and Harvard University. Special thanks to Sophia Baik, Ryan Calo, Danielle Citron, Julie Cohen, Yan Fang, Andrew Gilden, Jeff Gary, Woodrow Hartzog, Margot Kaminski, Cameron Kerry, Mihir Kshirsagar, Filippo Lancieri, Bill McGeveran, Laura Moy, Frank Pasquale, Jon Penney, Neil Richards, Paul Schwartz, Daniel Solove, Evan Selinger, Salomé Viljoen, and Felix Wu. Margaret Foster provided essential research assistance. I performed all errors on my own.

This Article provides a full critical account of the latest developments in privacy law, focusing on its practices rather than law on the books. It details and challenges current privacy law's focus on individual rights and internal compliance. And it explores potential new directions for privacy law based on the performative capacities of privacy law's practices, including new emancipatory practices and performances.

INTRODUCTION

In the last four years, there have been eleven proposals for comprehensive privacy legislation introduced in the United States Congress.[1] Two ballot initiatives and thirty-nine privacy bills have been introduced in twenty-eight states during that time.[2] This is in addition to the European Union's General Data Protection Regulation (GDPR), which took effect in 2018, and the California Consumer Privacy Act (CCPA), which took effect in 2020.[3] That is an unprecedented flurry of legislative activity.

---

1. *See* Consumer Data Privacy and Security Act of 2021, S. 1494, 117th Cong.; Data Care Act of 2021, S. 919, 117th Cong. (2021); Information Transparency & Personal Data Control Act, H.R. 1816, 117th Cong. (2021); Data Accountability and Transparency Act of 2020 (DATA), 116th Cong. (2020) [hereinafter DATA] (distributed as discussion draft); Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act), S. 4626, 116th Cong. (2020) [hereinafter SAFE DATA Act]; American Data Dissemination Act of 2019 (ADD Act), S. 142, 116th Cong. (2019); Consumer Online Privacy Rights Act (COPRA), S. 2968, 116th Cong. (2019) [hereinafter COPRA]; Data Care Act of 2019, S. 2961, 116th Cong. (2019); Mind Your Own Business Act of 2019 (MYOBA), S. 2637, 116th Cong. (2019) [hereinafter MYOBA]; Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019) [hereinafter Privacy Bill of Rights]. A discussion draft was introduced recently. Discussion Draft, A Bill to Provide Consumers with Foundational Data Privacy Rights, Create Strong Oversight Mechanisms, and Establish Meaningful Enforcement, 117th Cong., 2d Sess. (2021), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Bipartisan_Privacy_Discussion_Draft_Bill_Text.pdf [https://perma.cc/LM9J-9QKV].

2. *See* California Privacy Rights Act of 2020 (codified as amended at CAL. CIV. CODE § 1798.100–1798.199.100); 52 NEV. REV. STAT. § 603A (2020); H.R. 216, 2021 Leg., Reg. Sess. (Ala. 2021); S. 21–190, 73d Gen. Assemb., 1st Reg. Sess. (Colo. 2021); S. 893, 2021 Gen. Assemb., Jan. Sess. (Conn. 2021); H.R. 3910, 102d Gen. Assemb., 1st Reg. Sess. (Ill. 2021); S. 46, 192d Gen. Ct., Reg. Sess. (Mass. 2021); S. 567, 2021 Leg., 244th Reg. Sess. (N.Y. 2021); A. 6042, 2021 Leg., 244th Reg Sess. (N.Y. 2021); S. 6701, 2021 Leg., 244th Reg. Sess. (N.Y. 2021); S. 569, 2021 Gen. Assemb., 2021 Sess. (N.C. 2021); H.R. 1126, Gen. Assemb., 2021 Sess. (Pa. 2021); H.R. 3741, 87th Leg., Reg. Sess. (Tex. 2021); S. 1392, 2021 Gen. Assemb., 1st Spec. Sess. (Va. 2021); S. 5062, 67th Leg., 2021 Reg. Sess. (Wash. 2021); S. 1614, 54th Leg., 2d Reg. Sess. (Ariz. 2020); H.R 2729, 54th Leg., 2d Reg. Sess. (Ariz. 2020); H.R. 963, 26th Leg., Reg. Sess. (Fla. 2020); S. 2330, 101st Gen. Assemb., 1st Reg. Sess. (Ill. 2020); H.R. 5603, 101st Gen. Assemb., Reg. Sess. (Ill. 2020); H.R. 784, 2020 Gen. Assemb., 441st Sess. (Md. 2020); H.R. 1656, 2020 Gen. Assemb., 441st Sess. (Md. 2020); H.R. 3936, 91st Leg., 91st Sess. (Minn. 2020); L. 746, 106th Leg., 2d Reg. Sess. (Neb. 2020); H.R. 1236, 2020 Gen. Ct., 166th Sess. (N.H. 2020); Assemb. 3255, 219th Leg., 1st Ann. Sess. (N.J. 2020); H.R. 473, 2020 Gen. Assemb., 2020 Sess. (Va. 2020); S. 418, 30th Leg., Reg. Sess. (Haw. 2019); S. 2263, 101st Gen. Assemb., 1st Reg. Sess. (Ill. 2019); S. 946, 129th Leg., 1st Reg. Sess. (Me. 2019); H.R. 1253, 2019 Leg., 2019 Reg. Sess. (Miss. 2019); S. 176, 54th Leg., 1st Sess. (N.M. 2019); S. 224, 2019 Leg., Reg. Sess. (N.Y. 2019); S. 5642, 2019 Leg., Reg. Sess. (N.Y. 2019); H.R. 1049, 203d Gen. Assemb., 2019 Sess. (Pa. 2019); S. 234, 2019 Gen. Assemb., Jan. Sess. (R.I. 2019); H.R. 4390, 86th Leg., Reg. Sess. (Tex. 2019); H.R. 4518, 86th Leg., Reg. Sess. (Tex. 2019); Assemb. 2188, 219th Leg., 2020 Sess. (N.J. 2020); S. 2834, 218th Leg., 1st Ann. Sess. (N.J. 2018).

3. *See* Council Regulation (EU) 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, 2016 O.J. (L 119) [hereinafter GDPR]. The GDPR applies to U.S. companies in certain circumstances, so it is relevant for assessing the privacy law landscape even outside the E.U.. *See id.* at art. 3(2)(a)–(b); CAL. CIV. CODE §§ 1798.100–1798.199.100 (2018 Cal. Legis. Info.) [hereinafter CCPA].

Remarkably, most of these proposals look roughly similar: they add a combination of individual rights of control and internal compliance structures (the rights/compliance model) to the traditional model of privacy notices and consent buttons.[4] This means that policymakers seem committed to, or stuck on, a single model of privacy governance.

This uniformity is notable, as is policymakers' coalescence around the rights/compliance model of privacy law. It is unusual that politically polarized states—the "laborator[ies]" of very different visions of democracy—and a starkly divided Congress would roughly agree on a single framework for new privacy laws.[5] After all, there are other options on the table.[6] The choice of a rights/compliance model is even more surprising given that scholars generally agree that employing this framework in the U.S. regulatory context would be risky.[7]

Previous scholars have looked to the GDPR or the CCPA for inspiration, suggesting that new proposals are the products of legal and norm entrepreneurship by leading regulatory jurisdictions or individual actors.[8] These analyses are illuminating, but incomplete. Some take a law-on-the-books approach, ignoring the ways in which law is also a social practice involving

4. Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1559–62 (2019). As described in more detail below, I disagree with other scholars' descriptive analyses of these privacy proposals. Anupam Chandar, Margot E. Kaminski, and William McGeveran do not characterize proposed U.S. state laws as having a rights/compliance model. *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1733. Instead, they see them as largely individual rights-based only laws. That is true from a law-on-the-books perspective: the laws do not require extensive internal compliance like the GDPR. But as described in Part II.B.2, the proposals do require privacy impact assessments and any regime that guarantees rights also requires a company to build forms, evaluate data requests, and set up appeals processes. These are internal compliance structures. *See id.* at 1736 (2021) (arguing that recent proposals in the United States "differ[] significantly—and consciously—from the European model.").

5. New State Ice Co. v. Liebermann, 285 U.S. 352, 387 (Brandeis, J., dissenting) (referring to a state as a "laboratory" of policy experimentation); *see generally* JAMES E. CAMPBELL, POLARIZED: MAKING SENSE OF A DIVIDED AMERICA (2016) (analyzing political polarization in the United States.).

6. *See, e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT 93–157 (2018) (calling for a "design agenda for privacy law" that leverages various legal regimes to ensure that privacy is designed in, and manipulation is designed out of, information technologies); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 1003–12 (2021), (detailing what an information fiduciary model of governance would look like in practice); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205–09 (2016) (justifying imposing fiduciary duties on online service providers).

7. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1714, 1721–37 (2020).

8. *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 22–26 (2012) (suggesting that the E.U.'s ban on transfers of data to countries without adequate levels of protection would catalyze a race to the top to mimic the GDPR); Chander et al., *supra* note 4, at 1767 (arguing that new U.S. proposals are different from the GDPR and instead reflect the unique ways in which the CCPA was the product of norm entrepreneurship that harnessed state legislative processes to produce the law).

regulators, lawyers, compliance professionals, and individuals.[9] Others take a more nuanced approach, exploring how advocates harness institutional apparatuses to create privacy law.[10] But to look for origins and catalysts misses substance and efficacy. We need to know why policymakers chose *these* proposals and, more importantly, whether they are up to the task of protecting privacy in an era of data-extractive capitalism. [11]

This Article answers those questions. My descriptive claim is that privacy law can be understood as a collection of repeated and habituated performances that have normalized themselves among regulators, industry, and individuals as what privacy law is and should be, thereby excluding other options. Privacy law's performances, including internal compliance programs, privacy impact assessments (PIAs), consent toggles and opt-out buttons, consultations and settlements with industry, and exercises of individual rights have constructed privacy law in ways that entrench themselves from within. When practitioners complete PIAs or internal audits, they become accustomed to thinking that filling out documents *is* privacy law. When companies hire a chief privacy officer (CPO), they send a message to industry that hiring a CPO *is* privacy law. And when websites send emails saying they "care about" our privacy and require us to opt out of tracking, we become accustomed to thinking that self-governance and corporate management of our data *is* privacy law.

Some of these practices predate the GDPR and the CCPA;[12] others were developed by industry in the wake of the GDPR. And individual rights beyond notice-and-consent are decades old.[13] But all of these practices are performative, and our acculturation to them has entrenched them and defined our relationship

9. *See, e.g.*, Bradford, *supra* note 8. This tranche of scholarship erroneously implies that law is an institution exogenous to society. *See* PATRICIA EWICK & SUSAN S. SILBEY, THE COMMON PLACE OF LAW: STORIES FROM EVERYDAY LIFE 15–32 (1998) (suggesting that law is social in nature in that it is present in everyday social experiences); Roger Cotterrell, *Why Must Legal Ideas Be Interpreted Sociologically*, 25 J.L. & SOC'Y 171, 172–73 (1998) (arguing that sociological interpretations of legal institutions can help understand the meaning of law itself); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 3–8 (2019); MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW 1870-1960 (1992); KARL POLANYI, THE GREAT TRANSFORMATION: THE POLITICAL AND ECONOMIC ORIGINS OF OUR TIME (2d ed. 2001).

10. *See* Chander et al., *supra* note 4, at 1790.

11. "Data-extractive capitalism" refers to a particularly oppressive and dominating form of informational capitalism, an economic system in which data is processed to derive insights about individuals for profit. *See* COHEN, *supra* note 9, at 3–5.

12. *See* Decision and Order, Google, Inc., FTC Docket No. C-4336, at 4 (Oct. 13, 2011) [hereinafter Google Consent Decree], https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf [https://perma.cc/W594-63YA] (requiring Google to develop a "comprehensive privacy program").

13. *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 (1973) (describing the "Fair Information Practice Principles" (FIPP), which originally included rights to notice, access, correction, and reasonable security); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 957–59 (2017) (describing how the original FIPPs included more than just a right to notice).

to, and assumptions about, privacy law. Habits die hard, and these habits are not just getting stronger; they make it impossible for us to change. No wonder many new proposals look the same.

As described in more detail in Part I, performances are actions and behaviors that communicate something to the self and others.[14] We dress, speak, and interact in ways that reflect our identities and the identities we choose to share with others.[15] Following sociological and critical theory, these performances can also be performa*tive*—that is, repeated, everyday performances constitute, create, and reinforce social or legal categories, including identity, gender, and race.[16] Likewise, I argue that practices associated with individual privacy rights and corporate compliance have performatively constructed the category of *privacy law* by habituating us into thinking that only these practices are what privacy law is and should be.

Part II applies the performativity thesis to privacy law's practices, demonstrating how the information industry has entrenched practices that have influenced and molded the current wave of privacy law proposals.[17] Individuals, regulators, and industry all engage in performative practices of privacy law. Individuals navigate consents, cookie requests, privacy policies, and data request links. Supplementing privacy self-governance are practices in which regulators partner with industry to settle disputes and develop rules and where industry creates internal compliance structures for ongoing accountability. These practices have percolated up, constructing a roughly uniform approach to privacy law reflected in almost every recent proposal for comprehensive privacy law in the United States.

But those practices are not necessarily good for privacy. Privacy law's performances are constructions of industry. And as a result of internal inconsistencies and commitments to symbols and procedure, the model accustoms us to hollowed-out public institutions and insufficient privacy protection. In Part III, I make a normative claim that the performativity of privacy law's practices not only explains why current privacy discourse and proposals from U.S. policymakers look roughly the same, but also shows that the

14. *See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 15 (1959) (defining performance as "all the activity of a given participant on a given occasion which serves to influence in any way any of the other participants"). Richard Schechner defined performances as "twice-behaved" or "restored" behavior. RICHARD SCHECHNER, PERFORMANCE STUDIES: AN INTRODUCTION 28–29 (3d ed. 2013). For a more detailed discussion of performance theory, see *infra* Part I.A.

15. *See* GOFFMAN, *supra* note 14, at 15–23.

16. *See* JUDITH BUTLER, BODIES THAT MATTER: ON THE DISCURSIVE LIMITS OF "SEX" 2 (1993); Jacques Derrida, MARGINS OF PHILOSOPHY 307–30 (Alan Bass trans. 1982) (discussing how repeated expressive acts can create forms of identity); THE LAWS OF THE MARKETS (Michel Callon ed., 1998).

17. *See generally* Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19 (2021) (classifying the evolution of privacy law in terms of "waves" based on the periodization from feminist literature).

rights/compliance model is likely incapable of addressing the privacy and structural harms of informational capitalism.[18]

In particular, understanding privacy law from the perspective of performance highlights two categories of weaknesses in current proposals. 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 rights in privacy law, which has habituated us into thinking that managing our privacy is an individual responsibility, has also allowed industry to weaponize our exercise of those rights to undermine our privacy. A second set of weaknesses is based on privacy law's reliance on internal corporate processes. As Margot Kaminski has already warned, the social construction of privacy law around industry practices tends to favor the practices of the wealthiest and most dominant actors in the information industry, creating an anti-competitive landscape.[19] But the proposals' problems run deeper. The law's use of procedural performances as its regulatory lever also habituates privacy professionals, ignores data-extractive capitalism's inconsistency with democratic values, and adopts neoliberal assumptions about the law's place in economic ordering. Perhaps most importantly, the performative use of a managerialized public-private partnership is internally inconsistent: it endogenously creates public institutions that are dependent on industry expertise, efficiency, and nimbleness. Therefore, those public institutions become incapable of acting as the promised "backdrop threat" that guards against capture.[20]

The inadequacies inherent in recent U.S. privacy proposals require different, opposing performances that can socially construct privacy law and regulatory institutions as counterweights to corporate power. The goal is not to eliminate performances and the performativity of practices; that's not possible.[21] Rather, the goal is to perform privacy law in emancipatory ways—namely, to address the ways in which data-extractive capitalism creates vulnerabilities, power asymmetries, and subordination.[22] Part IV outlines an alternative framework inspired by what André Gorz called "non-reformist reforms," or reforms that raise our consciousness of our subordination, while taking us closer to the ultimate goal of transformational change.[23] Rebuilding public governance

18. *See* COHEN, *supra* note 9, at 5.

19. Kaminski, *supra* note 4, at 1577.

20. *Id.* at 1561. Notably, Kaminski argued that the GDPR does not adequately create and sustain this backdrop threat because of a lack of accountability, transparency, and civil society input.

21. *See* BUTLER, *supra* note 16, at x–xi, 7 (noting that there is no identity before performance).

22. *See* Jedediah Britton-Purdy, David Singh Grewal, Amy Kapczynski & K. Sabeel Rahman, *Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis*, 129 YALE L.J. 1784, 1789–90 (2020).

23. ANDRÉ GORZ, STRATEGY FOR LABOR: A RADICAL PROPOSAL 7 (Martin A. Nicolaus & Victoria Ortiz trans., 1967).

will take work, will, and money, but society already has the tools to start: collective power, penalties, invigorated public institutions, civil rights, worker unionization, and a seat at the table not just for civil society, but for marginalized populations whose voices have been drowned out by a neoliberal focus on what industry wants. Even these changes will not achieve the ultimate goal of a radically reconstituted public regulatory space. But they are the beginnings of a new approach. We must walk before we can run.

To review, this Article proceeds as follows. Part I brings together two related literatures in sociolegal studies: performativity and the endogeneity of law. This Section adds to the extant legal scholarship on performativity by focusing on how practices can create law. Part II applies the performativity thesis to privacy law's practices, showing how long-standing practices of regulators, industry, and individuals have become the defining features of recent proposals for comprehensive privacy law in the United States. This Section also contributes to the privacy literature in another way—namely, by focusing less on the specific provisions of the laws, and more on the regulatory, corporate, and individual practices that develop in their wake. Part III makes the Article's normative argument that the privacy law these performances have constructed is incapable of addressing the privacy and equitable harms of informational capitalism. Finally, Part IV proposes several alternative performances that could rescue privacy law from its rut.

I.
PERFORMATIVITY AND ENDOGENOUS LAW

This Article brings together three related theories from the social sciences to explain the current status and failures of privacy law: performativity, habit, and normalization. Performativity is the idea that our actions can create social categories, like identity. Habit is one process through which that happens, and normalization is the result. This Article applies those theories from understanding identity to understanding law.

Part I.A focuses on performativity and how individual practices construct personal identities, a process that relies on repetition, habituation, and normalization. When legal scholars have relied on performance theory to make arguments about the law, they have traditionally focused on this aspect of performativity. But practices do not only create identities; law itself is a product of people, practices, and discourses that determine what we think the law is and should be. This second literature, which focuses on the endogeneity of law, is discussed in Part I.B.

A. The Performativity Thesis

Privacy law practices are what J.L. Austin would call "performatives": they create the reality of privacy law.[24] Judith Butler famously argued that we construct the category of gender by performing it.[25] We dress, speak, have sex, cut our hair, and adopt physical mannerisms associated with, and constitutive of, our gender identities.[26] Performances have the capacity to create social meaning and social categories—that is, our performances are performa*tive*.[27]

The same is true for race and other identities.[28] Relying on this performativity thesis, legal scholars have argued that antidiscrimination law is underinclusive because it elides the many bases of discrimination that are performative of identity, such as hair styles, clothing, and recreational activities.[29] The performativity thesis has also allowed scholars to show how the practices that dominant social norms expect of parents has endogenously influenced family law from the ground up.[30]

B. Repetition and Habit: How Performativity Happens

One way our performances create social categories is through habit. Butler argues that our performative identities "materialize" gradually both from the top down and the ground up; they are the "processes of being acted on" and "the

24. *See* J. L. AUSTIN, HOW TO DO THINGS WITH WORDS 3, 10, 12 (1962). When Austin talked about performances, he was talking about speech: he used the example of saying "I do" during wedding ceremonies as a statement that does more than just express a sentiment. *Id.* at 12–13. Its utterance creates the marriage; the words made the marriage a reality and was, thus, performative. *Id.* This Article is about the performative capacities of practices, not exclusively speech.

25. Judith Butler, *Performative Acts and Gender Constitution: An Essay in Phenomenology and Feminist Theory*, 40 THEATRE J. 519, 524–26 (1988) [hereinafter *Performative Acts*].

26. JUDITH BUTLER, GENDER TROUBLE: FEMINISM AND THE SUBVERSION OF IDENTITY 142–45 (1990).

27. *See* ANDREW PARKER & EVE KOSOFSKY SEDGWICK, *Introduction* to PERFORMATIVITY AND PERFORMANCE 2 (Andrew Parker & Eve Kosofsky Sedwick eds., 1995) (noting that performances can create social meaning to the self and others).

28. *See, e.g.*, Camille Gear Rich, *Performing Racial and Ethnic Identity: Discrimination by Proxy and the Future of Title VII*, 79 N.Y.U. L. REV. 1134, 1158–65, 1171–85 (2004).

29. *See* Devon W. Carbado & Mitu Gulati, *The Fifth Black Woman*, 11 J. CONTEMP. LEGAL ISSUES 701, 710–19 (2001); Nancy Leong, *Identity Entrepreneurs*, 104 CALIF. L. REV. 1333, 1386–87 (2016). The literature on the performance of race is substantial. *See, e.g.*, IAN HANEY LOPEZ, WHITE BY LAW: THE LEGAL CONSTRUCTION OF RACE (Richard Delgado & Jean Stefancic eds., 1996); KENNETH W. MACK, REPRESENTING THE RACE: THE CREATION OF THE CIVIL RIGHTS LAWYER (2012); Ariela J. Gross, *Litigating Whiteness: Trials of Racial Determination in the Nineteenth-Century South*, 108 YALE L.J. 109, 112, 120–22, 132–51 (1998); Anthony V. Alfieri & Angela Onwuachi-Willig, *Next-Generation Civil Rights Lawyers: Race and Representation in the Age of Identity Performance*, 122 YALE L.J. 1484, 1492–1501 (2013); Susan D. Carle, *Conceptions of Agency in Social Movement Scholarship: Mack on African American Civil Rights Lawyers*, 39 L. & SOC. INQUIRY 522, 522 (2014). Kenji Yoshino has likewise argued that identity-based discrimination law insufficiently captures how heteronormative structures force queer people to engage in "covering" performances. KENJI YOSHINO, COVERING: THE HIDDEN ASSAULT ON OUR CIVIL RIGHTS 17–19 (2006).

30. *See* Clare Huntington, *Staging the Family*, 88 N.Y.U. L. REV. 589, 592, 619–27 (2013).

conditions and possibilities for acting."[31] A top-down phase involves social norms acting upon us, where society's strictures try to normalize us to align with its sociocultural histories. Butler suggested that this is the phase in which many of us are influenced to conform to how society says "men" and "women" should speak and act.[32] A bottom-up phase involves the capacity to react to those norms. As Maren Wehrle suggested, we "reproduce . . . norms in ways we might cho[o]se" from the ground up, sometimes in accordance with dominant paradigms and sometimes subverting them directly.[33] For instance, we develop new ways of walking, dressing, thinking, speaking, and behaving. They become typical for us, becoming part of who we are and how we define ourselves to others. Either way, whether we are affirming or disrupting social norms, our performances must be repeated in order to situate ourselves and our actions within society.

Arguably, that happens through a process of habituation. Theories of habit date back to at least Aristotle, who saw habit as essential for promoting virtue; habitually acting morally—that is, repeating over and over again the moral act—constructs a character that has internalized the norms embodied by those moral acts.[34] Similarly, Butler's "materialization" happens precisely because we operate through habit.[35] We generate habits within existing power structures. When a future Olympian learns to swim, for example, they have to practice, drill, and repeat. Eventually, their body becomes habituated to the movements of their arms and legs, holding their breath, and turning their head at specific times during those motions. But they accumulate these habits within certain rules and limits, whether imposed endogenously (they can only hold their breath for so long) or exogenously (they have to stay in their lane in the pool).

We can also acquire new habits that make us excel. In grade school, we learn to write under strict rules: never end a sentence with a preposition; always have a thesis, body, and conclusion; never start a sentence with "and." And yet, as we read more, write more, and learn more, we develop new "ways of being" that may challenge the rules in which we learned to write in the first place. Those new ways of writing become part of who we are as writers, generating our habitual identities from the ground up.

Although repeating performances can affirm identity,[36] habituation can also normalize deviant behaviors as ordinary, commonsense, obvious, and

31. JUDITH BUTLER, NOTES TOWARDS A PERFORMATIVE THEORY OF ASSEMBLY 63 (2015).

32. Maren Wehrle, *'Bodies (That) Matter': The Role of Habit Formation for Identity*, 20 PHENOMENOLOGY & COGNITIVE SCI. 365, 366–67 (2020).

33. *Id.* at 371.

34. ARISTOTLE, NICOMACHEAN ETHICS 1103b1–b5, 1094a20, 1094b6, 1098a15 (Roger Crisp trans., ed., 2000).

35. Wehrle, *supra* note 32, at 380.

36. *See, e.g.*, DAVID I. KERTZER, RITUAL, POLITICS, AND POWER 10 (1988) (noting that performances that accord with an identity to which we want to subscribe offer us "confidence that the

objectively good.[37] Political scandals are good examples of this phenomenon. As psychologists Adam Bear and Joshua Knobe have written, when a politician "continues to do things that once would have been regarded as outlandish, [their] actions are not simply coming to be regarded as more typical; they are coming to be seen as more normal. As a result, they will come to be seen as less bad and hence less worthy of outrage."[38] Similarly, when workers and those around them repeatedly cut corners, break rules, and ignore risks, they stop seeing those behaviors as deviant and come to see them as normal.[39] This happens in our daily lives too: studies show that the more television we watch, the more likely we are to think that watching a lot of television is normal.[40] Therefore, normalization is the confusion of frequency with propriety, nudging us to think that the things we do often are the normal things people do.

The takeaways from this literature are particularly important for privacy law and policy. First, performances are everywhere.[41] As Butler noted, "to understand identity as a *practice* . . . is to understand culturally intelligible subjects"—that is, "understandable" as a result of "a rule-bound discourse that inserts itself in the pervasive and mundane signifying acts of . . . life."[42] It makes sense then to consider privacy law's practices as performances. Second, performances are expressive. Performances "signify[]" identities by demonstrating to the self and to others how performers understand and occupy their roles.[43] This suggests that to understand privacy law, we should look at how privacy is actually performed, not necessarily what is written in the law.[44] Third,

world in which we live today is the same world we lived in before and the same world we will have."); Butler, *Performative Acts*, *supra* note 25, at 523–25.

37. Normalization is cognitive slippage from statistical frequency to moral propriety; it is a process through which common things come to be understood as acceptable, ordinary, and, ultimately, good. *See, e.g.*, Adam Bear & Joshua Knobe, *Normality: Part Descriptive, Part Prescriptive*, 167 COGNITION 25, 26 (2017).

38. Adam Bear & Joshua Knobe, *The Normalization Trap*, N.Y. TIMES (Jan. 28, 2017), https://www.nytimes.com/2017/01/28/opinion/sunday/the-normalization-trap.html [https://perma.cc/JE9J-AD2P].

39. *See* DIANE VAUGHAN, THE CHALLENGER LAUNCH DECISION: RISKY TECHNOLOGY, CULTURE, AND DEVIANCE AT NASA 77–195 (1997) (demonstrating how routinized decisions that violated rules and norms came to be normalized as part of engineering and testing work).

40. *See* Bear & Knobe, *supra* note 37, at 29 (finding the perception of the normal amount of television is based on frequency and what is perceived to be ideal).

41. BUTLER, GENDER TROUBLE, *supra* note 26, at 143–45.

42. *Id.* at 124–25.

43. *Id.*

44. This is closely related to actor-network theory (ANT) in sociological research. ANT posits that the development of knowledge should be understood by analyzing how individuals and groups interact, because the social and natural world is a "continuously generated effect of the webs of relations." John Law, *Actor Network Theory and Material Semiotics*, *in* THE NEW BLACKWELL COMPANION TO SOCIAL THEORY 141 (Bryan S. Turner ed., 2009); *see also* BRUNO LATOUR, REASSEMBLING THE SOCIAL: AN INTRODUCTION TO ACTOR-NETWORK-THEORY 57 (2005) (stating that social scientists wanting to propose alternative metaphysics must "first engage in the world-making activities of those they study"). *But see* Judy Wajcman, *Reflections on Gender and Technology Studies: In What State Is the Art?*, 30 SOC. STUD. SCI. 447, 452 (2000) (criticizing ANT and other Science and

in order to socially construct the law, performances must be widespread, repeated, and pervasive.[45] Butler noted that we are so compelled to engage in and repeat performative acts, because that is how we communicate—both to ourselves and to others—that this is who we are.[46] Finally, pervasive practices can have normalizing effects, pushing us to think that our routinized practices are the normal, appropriate, and normatively good practices. Therefore, the practices of privacy law we should study are those that are routinized and repeated among individuals, companies, and regulators.

C. Performances and Endogenous Law

A related sociolegal research agenda on performative practices focuses less on personal identity than on how practices can socially construct the law from the ground up. For instance, Lauren Edelman used a case study of Title VII of the Civil Rights Act of 1965 to argue that ideas and practices that emerge endogenously from regulated entities themselves can shape the law.[47] Title VII prohibits employment discrimination on the basis of race, sex, and other protected classifications.[48] But lawyers and compliance professionals working inside industry recast their obligations from substance—race and gender equality in the workplace—to procedure—nondiscrimination policies, diversity officers, appeals processes, and other internal organizational structures.[49] This process of "managerialization" transformed corporate symbols of compliance into weapons against claims of discrimination through which companies were able to point to their policies and organizational structures as evidence of fair treatment.[50] And these performances of accountability ultimately defined the law when federal courts not only accepted corporate procedures and practices as evidence of compliance, but also deferred to them as to what the law actually requires.[51] Although she never used the language of the performativity thesis, Edelman nevertheless argued that the practices of Title VII socially constructed the legal category of antidiscrimination law.[52]

Technology Studies theories for ignoring the contributions of marginalized populations, particularly women, in the development of new technology).

45. *See* GOFFMAN, *supra* note 14, at 13–19; BUTLER, *supra* note 16, at 2.

46. BUTLER, *supra* note 16, at 15.

47. LAUREN B. EDELMAN, WORKING LAW 12, 22 (John M. Conley & Lynn Mather eds., 2016).

48. *See generally* Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e–2000e-17.

49. EDELMAN, *supra* note 47, at 30–33.

50. *Id.* at 33–38. *But see id.*, at 6–10 (providing statistical evidence of continued racial and gender inequality in the workplace).

51. *Id.* at 38, 173.

52. Scholars have also relied on the performativity thesis to broaden our understanding of the value of privacy. *See, e.g.*, Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 192–93 (2008) (arguing that privacy captures interests far beyond the unwanted disclosure of personal information because our actions express and define our identities); Scott Skinner-Thompson, *Performative Privacy*, 50 U.C. DAVIS L. REV. 1673, 1697–1708 (2017) (arguing that privacy-enhancing behaviors, such as wearing hoodies in the physical world and using obfuscating technology online, perform expressive resistance to a surveillance society).

The practices of privacy law are having a similar impact. But legal scholars have insufficiently conceptualized privacy law's practices and inadequately understood how those practices have come together to create a raft of new, roughly similar privacy proposals that ultimately benefit data-extractive corporations. The next Section applies the performativity thesis to privacy practices. It demonstrates that the regulatory, corporate, and user practices of privacy law have performatively created what we think privacy law is and should be, a vision reflected in almost every recent proposal for comprehensive privacy law in the United States.

II.
PERFORMATIVITY AND THE SOCIAL PRACTICES OF PRIVACY LAW

Recent proposals for comprehensive privacy law in the United States can be understood as a collection of long-standing practices of regulators, industry, and individuals. Those practices are performative: they construct privacy law by habituating us into thinking those practices are what privacy law is and should be. Departing from the tradition of some other scholars, this Section consciously takes as its starting point the law on the ground—namely, actual practices of regulators, industry, and individuals—rather than the law on the books. Following Butler, who argued that performances predate and construct identity, I argue that privacy law performances construct privacy law, making normative choices along the way.[53] The best evidence of this is that these practices, many of which predate the GDPR and the CCPA, have come together to form the latest proposals for omnibus privacy laws in the United States, both at the federal and state levels. The remarkable uniformity of these statutes—they all propose to codify many of the same practices—speaks directly to the power of performances in shaping the law.

A. Regulatory Practices

There are two primary privacy enforcers in the United States—the Federal Trade Commission (FTC, or the Commission) and state attorneys general (AG).[54] They are empowered to write rules and enforce the law. But in practice, things are different. Rather than holding industry to account, regulators have traditionally positioned themselves as industry partners in order to gain corporate buy-in.[55] They also settle rather than litigate almost all claims. The FTC's

53. BUTLER, *supra* note 26, at 142–45.

54. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 760 (2016) [hereinafter Citron, *Privacy Policymaking*] (focusing on state AGs); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 583 (2014) (focusing on the FTC). Notably, the Consumer Financial Protection Bureau, particularly under the leadership of Director Rohit Chopra, has taken a greater interest in protecting consumers from predatory data practices in the financial sector.

55. There are indications that this is changing, especially under the leadership of FTC Chair Lina Khan, who, after her appointment to the post by President Biden, has arguably taken a more

strength as a regulator may ebb and flow with new appointments and new political majorities, but even under the leadership of Chair Lina Khan, the FTC still explicitly relies on industry to perform regulatory tasks. These practices are performative of privacy law: industry input and compromise have been built into most recent privacy proposals.

1. Regulator as Partner

The FTC and state AGs have long held meetings with industry representatives to persuade them to self-regulate and to solicit input on how to govern data collection.[56] The FTC meets with industry representatives regularly to "monitor the marketplace."[57] The Commission has also published reports on online profiling, e-commerce, and consumer debt collection, among other issues, only after meeting with, and receiving significant input from, industry representatives.[58] As Danielle Citron has shown, state AGs have established task forces with representatives from business and advocacy groups to try to reach consensus on best practices.[59] They have also brought companies together to determine what those best practices should be and to hear how companies are approaching compliance, often adopting those compliance measures as recommendations.[60] These consultations are widespread and routine, and they

aggressive posture toward corporate accountability. *See, e.g.*, Russell Brandom, *Federal Trade Commission Expands Antitrust Powers in Chair Lina Khan's First Open Proceeding*, VERGE (July 1, 2021), https://www.theverge.com/2021/7/1/22559131/ftc-open-meeting-antitrust-chair-lina-khan-sherman-act-powers [https://perma.cc/P9JX-4PTW].

56. *See* Citron, *Privacy Policymaking*, *supra* note 54, at 763–64; Solove & Hartzog, *supra* note 54, at 598–99.

57. FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 48 (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [https://perma.cc/436G-JU9W].

58. *E.g.*, FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS (2000), https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf [https://perma.cc/KP3C-PSHN]; FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS, PART 2 RECOMMENDATIONS (2000), https://www.steptoe.com/a/web/564/934.pdf [https://perma.cc/6Y3V-ZN6K]; FED. TRADE COMM'N, REPAIRING A BROKEN SYSTEM: PROTECTING CONSUMERS IN DEBT COLLECTION LITIGATION AND ARBITRATION ii (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-staff-report-repairing-broken-system-protecting/debtcollectionreport.pdf [https://perma.cc/54ZW-78HT]; *see also* Mozelle W. Thompson, *The Challenges of Law in Cyberspace—Fostering the Growth and Safety of E-Commerce*, 6 B.U. J. SCI. & TECH. L. 9, ¶¶ 1, 8–10 (1999) (discussing the FTC's interactions with industry leaders and how it views its role).

59. Citron, *supra* note 54, at 759.

60. *Id.* at 760.

date as far back as at least 2012, and perhaps earlier, long before the GDPR or the CCPA.[61]

Consultations with industry have normalized privacy regulators as partners or allies of industry. Jon Leibowitz, former FTC Chair, Davis, Polk, & Wardwell LLP partner, and co-chair of the industry-funded 21st Century Privacy Coalition, said that "promot[ing] . . . business innovation" is one of the FTC's goals and it "motivates industry" to achieve it.[62] Another former FTC Commissioner, Julie Brill, recently said that privacy regulators can use compliance safe harbors "to work with companies" and to "help them understand what other companies are doing."[63] Regulators and their staffs also present themselves as wanting to help facilitate innovation,[64] provide clarity about rules to guarantee predictability,[65] and ensure industry that they are committed to a regulatory "light-touch."[66] Indeed, as one assistant state AG told Professor Citron, "[w]e want companies to tell us how we can be clear about what we expect and how that clarity can help them satisfy the law and innovate."[67]

This normalized practice has made its way into new privacy statutes. Recent privacy proposals explicitly require the FTC to consult with industry to develop the rules and regulations industry must follow. For instance, the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act) requires the FTC to develop rules in consultation with "a professional standards body" made up of large technology companies to define the terms under which industry can collect children's data.[68]

---

61. *Id.* at 759–60. Professor Citron's research makes clear that regulators engaged in these practices by 2012. Given that they were explaining their offices' practices by 2012, it is reasonable to assume that some of these offices were working directly with industry before then.

62. *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers*, FED. TRADE COMM'N (Dec. 1, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers [https://perma.cc/6JEK-KLXH] (quoting FTC Chair Leibowitz as including "promot[ing] . . . business innovation" as one of the goals of the report and the FTC).

63. Univ. of Wash., *Privacy Redress Options Workshop*, CAL. EMP. LAWS. ASS'N (Dec. 10, 2020), https://medius.studios.ms/Embed/video-nc/CELAReadress-2020 [https://perma.cc/NU68-TK8T] (featuring comments by Julie Brill).

64. Facilitating innovation is built into the FTC's work. *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE iv, 1 (2010) (noting that the goal of several FTC convenings was to develop a framework for privacy that facilitates technological innovation); FED. TRADE COMM'N, TO PROMOTE INNOVATION: THE PROPER BALANCE OF COMPETITION AND PATENT LAW AND POLICY (2003), http://www.ftc.gov/os/2003/10/innovationrpt.pdf [https://perma.cc/QE68-6FN3] (proposing policy decisions based on what would facilitate innovation and the development of new technologies).

65. *See* Citron, *supra* note 54, at 760.

66. Ajit Pai, *The Future of Internet Freedom*, FED. TRADE COMM'N (Apr. 26, 2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0427/DOC-344590A1.pdf [https://perma.cc/5WPC-NVJ4]; *see also* COHEN, *supra* note 9, at 187 (quoting Jodi L. Short, *The Paranoid Style in Regulatory Reform*, 63 HASTINGS L.J. 633, 635 (2012) (referring to the "paranoid" style of regulation)).

67. Citron, *supra* note 54, at 760.

68. SAFE DATA Act § 206(d)(3)(D).

Elsewhere, the proposal authorizes the FTC to approve voluntary consensus standards and certification programs that companies developed on their own or in consultation with FTC staff.[69] The Privacy Bill of Rights also requires the FTC to reach out to companies and provide compliance guidance in line with "recognized industry practices."[70] And the Consumer Online Privacy Rights Act (COPRA) authorizes the FTC to accept data security standards issued by the National Institute of Standards and Technology,[71] an arm of the U.S. Department of Commerce, which works with industry to "promote U.S. innovation and competitiveness."[72] Similarly, in many states, AGs are required by statute to consult with companies before bringing enforcement actions.[73] New state proposals require AGs to write clarifying rules only after consultation with business.[74] And those rules also must "take into account the burden on the business."[75] In short, industry input has moved from practice to law on the books.

2. Compromises and Settlements

In addition to meeting with companies to develop rules and best practices, regulators generally resolve their privacy enforcement actions through consent decrees rather than litigation.[76] Likewise, state AGs sign informal assurances of voluntary compliance (AVCs) with companies under investigation.[77] Consent decrees, like AVCs, are agreed-upon settlements; they function more like contracts than court orders.[78] This practice has become part of privacy law.

Settlements are routine. Only three of the FTC's 271 reported privacy and security enforcement actions since 1998—twenty years before the GDPR went into effect—ended in a judicial opinion from a federal court.[79] The rest ended in

69. *See id.* at § 404(a).

70. Privacy Bill of Rights § 13(a)(3).

71. COPRA § 107(c).

72. *About NIST*, NAT'L INST. STANDARDS TECH.: U.S. DEP'T OF COM. (Jan. 11, 2022), https://www.nist.gov/about-nist/our-organization/mission-vision-values [https://perma.cc/K7KX-9XQU].

73. Citron, *supra* note 54, at 761.

74. CCPA § 1798.185(a).

75. *Id.* at 1798.185(a)(7); *see, e.g.*, H.R. 784, 2020 Gen. Assemb., 441st Sess. § 14-4211(7) (Md. 2020).

76. *See* Solove & Hartzog, *supra* note 54, at 606, 610.

77. Citron, *supra* note 54, at 761 ("States . . . often eschew formal adjudication for informal agreements that close investigations").

78. United States v. Armour & Co., 402 U.S. 673, 681 (1971) ("Consent decrees are entered into by parties to a case after careful negotiation has produced agreement on their precise terms."); United States v. ITT Cont'l Baking Co., 420 U.S. 223, 238 (1975) ("[A] consent decree . . . is to be construed for enforcement purposes basically as a contract.").

79. These numbers were based on a search on the FTC's website, which categorizes all of its enforcement actions. *See Legal Library: Cases and Proceedings*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/advanced-search [https://perma.cc/SB3X-WKXH] (searching for "privacy and security" cases under "Consumer Protection Topics"). The number of total FTC privacy cases is far higher than 271, which does not capture the many investigations that are dropped or end with negotiations before the complaint stage. The three litigated cases include: Fed.

consent orders and default judgments.[80] These settlements generally follow the same script: companies under investigation do not admit fault or assume responsibility for deceptive business practices, but they nevertheless pay fines, amend privacy notices, and promise to stop deceptive practices or adopt new practices.[81] State AGs frequently enter into individual and multi-state AVCs with companies.[82] Indeed, Professor Citron found no fully litigated AG enforcement actions related to privacy.[83]

These settlements are also expressive. Consent decrees convey messages to regulated entities and the public about how the FTC understands its role as a regulator. As Daniel Solove and Woodrow Hartzog have noted, privacy lawyers "parse and analyze the FTC's settlement agreements, reports, and activities as if they were pronouncements by the Chairman of the Federal Reserve."[84] Like other areas of law, FTC consent decrees have expressive value that influences norms on the ground.[85] They express what kinds of privacy practices the FTC thinks are appropriate and what practices are unfair, deceptive, or misleading. Even those commissioners in dissent try to influence corporate practices and the course of FTC actions in their dissents.[86] The FTC also announces consent decrees with fanfare, press releases, quotations from commissioners about corporate accountability and consumer welfare, and a media blitz about any fines it imposed.[87] AGs, eager to burnish political bona fides, have presented their

Trade Comm'n v. Accusearch, Inc., 570 F.3d 1187, 1193 (10th Cir. 2009) (endorsing the FTC's power to bring cases under its "unfair or deceptive" practices authority); Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 602 (D. N.J. 2014) (finding that the FTC properly pled and had authority to regulate defendants' failure to maintain reasonable and appropriate data security); LabMD Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1229 (11th Cir. 2018) (limiting the FTC's power to require companies to take "reasonable" security measures).

80. Solove & Hartzog, *supra* note 54, at 606, 610.

81. *Id.* at 608–19.

82. Citron, *supra* note 54, at 761.

83. *See id.* at 761–63.

84. Solove & Hartzog, *supra* note 54, at 585.

85. Law has expressive value that influences public perceptions of what is right and wrong. *See, e.g.*, Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009); Elizabeth S. Scott, *Social Norms and the Legal Regulation of Marriage*, 86 VA. L. REV. 1901 (2000); Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2022 (1996).

86. *See, e.g.*, Fed. Trade Comm'n, Office Comm'n Rohit Chopra, Dissenting Statement by Commissioner Rohit Chopra: *In re Facebook, Inc.*, Commission File No. 1823109 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf [https://perma.cc/F46U-2C48].

87. Consider, for example, the FTC's media campaign when it sued Facebook for "illegally maintaining its personal social networking monopoly through a years-long course of anticompetitive conduct." *See* Fed. Trade Comm'n, *FTC Sues Facebook for Illegal Monopolization* (Dec. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization [https://perma.cc/E73G-2JBG]. Press associated with the lawsuit has quoted FTC staff and several of the 48 AGs that joined the lawsuit. *See, e.g.*, Cecilia Kang & Mike Isaac, *U.S. and States Say Facebook Illegally Crushed Competition*, N.Y. TIMES (Dec. 9, 2020), https://www.nytimes.com/2020/12/09/technology/facebook-antitrust-monopoly.html [https://perma.cc/7Y3V-DVG3] (quoting New York AG Letitia James and Ian Conner, the head of

informal agreements with companies as accomplishments on behalf of the privacy rights of state residents.[88] They also discuss their settlements with the public in order to persuade companies to change their behavior, relying on what Citron called their "privacy-norm entrepreneurship."[89]

Scholars have also referred to these orders as a privacy "common law," constructing law case-by-case like a state court constructing tort, contract, or property law.[90] Even more notable, however, is the way in which settlement practices have become part of recent privacy law proposals. Some states require their AGs to settle with those companies under investigation before even being allowed to pursue litigation.[91] Other states explicitly envision their AGs relying on AVCs or Assurances of Discontinuance even if the statutes do not require it.[92] The CCPA explicitly envisions its AG settling enforcement actions.[93] Hawai'i's Office of Consumer Protection would enforce that state's privacy law, but the Office has no history of litigating privacy enforcement actions.[94]

This is nothing new. The Administrative Conference of the United States long ago found that federal agencies "resolve the great majority of civil money penalty cases without reaching the stage of formal administrative adjudication or court collection proceeding."[95] The U.S. Department of Justice has also noted that "even where formal proceedings are fully available," as in the case of most new privacy proposals, "informal procedures constitute the vast bulk of administrative adjudication and are truly the lifeblood of the administrative process."[96] Scholars have found the same to be true of the FTC and state AGs in the last forty years.[97] Codifying the availability of enforcement actions will do nothing to change this practice and may even entrench it further.

---

antitrust enforcement at the FTC); Tony Romm, *U.S., States Sue Facebook as an Illegal Monopoly, Setting Stage for Potential Breakup*, WASH. POST (Dec. 9, 2020), https://www.washingtonpost.com/technology/2020/12/09/facebook-antitrust-lawsuit/ [https://perma.cc/XNW7-3HND] (quoting FTC Chairperson Joe Simons and AG James).

88. *See* Citron, *supra* note 54, at 750.

89. *Id.* at 806.

90. Solove & Hartzog, *supra* note 54, at 619.

91. Citron, *supra* note 54, at 761.

92. Minnesota H.F. 1492 § 325O.10 (empowering the AG to bring an enforcement action in accordance with Minn. Stat. Ann. § 8.31, which, in subdivision 2a, explicitly allows the AG to rely on an "assurance of discontinuance of any act or practice the attorney general deems to be in violation of the laws").

93. CCPA § 1798.155(c).

94. Hawaii S.B. § 487J-5; *see also Office of Consumer Protection Blog*, HAW. DEP'T OF COM. & CONSUMER AFFS., http://cca.hawaii.gov/blog/category/divisions/ocp/ [https://perma.cc/J6H6-U47G] (reporting only settlements with investigated companies).

95. ADMIN. CONF. OF THE U.S., AGENCY ASSESSMENT AND MITIGATION OF CIVIL MONEY PENALTIES 2 (1979).

96. DEAN ACHESON, FRANCIS BIDDLE, RALPH F. FUCHS, LLOYD K. GARRISON, D. LAWRENCE GRONER, HENRY M. HART, CARL MCFARLAND, JAMES W. MORRIS, HARRY SHULMAN, E. BLYTHE STATSON, ARTHUR T. VANDERBILT & WALTER GELLHORN, FINAL REPORT OF THE ATTORNEY GENERAL'S COMMITTEE ON ADMINISTRATIVE PROCEDURE 35 (1941).

97. Solove & Hartzog, *supra* note 54, at 619–27; Citron, *supra* note 54, at 758–63.

3. Industry as Self-Regulator

In addition to tinkering with corporate notices, regulators now require companies to develop internal organizational structures for data governance.[98] This began in the United States in 2011, when Google agreed to establish a "comprehensive privacy program" designed to assess the privacy risks of new products and to protect the privacy of collected information.[99] This requirement then became the norm.[100] State AGs soon followed suit. After Google collected data from unsecured wireless networks through its Street View cars, thirty-eight states and the District of Columbia pushed the company to agree to build a privacy program, designate a privacy coordinator, train employees, and create new internal policies and procedures on privacy practices.[101] In *People v. Payday Loan Store of Illinois*, the state required the company to provide employee training and adopt new internal privacy protocols.[102] Similarly, in *State v. Villareal*, Texas required a company to develop comprehensive security programs.[103] And in *In re HealthNet*, New York settled an investigation by requiring the company to train staff, develop new internal programs, and conduct security audits.[104] The list goes on.[105] Therefore, it has become routine for regulators to shift the burdens of ongoing monitoring and governance to industry itself.

A central piece of privacy governance is the audit. Indeed, most FTC privacy consent decrees have required companies to conduct biennial "assessments" to ensure they are complying with the order.[106] Companies identify, hire, and verify the qualifications of the assessor themselves.[107] These audits are performances, and cynical ones at that. They use boilerplate

98. *See infra* Part II.B for a more detailed discussion of the performativity of compliance practices.

99. Google Consent Decree, *supra* note 12, at 4.

100. *See* Solove & Hartzog, *supra* note 54, at 617–18.

101. Press Release, Off. of the Att'y Gen. of Conn., *Attorney General Announces $7 Million Multistate Settlement with Google over Street View Collection of WiFi Data* (Mar. 12, 2013), https://portal.ct.gov/AG/Press-Releases-Archived/2013-Press-Releases/Attorney-General-Announces-7-Million-Multistate-Settlement-With-Google-Over-Street-View-Collection-o [https://perma.cc/HUL3-L3ZX].

102. Notice of Dismissal by Agreement, No. 10CH44962 (Ill. Cir. Ct. Oct. 3, 2012) (requiring employee training and adoption of new internal policies).

103. Order Granting Permanent Injunction, No. 2010-CI-13625 (Tex. Dist. Ct. Aug. 26, 2010) (agreeing that the company would adopt comprehensive security program).

104. Citron, *supra* note 54, at 781 (citing Assurance of Voluntary Compliance, *In re* Health Net, No. 10-040 (Office of the Att'y Gen. N.Y. Aug. 2, 2010)) (agreeing to trainings, audits, and comprehensive programs).

105. For a comprehensive discussion of state AGs entering into AVCs with information industry companies, please see Citron, *supra* note 54, at 761–62, 769–71, 776, 781, 806–09.

106. Solove & Hartzog, *supra* note 54, at 618.

107. *See, e.g.*, Decision and Order, Facebook, Inc., 154 F.T.C. 1 (2012) (requiring Facebook to hire a third-party auditor).

language.[108] They follow a standard script: the company hires an outside assessor who comes in every two years to ask the same standard set of questions.[109] All of them are answered by executive attestation, meaning that an assessor concludes that a company is complying with an FTC order based solely on the assurances of corporate executives.[110] For instance, Google's assessor found that the company's new privacy program met FTC requirements, but only appended the company's privacy program statement as proof.[111] Uber's assessors did not complete an independent investigation, either; they relied solely on "data security policies" and interviews with executives to conclude that the company was meeting its requirements.[112] Therefore, assessments are little more than pre-written scripts on the front stage, complete with dialogue from defined actors and repeated over and over again like a long-running show.

Despite this, assessments are nevertheless performative: they socially construct privacy regulation. David Vladeck, a former Director of the FTC's Consumer Protection Bureau, has called assessments an "important" part of the FTC's work.[113] In formal response to public comments about its 2012 settlement with Facebook, the FTC told many commentators that more robust audits were unnecessary: "The Commission believes that the biennial privacy assessments described above will provide an important means to monitor Facebook's compliance with the order."[114] Assessments are now routine parts of FTC

108. Chris Jay Hoofnagle, *Assessing the Federal Trade Commission's Privacy Assessments*, 14 IEEE SEC. & PRIV. 58, 61 (2016).

109. This standard script includes the following questions: "Have they appointed someone responsible for looking at privacy? Are they doing risk assessments? Have they trained employees? Are they doing continual testing to make sure they're closing loopholes? Do they have service providers that handle consumer data; do they specify privacy protections in the contracts with them?" Kashmir Hill, *So, What Are These Privacy Audits that Google and Facebook Have to Do for the Next Twenty Years*, FORBES (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/#3bbf76805000 [https://perma.cc/Q3XM-RWJP].

110. Megan Gray, *Understanding and Improving Privacy "Audits" Under FTC Orders*, STAN. L. SCH. CTR. INTERNET & SOC'Y 6 (Apr. 18, 2018), https://cyberlaw.stanford.edu/files/blogs/white%20paper%204.18.18.pdf [https://perma.cc/A4KH-C5P7].

111. *Id.* at 6 n.15; *see also EPIC FOIA Uncovers Google's Privacy Assessment*, ELEC. PRIV. INFO. CTR. (Sept. 28, 2012), https://epic.org/2012/09/epic-foia-uncovers-googles-pri.html [https://perma.cc/6BKU-9AU2].

112. Evan Schuman, *Uber Shows How Not to Do a Privacy Report*, COMPUT. WORLD (Feb. 5, 2015), https://www.computerworld.com/article/2880596/uber-shows-how-not-to-do-a-privacy-report.html [https://perma.cc/EH23-JNMP].

113. Jessica Leber, *The FTC's Privacy Cop Cracks Down*, MIT TECH. REV. (June 26, 2012), https://www.technologyreview.com/s/428342/the-ftcs-privacy-cop-cracks-down/ [https://perma.cc/28YZ-GDT6].

114. *E.g.*, Letters to Commenters, *In re* Facebook, Inc., FTC File No. 092 3184, https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmbltrs.pdf [https://perma.cc/79GS-YL24] (Argentar letter).

practice. As such, privacy professionals and privacy lawyers expect assessments as a matter of course.[115]

These audits have moved from practice to statutes, as well. Minnesota would require data collectors to audit their own privacy programs and those of their partners and vendors.[116] COPRA tells companies to hire an external auditor to assess their privacy practices.[117] The Mind Your Own Business Act (MYOBA) requires companies to complete annual attestations of compliance with written statements and affirmations from company executives and the CPO.[118] The Privacy Bill of Rights mandates regular audits of internal privacy and security practices, completed either internally or by an independent assessor.[119]

These practices open doors for industry to bring its experts to the table and to influence its own regulatory context. As the next Section describes, recent proposals would also codify many other organizational practices that predate the GDPR, including internal offices, policies, and programs that document ongoing compliance.

B. Compliance and Internal Structures

Traditional privacy law in the United States began with regulators disclaiming any interest in privacy regulation.[120] As a result, data collectors voluntarily posted privacy and data use notices.[121] That practice was performative of privacy law: eventually, the FTC, several federal laws, and state laws like the California Online Privacy Protection Act codified these practices into law.[122] In this way, the routinized performance of writing and posting privacy policies created what policymakers and industry thought privacy law should be. A similar process is happening now, but instead of codifying mere notice, proposals for omnibus U.S. privacy laws would also codify a series of

115. *See* Solove & Hartzog, *supra* note 54, at 618.

116. H.R. 3936, 91st Leg., 91st Sess. (Minn. 2020) § 25O.04(d)(3).

117. COPRA § 108(b)(2).

118. MYOBA § 5(a)(1)–(b)(1).

119. Privacy Bill of Rights § 13(b)(3)(A)–(B).

120. *See* MARTHA K. LANDESBERG & LAURA MAZZARELLA, FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 12–14 (1999); *Consumer Privacy on the World Wide Web: Hearing Before the H. Subcomm. on Telecom's, Trade, & Consumer Protection of the H. Comm. on Commerce*, 105th Cong., 2d Sess. (1998) (prepared statement of the Fed. Trade Comm'n by Robert Pitosfky, Chairperson) (advocating for self-regulation); *Self-Regulation and Privacy Online: Hearing before the S. Subcomm. on Comm's of the Comm. on Com., Sci., & Transp.*, 106th Cong., 1st Sess. 4 (1999) (prepared statement of the Fed. Trade Comm'n by Robert Pitofsky, Chairperson) (also advocating for self-regulation).

121. Solove & Hartzog, *supra* note 54, at 590–95.

122. *E.g.*, CAL. BUS. & PROF. CODE § 22575 (West 2020); Children's Online Privacy Protection Act, 15 U.S.C. § 6502(b)(1)(A)(i) (requiring websites geared toward children to disclose what data they collect—whether obtained actively or passively—how it will be used, whether it will be shared, and how to delete or opt out of data collection); Gramm-Leach-Bliley Act, 15 U.S.C. § 6803(a)(1)–(2); 16 C.F.R. § 313.6(a)(3), (6) (imposing similar requirements on certain financial institutions).

internal governance practices that some industry players innovated since long before the GDPR. These practices have again constructed the category of privacy law. But this time, instead of constructing a self-regulatory regime, they have built one characterized by managerialized compliance.

1. Managerialized Compliance

Managerialism is the "infusion of managerial or business values and ideas into law."[123] Many recent proposals for comprehensive privacy law in the United States explicitly envision that compliance professionals—privacy professionals, privacy lawyers, and other compliance experts—will bring the law into their organizations, translate its requirements for their bosses, and implement it throughout the company. But along with that shift in responsibility comes the "reconceptualization of law so that it is more consistent with general principles of good management."[124] Theoretically, managerialism is agnostic as to legal values; good management is not necessarily in conflict with the underlying purposes of social legislation. But managerialism does make regulated entities themselves the intermediaries between the laws on the books and the people those laws are meant to protect. That gives industry the power to define what the law means in practice.

Managerialism can, therefore, undermine what scholars call collaborative governance. Collaborative governance is an approach to regulation that relies on a partnership between public authorities and private actors to achieve regulatory goals.[125] Collaborative governance, at its best, is "a highly tailored, site-calibrated regulatory system that aims to pull inputs from, obtain buy-in from, and affect the internal institutional structures and decision-making heuristics of the private sector" while maintaining popular legitimacy and achieving better social welfare outcomes.[126] In the privacy space, collaborative governance is meant to supplement privacy's traditional reliance on transparency, notice, and consent.[127]

123. EDELMAN, *supra* note 47, at 25.

124. *Id.* at 25–26; *see* COHEN, *supra* note 9, at 144–45.

125. Kaminski, *supra* note 4, at 1559. For a more comprehensive definition of collaborative governance, see Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 21–33 (1997); Orly Lobel, *New Governance as Regulatory Governance*, *in* THE OXFORD HANDBOOK OF GOVERNANCE 65–67 (David Levi-Faur ed., 2012); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 371–76 (2004).

126. Kaminski, *supra* note 4, at 1560. Other scholars have argued in favor of collaborative governance approaches to privacy law. *See, e.g.*, KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND 12–13 (2015) (suggesting that the public-private partnerships created by privacy law provide space for CPO innovation); Dennis D. Hirsch, *Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law*, 2103 MICH. ST. L. REV. 83, 99–102; W. Nicholson Price II, *Regulating Black-Box Medicine*, 116 MICH. L. REV. 421, 465–71 (2017).

127. Kaminski, *supra* note 4, at 1557–58. *See also* Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for*, 16 DUKE

In collaborative governance, the government plays the role of a "backdrop threat" that encourages private sector engagement, convenes regulated entities and civil society together, certifies compliance protocols, and, if necessary, enforces the law when things go awry.[128] Private actors develop the systems of compliance on their own with the government as a top-down regulator.[129] To ensure accountability, collaborative governance relies on negotiated settlements, safe harbors, codes of conduct, audits, informal delegations of interpretive authority to private actors, impact assessments, ongoing self-monitoring, and incentives for private ordering in the public interest.[130] The goal is to keep sufficient flexibility in the legal system so regulated entities will want to participate and to ensure companies do so for the public good.[131]

Proponents see several benefits to the collaborative model. Public-private partnerships bring private sector expertise to governance, which proponents believe especially necessary in the complex and highly digitized information economy.[132] Technological development also moves fast, so the collaborative governance model offers "an ongoing, iterative system of monitoring and compliance" in place of the long, drawn-out process of administrative rulemaking.[133] The model also enhances industry buy-in and perceived legitimacy by giving regulated entities a seat at the table and enabling them to help regulators craft workable solutions.[134] In short, there are reasons collaborative governance is so popular.

Proponents also recognize the dangers of the approach. Collaborative governance requires substantive outer limits to prevent everything—including protecting basic human rights—from boiling down to an ongoing negotiation with a profit-seeking corporation.[135] For collaborative governance to work, rights must be clearly defined and judicial review, in addition to large fines, may be necessary to constrain corporate actions at the margins.[136] As the next Section shows, scholars are right to worry. Managerialism has taken hold in practice, undermining privacy law in the process.

2. Performative Managerial Practices

Research conducted inside the information industry demonstrates that privacy leaders, privacy lawyers, and other professionals have long built internal

L. & TECH. REV. 18, 74–75 (2017) (noting how individuals lack the technical skill to identify information economy abuses and are limited by cognitive biases that make exercising rights difficult).

128. Kaminski, *supra* note 4, at 1561.
129. *See id.* at 1561–62.
130. *Id.* at 1564–66.
131. *Id.* at 1567.
132. *See* BAMBERGER & MULLIGAN, *supra* note 126, at 12–13.
133. Kaminski, *supra* note 4, at 1562.
134. *See id.*
135. *Id.* at 1577.
136. *Id.* at 1579.

corporate structures as part of their privacy compliance work. Based on interviews with several CPOs regarded as leaders in the field, Kenneth Bamberger and Deirdre Mulligan found that privacy professionals created a "company law" of privacy to fill in the gaps left open by privacy law on the books.[137] These professionals drafted internal rules for data processing in accordance with the E.U.'s 1995 Privacy Directive.[138] They also conceptualized privacy in terms of risk management and developed processes for assessing and documenting that risk.[139] Companies created new privacy offices and hired staff.[140] They started training their employees on privacy and security, designated some of them as privacy officers, and put them to work building new procedures and setting new policies.[141] Audits of privacy practices were part of the corporate routine as early as 2009.[142] This suggests that privacy practitioners were building internal organizational structures long before the GDPR.

Those practices have socially constructed privacy law. FTC consent decrees now require companies to create a "comprehensive privacy program,"[143] which includes hiring staff, situating staff inside organizational hierarchies, completing risk analyses for new products, and developing privacy trainings.[144] Companies also have to conduct biennial assessments of that program.[145] Ten proposals for comprehensive U.S. privacy law would codify some or all of these requirements.[146]

---

137. BAMBERGER & MULLIGAN, *supra* note 126, at 65; Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 269–70 (2011).

138. Bamberger & Mulligan, *supra* note 137, at 265, 270; *see* Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 40 [hereinafter Privacy Directive].

139. Bamberger & Mulligan, *supra* note 137, at 271–72; *see* Kenneth Bamberger & Deirdre Mulligan, *Catalyzing Privacy: New Governance, Information Practices, and the Business Organization*, 33 L. & POL'Y (2011).

140. Bamberger & Mulligan, *supra* note 137, at 261–63.

141. *Id.* at 260–63.

142. *Id.* at 263. There is evidence, however, that this work did not have any material effect on data-extractive design. *See* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUSTON L. REV. 659, 678–701 (2018).

143. Google Consent Decree, *supra* note 12.

144. Solove & Hartzog, *supra* note 54, at 617–18, 673.

145. *Id.* at 618–19; Citron, *supra* note 54, at 761–62.

146. *E.g.*, CCPA § 1798.135(a)(3) (training); H.R. 5603, 101st Gen. Assemb., Reg. Sess. § 40(6) (Ill. 2020) (training); H.R. 784, 2020 Gen. Assemb., 441st Sess. § 14-4204(E) (Md. 2020) (training); H.R. 3936, 91st Leg., 91st Sess. § 14-4204(E) (Minn. 2020) § 325O.04(b)(1) (organizational measures to assist in compliance); H.R. 3936 § 325O.04(d)(3) (conduct audits of processors); S. 176, 54th Leg., 1st Sess. § 6 (N.M. 2019) (training); H.R. 4390, 86th Leg., Reg. Sess. § 541.053 (Tex. 2019) (data security program); H.R. 4390 § 541.058 (privacy accountability program to assess risk); COPRA § 107(b)(4) (training), § 201 (internal privacy program with certification by executives), § 202(a)–(b)(1) (privacy and security officers), § 202(b) (comprehensive privacy program), § 202(b)(2) (annual assessments of program); MYOBA §§ 6(a)(7) (biennial review), 7(b)(1)(A)–(B) (establish reasonable privacy policies and internal organizational technical measures), § 7(b)(C) (designating privacy coordinators); Privacy Bill of Rights §§ 13(a)(1) (internal practices to ensure confidentiality of information), 13(b)(3) (audits of privacy programs in place), 14 (designate privacy and security officer);

Indeed, new proposals would codify many of these internal corporate practices, including trainings, recordkeeping, and privacy risk assessments.[147] Four proposals state that companies must hire a CPO or designate a privacy officer.[148] Several laws require companies to create "organizational" measures, like comprehensive privacy programs, to ensure compliance.[149] Other internal governance measures include regular audits of processors, vendors, and the privacy programs themselves.[150]

Some requirements in these proposals are new. A few proposals ask industry to develop internal processes for ensuring that third-party vendors comply with the law,[151] certify compliance with executive attestations,[152] and develop standard disclosures.[153] A bill in Minnesota would require an internal appeals process, and five other state laws require independent tests and annual impact assessments of automated processing or facial recognition.[154] The Mind Your Own Business Act (MYOBA) would require companies to develop an internal process to track opt-out requests of consumers with whom they are not in a direct relationship but whose data they nevertheless hold.[155] And the SAFE DATA Act calls on a "professional standards body" to write its own rules that,

---

SAFE DATA Act §§ 204(a) (establishing "reasonable administrative" measures), 301(a) (designating a CPO and other responsible employees).

147. Provisions requiring trainings include the following: S. 1614, 54th Leg., 2d Reg. Sess. § 18-701(L)(5) (Ariz. 2020); CCPA § 1798.135(a)(3); S. 418, 30th Leg., Reg. Sess. § 487(J)–(H)(6) (Haw. 2019); H.R. 5603 § 40(6); H.R. 784 § 14-4204(E); H.R. 1656, 2020 Gen. Assemb., 441st Sess. §§ 1656, 14–4204(E) (Md. 2020); S. 176 § 6; COPRA § 107(b)(4). Statutory provisions requiring record-keeping include the following: S. 418 § 487(J)–(H) (requiring lists); MYOBA § 6(a)(2); Online Privacy Act § 202(b). Statutes requiring PIAs include: S. 2263, 101st Gen. Assemb., 1st Reg. Sess. § 30 (Ill. 2019); S. 2330, 101st Gen. Assemb., 1st Reg. Sess. § 35(l) (Ill. 2020); H.R.3936 § 325O.08; H.R. 4390 § 541.058 (accountability program to assess risk); H.R. 473, 2020 Gen. Assemb., 2020 Sess. § 59.1-576 (Va. 2020); S. 5062, 67th Leg., 2021 Reg. Sess. § 109 (Wash. 2021); MYOBA § 7(b)(G)–(H); SAFE DATA § 107(a)(1), (b); *see also* Kaminski, *supra* note 4, at 1603–05 (noting that PIAs are internal documents meant to help balance risks and benefits and intended to keep privacy front of mind during design).

148. *See* COPRA § 202(a)(1)–(2); MYOBA § 7(b)(C); Privacy Bill of Rights § 14; SAFE DATA Act § 301(a)–(b).

149. *See, e.g.*, H.R. 3936 § 325O.04(b)(1) (processor required to have organizational measures to assist data controller with compliance); COPRA §§ 201, 202(b) (comprehensive privacy program and internal reporting structure ensuring that privacy professionals are involved and responsible for compliance); MYOBA §§ 6(a)(7) (biennial review of information provided to consumers for exercising opt out requests), 7(b)(A)–(B); Privacy Bill of Rights § 13(a)(1).

150. H.R. 3936 § 325O.04(d)(3); COPRA § 202(b)(2); MYOBA § 5(a)(1); SAFE DATA Act § 204(a).

151. H.R. 4390 § 541.059; COPRA § 203(c)(1)(A)–(B); Data Care Act § 3(b)(3)(C); MYOBA § 6(a)(8); Privacy Bill of Rights § 10.

152. COPRA § 201; MYOBA § 5(a)(1).

153. MYOBA § 6(a)(10).

154. H.R. 3936 § 325O.05 subdiv. 3 (requiring internal appeals process); H.R. 3936 § 325O.085(a) (independent tests of facial recognition); COPRA § 108(b); MYOBA § 7(b)(G); Privacy Bill of Rights § 13(b)(3); SAFE DATA Act § 206(b)(4).

155. MYOBA § 6(a)(4).

if followed, would constitute compliance with the law.[156] But these new requirements are in line with the old. For some time, privacy law has relied on internal corporate governance structures for ongoing monitoring and compliance. Bamberger and Mulligan found that those practices have normalized themselves, and now, new privacy statutes are based on them. That is the essence of performativity: legal categories defined by behaviors on the ground that express what privacy law is and should be.

C. Exercising Rights of Control

Privacy law has always centered the idea of control: notices and consent privileges help people "make decisions about how to manage their data."[157] As a result, Daniel Solove characterized traditional privacy law's notice-and-consent regime as "privacy self-management," involving "the various decisions people must make about their privacy and the tasks people are given . . . to do regarding their privacy, such as reading privacy policies, opting out, changing privacy settings, and so on."[158] These tasks are performances: toggling consents, click-to-agree buttons, and confirming or rejecting cookie requests. As the philosopher Gordon Hull has argued, the routinization of these practices has inured us into thinking that privacy self-management is privacy law.[159] Recent privacy law proposals in the United States reflect as much. They may add additional rights of control, but they follow the same script: we have to navigate our own privacy through clicks and consents on digital platforms themselves.

1. Discourses of Control

Industry almost exclusively uses the discourse of control when its representatives talk about their privacy work. Although research into nonexpert visions of privacy suggests that we think about privacy in many different ways, many tend to echo notions of control as well.[160] These discourses are pervasive and routinized pieces of the information economy.

156. SAFE DATA Act §§ 206(c)(3), 404(a).

157. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013). There is a robust literature demonstrating the centrality of control discourse and practices in privacy law. For summaries of that literature, see, for example, Hartzog, *supra* note 13, at 959 (explaining how "control" won out as the focus of the FIPS and privacy law); ARI EZRA WALDMAN, PRIVACY AS TRUST 29–33 (2018) (summarizing the privacy scholarly literature on control).

158. Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 3 (2021).

159. Gordon Hull, *Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data*, 17 ETHICS & INFO. TECH. 89, 89 (2015).

160. *See* Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako & Lorrie Faith Cranor, *Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration*, 2018 PROC. PRIV. ENHANCING TECH. 5, 5 (2018); CHRISTINA NIPPERT-ENG, ISLANDS OF PRIVACY 7 (2010).

Mark Zuckerberg used the word "control" forty-nine times in one Senate hearing to refer to Facebook's privacy work.[161] In 2020, Zuckerberg said the company changed its platform "to protect user privacy and give people more control."[162] At a 2019 hearing before the Senate Commerce Committee, Jon Leibowitz testified that the "framework" for a federal privacy law should give "consumers more control over their data."[163] His proposals called for giving consumers "statutory rights to control how their personal information is used and shared," and "promot[ing] consumer control and choice by imposing requirements for obtaining meaningful consent."[164] Michael Beckerman, the President and CEO of the Big Tech-funded Internet Association, expressed that people should have access to and control of their data.[165] Beckerman suggested that legislation should "empower[] people to better understand and control how personal information they share is collected, used" and should include "the development of tools to give users more control over their personal information."[166] In 2018, Bud Tribble, then-Vice President for Software Technology at Apple, and Rachel Welch, Senior Vice President for Policy and External Affairs at Charter Communications, made similar comments.[167]

Sundar Pinchai, CEO of Alphabet, Google's parent company, has said that he "always believed that privacy is a universal right and . . . Google is committed

161. *Facebook, Social Media Privacy, and the Use and Abuse of Data*, Hearing before the S. Subcomm. on Com., Sci., & Transp. of the Comm. on the Judiciary, 115th Cong., 2d Sess. (2018) (oral statement of Mark Zuckerberg, CEO, Facebook, Inc.) [hereinafter Facebook Hearing].

162. *Online Platforms and Market Power Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google: Hearing before the H. Comm. on the Judiciary, Subcomm. on Antitrust, Com., & Admin. L*, 116th Cong (2020) [hereinafter Online Platforms Hearing] https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=3113 [https://perma.cc/7M7S-7BTV] (written testimony of Mark Zuckerberg, CEO, Facebook, Inc.)

163. *Policy Principles for a Federal Data Privacy Framework in the United States: Hearing before S. Comm. on Com., Sci., & Transp*., 116th Cong., 2d Sess. (2019) [hereinafter Policy Principles Hearing], https://www.commerce.senate.gov/2019/2/policy-principles-for-a-federal-data-privacy-framework-in-the-united-states [https://perma.cc/MA2H-RHZR] (oral testimony of Jon Leibowitz at 45:00); *see also* Brendan Sasso & National Journal, *The 'Privacy Coalition' That Wants to Trim Data Regulation for Telecom Giants*, ATLANTIC (May 11, 2015), https://www.theatlantic.com/politics/archive/2015/05/the-privacy-coalition-that-wants-to-trim-data-regulations-for-telecom-giants/456477/ [https://perma.cc/KH7F-PCZA] (describing Mr. Leibowitz's positions as reflecting the deregulatory interests of an advocacy group for telecommunications companies).

164. Policy Principles Hearing, *supra* note 163 (written testimony of Jon Leibowitz at 4); *id.* (oral statement of Jon Leibowitz).

165. *Id.* (oral testimony of Michael Beckerman at 47:55); *see* INTERNET ASS'N, https://internetassociation.org/our-members/ [https://perma.cc/3PTN-593L].

166. Policy Principles Hearing, *supra* note 163 (written testimony of Michael Beckerman at 1, 4).

167. *Examining Safeguards for Consumer Data Privacy: Hearing before S. Comm. on Com., Sci. & Transp.*, 115th Cong., 2d Sess. (2017), https://www.commerce.senate.gov/2018/9/examining-safeguards-for-consumer-data-privacy [https://perma.cc/VJM3-RHVW] (oral statement of Bud Tribble at 55:53); *id.* (oral statement of Rachel Welch at 1:00:07).

to keeping your information safe . . . [and] putting you in control."[168] The Engine Advocacy and Research Foundation—a lobbying group funded by Google, but claiming to be a voice for entrepreneurs—told Congress to pass a "robust" federal privacy law that "provide[s] transparency, control, and user choice."[169] The National Association of Realtors also wants the same.[170] Keith Enright, Google's then-Chief Privacy Officer, told a Senate committee in 2018 that Google's "key elements" for any privacy discussion are "transparency, control, portability, and security."[171] Executives at Twitter repeated the privacy-as-control discourse, noting that "privacy" means the company "should be transparent about, and provide meaningful control over what data is being collected, how it is used, and when it is shared."[172] All in all, in more than fifteen hearings between 2015 and 2020 before the Senate Commerce Committee alone, information industry executives pushed the discourse of privacy-as-control *every single time*.

Control also permeates popular conceptions of privacy. When asked to illustrate their mental frames about privacy through drawing and art, many participants in a Carnegie Mellon study drew images of control levers and wrote captions about the "right to control" or to "choose" what things in a wallet to share with others.[173] And more than half of the individuals included in a study about privacy in densely populated areas defined privacy as either the "ability/power to control access to some thing, place, or piece of information and its dissemination" or "the freedom to do/live/make decisions," both of which are based on control.[174]

168. Online Platforms Hearing, *supra* note 162 (oral statement of Sundar Pinchai, CEO of Alphabet, Inc, at 4:45:50.); *id.* (oral statement of Sundar Pinchai at 37:58).

169. *Small Business Perspectives on a Federal Data Privacy Framework: Hearing before S. Subcomm. on Mfg., Trade & Consumer Prot. of the Comm. on Com., Sci., & Transp.*, 116th Cong., 1st Sess. (2019) [hereinafter Small Business Hearing], https://www.commerce.senate.gov/2019/3/small-business-perspectives-on-a-federal-data-privacy-framework [https://perma.cc/7GNC-69PV] (oral testimony of Evan Engstrom, Executive Director of the Engine Advocacy and Research Foundation at 39:49); *see* David Dayen, *An Advocacy Group for Startups Is Funded by Google and Run by Ex-Googlers*, INTERCEPT (May 30, 2018), https://theintercept.com/2018/05/30/google-engine-advocacy-tech-startups/ [https://perma.cc/9AR2-5NEH].

170. Small Business Hearing, *supra* note 169 (oral testimony of Nin Dosanjh, Vice Chair, Technology Policy Committee, National Association of Realtors, at 51:28).

171. *Examining Safeguards for Consumer Data Privacy*: *Hearing before S. Comm. on Com., Sci. & Transp.*, 115th Cong., 2d Sess. (2018), https://www.commerce.senate.gov/2018/9/examining-safeguards-for-consumer-data-privacy [https://perma.cc/3B3X-M7ZP] (oral testimony of Keith Enright).

172. *Id.* (oral testimony of Damien Kieran, Global Data Protection Officer and Associate General Counsel, Twitter, Inc., at 50:45).

173. *See* Oates et al.*, supra* note 160, at 5.

174. NIPPERT-ENG, *supra* note 160, at 7.

2. Privacy-as-Control as Performative

The pervasive and widespread assumption that privacy is about control over data parallels pervasive and widespread practices of privacy-as-control. We read privacy policies, consent to data tracking on a website-by-website basis, click buttons to opt out of certain information processing, and otherwise take personal agency to exercise control over information.[175] These practices have been around for decades, and their repetition has a habituating effect. Gordon Hull suggested that repeating self-governance practices normalizes surveillance and habituates us into thinking that privacy law's responsibilities fall to us.[176] Websites and apps deploying rights of control "present[] an information environment in which individuals see themselves as functioning autonomously."[177] We take actions like we are in control by clicking "accept," or clicking "agree," or exercising our right to correct or opt out of data collection. And every time we do so, we are inculcated with the belief that these behaviors—the scaled detritus of privacy-as-control—are privacy law.

Like Austin and Butler, Michel Foucault thought that our actions do not just achieve their immediate effects.[178] That is, clicking "agree" does more than just grant access to a platform. The behavior's routinization and repetition have normalizing effects, making it seem like common sense and ordinary. Our actions "establish[] . . . a moral conduct that commits an individual, not only to other activities always in conformity with values and rules" associated with those actions, "but to a certain mode of being, a mode of being characteristic of the ethical subject."[179] Put another way, exercising rights of control are repeated actions that socially construct our perception of what privacy law is and should be—for example, that self-navigation is the normal, commonsense thing to do. In this way, privacy law's rights of control are performative because our exercises of those rights create a legal regime of individual rights. It should be no surprise, then, that most recent privacy proposals all guarantee similar individual rights of control.

175. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235 (2015).

176. Hull, *supra* note 159, at 90.

177. *Id.* at 96.

178. *Id.* at 97.

179. 2 MICHEL FOUCAULT, THE HISTORY OF SEXUALITY: THE USE OF PLEASURE 28 (Robert Hurley trans., 1985).

These proposals include the right to access data about us,[180] have our data deleted,[181] and opt out of tracking.[182] Some statutes guarantee a right to correct inaccurate or outdated data.[183] Some include the right to move data from one company to another, known as the right to portability.[184] Several proposals guarantee a right to restrict data processing.[185] The proposed New York Privacy Act would give citizens a right against purely algorithmic or automated decisions about their lives.[186] And the Data Accountability and Transparency Act, or DATA Act, guarantees individuals a right to request human review of automated decision-making systems.[187]

Notably, some new privacy laws build on the notice-and-consent paradigm. Almost all state and federal proposals in the United States are opt-out regimes, which means that data collection and processing is presumed lawful unless individuals affirmatively withdraw their consent. Some proposals go further, doubling down on the power of consent. For instance, two proposals in Arizona would let technology companies sell customer data, avoid all restrictions on

180. Twenty-five laws guarantee a right of access. CCPA §§ 1798.100(d), 1798.110, 1798.115; S. 1614, 54th Leg., 2d Reg. Sess. § 18-701(A)(D) (Ariz. 2020); S. 418, 30th Leg., Reg. Sess. § 487(J)–(C) (Haw. 2019); S. 2263, 101st Gen. Assemb., 1st Reg. Sess. § 20(1) (Ill. 2019); S. 2330, 101st Gen. Assemb., 1st Reg. Sess. § 20 (Ill. 2020); H.R. 5603 §§ 20, 25; H.R. 784, 2020 Gen. Assemb., 441st Sess. § 14-4203 (Md. 2020); H.R. 1656 § 14-4203; H.R. 3936, 91st Leg., 91st Sess. § 325O.05, subd. 1(1) (Minn. 2020); H.R. 1253, 2019 Leg., 2019 Reg. Sess. §§ 3(1), 5, 6 (Miss. 2019); L. 746, 106th Leg., 2d Reg. Sess. §§ 6, 8 (Neb. 2020); Assemb. 3255, 219th Leg., 1st Ann. Sess. § 2(I)(e) (N.J. 2020); S. 2834, 218th Leg., 1st Ann. Sess. § 3 (N.J. 2018); S. 176, 54th Leg., 1st Sess. § 3(a) (N.M. 2019); S. 5642, 2019 Leg.,Reg. Sess. § 1103(1), (5) (N.Y. 2019); H.R. 1049, 203d Gen. Assemb., 2019 Sess. § 4(a)(1)–(2), (b) (Pa. 2019); S. 234, 2019 Gen. Assemb., Jan. Sess. §§ 6-48.1 to 6-48.3(a), 6-48.1-6 (R.I. 2019); H.R. 4518, 86th Leg., Reg. Sess. § 541.053 (Tex. 2019); H.R. 473 § 59.1-574, S. 5062, 67th Leg., 2021 Reg. Sess. § 103(1) (Wash. 2021); COPRA § 102(a); Privacy Bill of Rights § 6(a)(1); SAFE DATA Act § 103(a); Online Privacy Act § 101; DATA § 201.

181. Twenty-five laws guarantee a right to delete. CCPA § 1798.105; S. 1614 § 18-701(E); S. 418 § 487(J)–(D); S. 2263 § 20(3); S. 2330 § 25(3); H.R. 5603 § 15; S. 2351, 88th Gen. Assemb., 2020 Reg. Sess. § 3 (Iowa 2020); H.R. 784 § 14-4205; H.R. 1656 § 14-4205; H.R. 3936 § 325O.05, subd. 1(3); H.R. 1253 § 4(1); L. 746 § 9; Assemb. 3255 § 3; S. § 176 3(b); S. 5642 § 1103(3); H.R. 1049 § 4(e); S. 234 § 6-48.1-4; H.R. 4518 § 541.052; H.R. 473 § 59.1-574; S. 5062, 67th Leg., 2021 Reg. Sess. § 103(3) (Wash. 2021); COPRA § 103; Privacy Bill of Rights § 6(a)(5)(A); SAFE DATA Act § 103(a); Online Privacy Act § 103; DATA § 204.

182. Twenty-three laws include a right to opt out. S. 1614 § 18-701(F)–(G); CCPA §§ 1798.120, 1798.135(a)–(b); H.R. 963, 26th Leg., Reg. Sess. § 501.062(2)(b) (Fla. 2020); S. 418 § 487(J)–(F); S. 2263 § 20(6); S. 2330 § 25(1); H.R. 5603 § 30; H.R. 784 § 14-4206; H.R. 1656 § 14-4206; H.R. 3936 § 325O.05, subd. 1(5); H.R. 1253 § 7; Assemb. 2188, 219th Leg., 2020 Sess. § 4 (N.J. 2020); Assemb. 3255 § 6; S. 2834 § 4; S. 176 §§ 3(d), 4(f); H.R. 1049 § 4(a)(3); S. 234 § 6-48.1-7; H.R. 4518 § 541.054; H.R. 473 § 59.1-574; *id.* § 59.1-574; S. 5062 § 103(5); COPRA § 105(b); MYOBA § 6; SAFE DATA Act § 104(d).

183. S. 2263 § 20(2); S. 2330 § 25(2); H.R. 3936 § 325O.05, subd. 1(2); S. 5642 § 1103(2); H.R. 473 § 59.1-574; S. 5062 § 103(2); COPRA § 104; Privacy Bill of Rights § 6(a)(4); SAFE DATA Act § 103(a); Online Privacy Act § 102; DATA § 203.

184. H.R. 3936 § 325O.05, subd. 1(4); H.R. 473 § 59.1-574; S. 5062 § 103(4); COPRA § 105(a); Privacy Bill of Rights § 6(a)(3); SAFE DATA Act § 103(a); DATA § 201.

185. S. 2263 § 20(4); H.R. 473 § 59.1-574.

186. S. 5642 § 1103(6).

187. DATA §§ 205, 206.

processing data about adults, and make decisions based on consumer profiling if they obtain consent.[188] Two proposals introduced in the Illinois Senate would allow companies to skirt limits on processing sensitive data, even processing that posed a significant risk to privacy, if they obtain consent.[189] And Maine's privacy law, which took effect in 2019, lifts all restrictions on the use, disclosure, sale, and third-party access to personal information, if companies obtain consent.[190]

Therefore, when viewed from the perspective of social practice, many recent privacy proposals in the United States reflect long-standing privacy-as-control discourses and practices. Even the rights themselves are not that new. The 1973 federal report from the Department of Housing, Education, and Welfare (HEW), which gave rise to early privacy law's notice-and-consent performances, also called for rights of access and deletion, among other individual rights.[191] The repetition of those discourses and practices has had a performative effect—routinized privacy practices have become privacy law.

D. The Emergent Law of Privacy

Scholars trying to understand the evolution of privacy law have elided this point that routinized privacy practices have become privacy law. Anu Bradford suggested that a "Brussels Effect" would make all privacy laws accord with those of the E.U.[192] Bradford predicted that multinational companies would voluntarily adopt E.U. rules, in part, because of the E.U.'s unique combination of market power and regulatory capacity.[193] And since data flows are difficult to constrain within political boundaries, Bradford reasoned that companies in the information industry will be uniquely susceptible to the E.U.'s regulatory power.[194] E.U. law also bans data transfers from the E.U. to other countries if those countries do not have "adequate" data protection laws.[195] Therefore, Bradford predicted that industry and governments would strengthen their practices to meet E.U. demands.[196] However, Anupam Chander, Margot Kaminski, and Bill McGeveran rightly noted that the E.U. has had a privacy law for decades—the E.U. Privacy Directive, which went into effect in 1995, and did not spur

188. S. 1614, 54th Leg., 2d Reg. Sess. § 18-701(H) (Ariz. 2020); H.R. 2729, 54th Leg., 2d Reg. Sess. §§ 18-574(B), 18-577(G)(3) (Ariz. 2020).

189. S. 2263 § 30(3); S. 2330 § 35(l)(3).

190. Maine Rev. Stat. Ann. § 9301(3) (2020). The GDPR also allows companies to rely on user consent to data processing, although consent is only one of six lawful bases for justifying data collection and use. GDPR, *supra* note 3, at art. 6(1).

191. 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 59–63 (1973), https://aspe.hhs.gov/report/records-computers-and-rights-citizens [https://perma.cc/U3JY-EJW3].

192. Bradford, *supra* note 8, at 3, 22–26.

193. *Id.* at 10–19.

194. *Id.* at 17–19, 25–26.

195. *Id.* at 24–26; *see also* GDPR, *supra* note 3, at art. 45, 61–62; Privacy Directive, *supra* note 138, at art. 25 & recitals 56–57.

196. Bradford, *supra* note 8, at 24–26.

Congress or the states to act.[197] They suggested that it was the legal entrepreneurship of leading privacy advocates in California, who took advantage of that state's unique law-making process, that catalyzed the explosion of recent privacy proposals in the United States.[198]

Implicit in Bradford's argument is a formalistic distinction between law and society. Bradford looked to a law-on-the-books catalyst for other laws on the books, conceptualizing law as an autonomous institution off on its own. But sociolegal scholars and the Legal Realists have taught us otherwise.[199] In their view, the relationship between law and society is a reciprocal one, and one famously ignored by the legal formalists of an antiquated age.[200] Law reflects and influences social change, whether it be changes in the family or shifts to an industrial or information economy.[201] To think the law is only influenced by other law is to ignore society's role.

There are other limitations to the conventional wisdom's focus on the GDPR's or the CCPA's influence. Some scholars put considerable faith in the norm entrepreneurship of a small group of privacy advocates who forced the California legislature's hand in 2018 but neglected to consider what companies were already doing internally by that time.[202] These scholars recognize that the rights/compliance model was not invented by the CCPA, but insufficiently account for how that makes the narrative more complex. Privacy law-as-compliance in the United States dates as far back as 2011, when the FTC first required Google to develop a "comprehensive privacy program."[203] Individual rights to access, restrict processing, and correction are even older; they were part of the original Code of Fair Information Practice recommended by HEW in 1973.[204] As such, they predate every E.U. privacy law—and even the E.U. itself.[205]

Plus, neither the formalist nor realist theory explains why policymakers and advocates agreed on *these* proposals. Chander, Kaminski, and McGeveran did not characterize recent privacy proposals as a mix of rights and compliance, instead seeing them as primarily rights-based.[206] However, as discussed above, compliance is a critical piece of these proposals when viewed from the

197. *See* Chander et al., *supra* note 4, at 1737–38.

198. *Id.*

199. *See, e.g.*, HORWITZ, *supra* note 9.

200. Roscoe Pound, *Mechanical Jurisprudence*, 8 COLUM. L. REV. 605, 606–07 (1908) (describing the belief in the law's neutrality as central to legal formalism).

201. *See generally* Polanyi, *supra* note 9 (providing a canonical account of the social, economic, and legal shifts from a pre-market to an industrial society); COHEN, *supra* note 9, at 5–8 (offering a similar canonical account of the role of law in the shift to the information age).

202. Chander et al., *supra* note 4, at 1737–38.

203. Google Consent Decree, *supra* note 12, at 6.

204. U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 191, at 8–15.

205. The E.U. was created in 1993 by the Maastricht Treaty. The E.U.'s Privacy Directive was passed in 1995. *See* Privacy Directive, *supra* note 138, at 31.

206. Chander et al., *supra* note 4, at 1737–38.

perspective of practice.[207] Even a proposal that simply allows individuals to access and delete their data requires companies to create internal processes to intake, assess, respond to, and implement those requests. Moreover, E.U. regulators have made it clear that there is no single path to adequacy.[208] And yet, U.S. lawmakers have chosen only one set of practices. They could have gone further and imposed substantive limits on data collection that would also win an adequacy determination. They could have taken Woodrow Hartzog's advice and used various legal tools to ensure that privacy protections and anti-manipulation guarantees are designed into new technology products.[209] They didn't; they all chose individual rights and compliance-based governance.

Perhaps policymakers are risk averse or lack imagination.[210] Perhaps we are all steeped in the same governing discourses that define how we think about privacy, leading policymakers to adopt similar ideas that do not upset traditional structures of power.[211] Political scientists might explain the similarities by pointing to the Overton Window, or the theory that only a small set of policy options are acceptable in any given political moment.[212]

But Overton Windows move. Discourses are challenged and replaced. And yet, recent privacy law proposals codify roughly the same social practices: they envision collaborative regulators, internal corporate compliance structures, and a series of rights to privacy self-management. This Section has shown why. Recent privacy proposals follow a rights/compliance approach because long-standing practices—industry input in regulations, settlements and consent decrees, self-audits, PIAs, recordkeeping, codes of conduct, privacy offices, and privacy self-navigation—socially constructed privacy law from the ground up. Most state and federal proposals would codify social practices of privacy that regulators, industry, and individuals have been engaged in for some time, long before the GDPR and the CCPA. The repetition of these performances may have normalized them, acculturating stakeholders to think that this is what privacy law is and should be. Policymakers could not think of other options because performances of privacy on the ground had already created the category of privacy law for them. And that, as the next Section indicates, is a problem.

---

207. *See supra* Part II.B.2.

208. Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 783–85, 787, 794 (2019) (recognizing various approaches to achieving "adequacy").

209. *See generally* HARTZOG, *supra* note 6.

210. *See, e.g.*, Susan Rose-Ackerman, *Risk Taking and Reelection: Does Federalism Promote Innovation?*, 9 J. LEGAL STUD. 593, 594, 605 (1980); Christopher Serkin, *Big Differences for Small Governments: Local Governments and the Takings Clause*, 81 N.Y.U. L. REV. 1624, 1668 (2006).

211. *See* MICHEL FOUCAULT, THE ARCHAEOLOGY OF KNOWLEDGE AND THE DISCOURSE ON LANGUAGE 201 (A. M. Sheridan Smith trans.,1972) (explaining the way in which discourses shape the way we think and talk about a subject); Michel Foucault, *The Order of Discourse*, *in* UNTYING THE TEXT: A POST-STRUCTURALIST READER 51–52 (Robert Young ed., 1981) (arguing that discourses are used by those in power to maintain power by sustaining discourses that support their control).

212. *A Brief Explanation of the Overton Window*, MACKINAC CTR. FOR PUB. POL'Y, https://www.mackinac.org/OvertonWindow [https://perma.cc/7XMK-FBH4].

III.
THE DANGERS OF A RIGHTS/COMPLIANCE APPROACH

I have suggested that recent privacy proposals in the United States look the way they do because long-standing corporate, regulatory, and self-management performances have socially constructed privacy law in our legal consciousness. In this Section, I make a normative claim: the performativity of rights/compliance practices demonstrates why the approach is unlikely to achieve stronger privacy protections for individuals and is incapable of addressing informational capitalism's structural asymmetries and discriminatory harms. The following Sections discuss two clusters of reasons for this: one based on the individual rights model and the other based on the compliance model.

A. The Misplaced Individual Rights Model

The practices associated with individual rights of control seem empowering: we can click on links to ask that our data be deleted, corrected, and moved. But although more control sounds like a good thing, *individual* rights will not solve *collective* privacy problems.[213] Habituating ourselves to the fiction that we, as individual users, are truly capable of managing our privacy online is precisely what the information industry wants. This is in no small part because this fiction allows technology companies to weaponize our exercise of those individual rights to immunize themselves from responsibility and accountability.

1. Insufficiencies of Individual Rights Discourse

The discourse of individual rights is dangerous if the law's goal is to provide substantive privacy protections in the information economy. Granted, early privacy law and scholarship focused on individual rights.[214] But that narrow conception inadequately appreciates the privacy concerns inherent in the advertising-based business models of data-extractive capitalism. Social surveillance, for example, undermines our ability to think independently, eviscerates our autonomy, and turns everyday practices into information-sharing events.[215] Privacy also serves collective ends: protecting community, enhancing

213. I am not the first to recognize this, of course. Some argue that privacy impact assessments can encourage companies to analyze how their products impact not just individuals, but groups. *See e.g.*, Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations*, 11 INT'L DATA PRIV. L. 125, 138 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id= 3456224 [https://perma.cc/9KYZ-3XKT].

214. *See, e.g.*, Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 12–59 (2008) (summarizing the literature on different conceptions of privacy).

215. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 3-9 (2015) (arguing that privacy gives individuals the ability to develop new, inchoate, or dissident ideas); HARTZOG, *supra* note 6, at 161 (describing the ways in which the designs of platform interfaces and other technologies manipulate our choices); Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology*, PROC. 2012 IEEE SYMP. ON SEC. & PRIV. 413, 415

democracy, increasing solidarity, and ensuring ongoing social interaction.[216] For instance, as Robert Post argued, privacy is meant to "safeguard[] rules of civility," rather than any individual right against eavesdropping or snooping.[217] And Julie Cohen has demonstrated that privacy is about establishing the parameters of social space in ways that make continued interaction with others possible.[218]

Just like privacy is inherently a social construct, data-extractive capitalism can cause social harms. For example, data processing abets the entrenchment of traditional power structures and social and economic inequality.[219] Data-driven technologies routinely discriminate against persons of color, contributing to both higher rates of incarceration and glaring incidents of unjust deprivations of liberty.[220] And studies have found that information products have been used to take away welfare benefits from the poor, separate immigrant families, and subordinate women as victims of sexploitation.[221] Technology directly shapes collective lives and is deeply embedded in institutions that are structured to reinforce race, gender, and sexual orientation discrimination.[222]

Learning those lessons, Salomé Viljoen argued that the information economy has a "sociality problem" in which individual rights ostensibly allow us to regulate "vertical" relationships with platforms, but cannot address the "horizontal" relationships among individuals who share the same relevant

---

(2012), https://cyberlaw.stanford.edu/files/publication/files/trackingsurvey12.pdf [https://perma.cc/9LAR-NCD3].

216. SOLOVE, *supra* note 214, at 84–88 (arguing that privacy has social value); WALDMAN, *supra* note 157, at 49–76 (showing how privacy is necessary for social engagement).

217. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959–68 (1989).

218. Julie E. Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426–28 (2000).

219. *See, e.g.*, Frank Pasquale, *Two Narratives of Platform Capitalism*, 35 YALE L. & POL'Y REV. 309, 311 (2016) (discussing the legal implications of the ways in which data use entrenches social hierarchies); Frank Pasquale, *Paradoxes of Privacy in an Era of Asymmetrical Social Control*, *in* BIG DATA, CRIME AND SOCIAL CONTROL 31 (Aleš Završnik ed., 2017); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 671 (2016) (demonstrating the capacity for algorithmic decision-making systems to have unequal impact on marginalized populations).

220. *See, e.g.*, Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/WF8Y-ZTK6]; Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/QG5S-7596].

221. *See, e.g.*, VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018) (showing the connection between data processing and subordination of the poor); Alvaro M. Bedoya, *The Cruel New Era of Data-Driven Deportation*, SLATE (Sept. 22, 2020), https://slate.com/technology/2020/09/palantir-ice-deportation-immigrant-surveillance-big-data.html [https://perma.cc/CPH8-764Q].

222. *See* Victor Ray, *Why So Many Organizations Stay White*, HARV. BUS. REV. (Nov. 19, 2019), https://hbr.org/2019/11/why-so-many-organizations-stay-white?ab=seriesnav-bigidea [https://perma.cc/XNA8-3JGW] (demonstrating that institutions are not "race-neutral" by citing statistics on the scarcity of minority representation in organizational hierarchies).

characteristics.[223] Because the information industry's business model is dedicated to "deriving [] population-level insights [from] data subjects" that are then applied to individuals who share those characteristics through design nudges, behavioral advertising, and political microtargeting, what we share affects how others who are like us are treated.[224] That is, by merely using technologies that track and extract data from us, we become unwitting accomplices in the process through which industry translates our behavior into designs, technologies, and patterns that shape and manipulate everyone else. Abetting this system is a precondition of participation in the information age. For Viljoen, then, the information economy's core evil is that it conscripts us all in a project of mass subordination that is—not so incidentally—making a few people very rich.[225] Even at their best, individual rights that only govern vertical relationships are insufficient to address or ameliorate that kind of subordination.[226]

But discourse is only the beginning. Codifying these practices of privacy self-management directly undermines privacy protections. That may sound counterintuitive. In truth, individual rights to data can be weaponized by industry to erode privacy protections wholesale.

2. Weaponizing Consent

Privacy law's individual rights approach is based on the presumption that individuals have sufficient power and agency to exercise those rights autonomously and in accordance with their preferences. We do not.[227] Rather,

223. *See* Salomé Viljoen, *A Relational Theory for Data Governance*, 131 Yale L.J. 573, 603–616 (2021).

224. *Id.* at 637.

225. *Id.* at 573.

226. *Id.*

227. *See* DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2011); Daniel Kahneman & Amos Tversky, *Judgments of and by Representativeness*, *in* JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES 84–98 (Daniel Kahneman, Paul Slovic & Amos Tversky eds. 1982); RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008); Daniel Kahneman, Amos Tversky & Paul Slovic, *Judgment Under Uncertainty: Heuristics and Biases*, 185 SCI. 1124 (1974). Our disclosure behavior depends on comparative judgments and is skewed by framing biases and hyperbolic discounting, all of which, research shows, make us more likely to disclose information at any given time than exercise our rights to opt out. *See* Alessandro Acquisti, Leslie K. John & George Loewenstein, *The Impact of Relative Standards on the Propensity to Disclose*, 49 J. MKTG. RSCH. 160 (2012); Leslie K. John, Alessandro Acquisti & George Loewenstein, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. CONSUMER RSCH. 858, 868 (2011). Plus, the platforms through which we must exercise our rights of control are designed for us by the very companies that rely on data-extractive business models. Their websites are laden with manipulative dark patterns and other design tricks that skew and nudge our behaviors in ways that benefit them. Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ASS'N COMPUTING MACH. ON HUMAN-COMPUT. INTERACTION 1, 2–3 (2019). The rights/compliance model may assume and entrench the idea that we are capable of exercising our rights, but the data tells us otherwise.

the problem runs deeper. Reifying that assumption allows industry to weaponize individual rights—particularly the right to consent—against our privacy, undermining everyone's ability to exercise rights of control in the first place.

Traditionally, consent was the shibboleth of privacy law.[228] Proponents of the rights/compliance model make much about how laws like the GDPR are not consent-based regimes.[229] They are correct, but only to a point. Consent is not the only justification for processing personal data under the GDPR. Even when processing is pursuant to user consent, the individual rights and compliance requirements are supposed to remain in place.[230] But even these commentators acknowledge that individual consent is one of the two most common justifications for data collection under the GDPR.[231] And yet, as scholars have shown, wherever consent is operable in the information economy, it is both a weapon of data extraction and a shield against accountability.[232]

On the misleading premise that individuals are capable of making their own informed choices about what they share and with whom they share it, industry weaponizes consent in ways that make other individual rights of control mostly meaningless. In 2019, for instance, while Facebook was trying to dismiss a lawsuit for the company's failure to stop Cambridge Analytica from unlawfully mining user data, the company's attorney told Judge Vince Chhabria that "[t]here is no privacy interest" in any information Facebook has.[233] Users "consent[ed]" to the terms of service and engaged in "an affirmative social act to publish," which "under centuries of common law, . . . negated any reasonable expectation of privacy."[234] When the judge asked if it would be an invasion of privacy for Facebook to break a promise not to share an individual's information with third parties, Facebook's counsel claimed that "Facebook does not consider that to be actionable," citing user behavior and consents as evidence that users had given up control of their data.[235] In its briefing, the company went even further, arguing

228. *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019) ("Consent is the foundation of the relationships we have with search engines, social networks, commercial web sites, and any one of the dozens of other digitally mediated businesses we interact with regularly.").

229. *E.g.*, Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 109 (2021); Gabriela Zanfir-Fortuna, *10 Reasons Why the GDPR Is the Opposite of a 'Notice and Consent' Type of Law*, MEDIUM (Mar. 13, 2019), https://medium.com/@gzf/10-reasons-why-the-gdpr-is-the-opposite-of-a-notice-and-consent-type-of-law-ba9dd895a0f1 [https://perma.cc/7WJK-2LLY].

230. Jones & Kaminski, *supra* note 229, at 108–10.

231. *Id.* at 109.

232. Solove, *supra* note 157, at 1880 ("Privacy self-management takes refuge in consent. [It] . . . legitimizes nearly any form of collection, use, or disclosure of personal data.").

233. Transcript of Record at 7, *In re* Facebook, Inc. Consumer Privacy User Profile Litigation, No. 18-MD-02843 (N.D. Cal. May 29, 2019).

234. *Id.*

235. *Id.* at 15.

that because individuals "can control how" their content is shared, anything they then share is ripe for use by Facebook and third parties.[236]

In *Campbell v. St. John*,[237] a case about Facebook's practice of scanning users' private messages to collect data for behavioral advertising, Facebook argued that users lacked standing to challenge any Facebook data practice because they "consented to the uses of . . . data."[238] In *Smith v. Facebook*,[239] the company made the same argument, noting that Facebook should be allowed to track users wherever they go on the Internet, because users "are bound by their consent to those policies."[240] And in *In re Google, Inc. Cookie Placement Consumer Privacy Litigation*,[241] Google moved to dismiss all claims pertaining to the unauthorized use of cookie tracking and the unlawful interception of user data by arguing that "both Plaintiffs and the websites they communicated with provided their consent for Google . . . when they sent a GET request . . . so that they could browse websites containing Google ads."[242] In other words, Google claimed that the mere use of its search engine is tantamount to consenting to all of Google's data use practices, putting the burden of any consequences on the individual user.

Similarly, in *Patel v. Facebook*,[243] which challenged the company's collection and use of biometric information, Facebook argued that no plaintiff could ever successfully bring a lawsuit against the company for use of any kind of information, let alone biometric data, because "plaintiffs knew exactly what data Facebook was collecting, for what purpose, and how to opt out of Tag Suggestions."[244] Facebook suggested that this immunity was so broad that it held up even if the company's notices were not sufficiently specific.[245] Facebook reasoned that since users consented to all data collection practices when they signed up for accounts, and since privacy law only requires choice, consent, and

236. Reply in Support of Defendant Facebook, Inc.'s Motion to Dismiss Plaintiffs' First Amended Consolidated Complaint, *In re* Facebook, Inc. Consumer Privacy User Profile Litigation, 402 F. Supp 767, 792 (N.D. Cal. 2019).

237. Campbell v. Facebook, Inc., 951 F.3d 1106 (9th Cir. 2020).

238. *Id.* at 1119 n.9.

239. Smith v. Facebook, Inc., 745 F. App'x 8 (9th Cir. 2018).

240. Appellee's Brief at 21, Smith v. Facebook, Inc., 745 F. App'x 8 (9th Cir. 2018) (No. 17-16206), https://epic.org/amicus/facebook/smith/Smith-v-Facebook-9th-Cir-Facebook-Brief.pdf [https://perma.cc/ZA8R-SAEC].

241. *In re* Google, Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015).

242. Answering Brief of Defendant-Appellee Google Inc. at 36–37, *In re* Google, Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015) (No. 13-4300).

243. Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

244. Appellant's Brief at 33, Patel v. Facebook, 932 F.3d 1264 (9th Cir. 2019) (No. 18-15982).

245. Facebook, Inc.'s Motion for Summary Judgment, *In re* Facebook Biometric Information Privacy Litigation, 326 F.R.D. 535 (N.D. Cal. 2018) (No. 3:15-CV-03747-JD), *aff'd sub nom.* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

control, users who signed up but never opted out had given up their rights to their data.[246]

Facebook has even argued that its own privacy promises are meaningless because it had the power to define the rights of its customers. For example, in several ongoing lawsuits, Facebook has argued that its promise to remove cookies that identify a particular user's account was not a "promise[] not to record the communication[]" and that promises of anonymity do not create expectations of privacy.[247] In the same case, Facebook argued that all user information available to Facebook—including every website users visit—is "voluntarily disclosed."[248] It is easy to see the company making similar arguments on the ground that individuals are freely capable of exercising their rights of access, deletion, correction, and opt out in order to hold users responsible for all data use practices that result.

Notably, at all times during the five years in which Facebook's and Google's lawyers made these arguments, both companies had privacy-focused internal organizational structures in place.[249] Both companies had long been operating under FTC consent decrees that required, among other things, comprehensive privacy programs.[250] Both companies also claimed to be compliant with the GDPR as of 2018,[251] a year before *Patel* and two years before Facebook argued that the only way its users could expect privacy on the Internet

246. *Id.*

247. Defendant Facebook, Inc.'s Reply in Support of Motion to Dismiss Plaintiffs' Second Amendment Consolidated Class Action Complaint at 11, *In re* Facebook, Inc. Internet Tracking Litigation, 263 F.Supp.3d 836 (N.D. Cal. 2017) (No. 5:12-md-02314 EJD).

248. Defendant Facebook, Inc.'s Motion to Dismiss Plaintiffs' Second Amended Consolidated Class Action Complaint at 33, *In re* Facebook, Inc. Internet Tracking Litigation, 263 F.Supp.3d 836 (N.D. Cal. 2017) (No. 5:12-md-02314 EJD).

249. Google developed a privacy department as a result of a 2011 consent decree with the FTC. *See* Google Consent Decree, *supra* note 12. Facebook did the same in response to its 2011 agreement with the FTC. Agreement Containing Consent Order, at 5–6, *In re* Facebook, Inc., File No. 092 3184 (Nov. 29, 2011) [hereinafter Facebook Consent Decree], https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf [https://perma.cc/Z6R7-9XRR].

250. Michelle Quinn & Tony Romm, *Google Tells FTC of Privacy Progress*, POLITICO (Feb. 10, 2012), https://www.politico.com/story/2012/02/google-tells-ftc-of-progress-on-privacy-072731 [https://perma.cc/48GD-FZYA]; *see* Google Consent Decree, *supra* note 12; Facebook Consent Decree, *supra* note 249.

251. *Facebook's Commitment to Data Protection and Privacy in Compliance with the GDPR*, FACEBOOK BUS. (Jan. 29, 2018), https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr [https://perma.cc/773N-FP69]; Warwick Ashford, *Facebook Is Ready for GDPR, Says Zuckerberg*, COMPUT. WKLY. (May 23, 2018), https://www.computerweekly.com/news/252441730/Facebook-is-ready-for-GDPR-says-Zuckerberg [https://perma.cc/AN9F-X4H2]; Ashley Rodriguez, *Google Says It Spent "Hundreds of Years of Human Time" Complying with Europe's Privacy Rules*, QUARTZ (Sept. 26, 2018), https://qz.com/1403080/google-spent-hundreds-of-years-of-human-time-complying-with-gdpr/ [https://perma.cc/Y8GM-ZPE3].

was if they used a Virtual Private Network, or VPN.[252] Therefore, Facebook and Google demonstrate that having compliance systems in place and other rights available does not stop the companies from engaging in legal practices that erode privacy rights for users. Performative rights-based practices allowed these companies' lawyers to conceptualize privacy law in a way that enables industry to "take[] refuge" in consent's attendant immunity.[253]

B. The Problem of Compliance

A second category of structural weaknesses in recent privacy proposals stems from their codification of performative compliance practices. The following Sections identify three of those weaknesses. First, the law's endogenous construction from corporate performances on the ground suggests that managerialized compliance will be dominated by the practices of industry leaders, which may conscript the law in favor of monopolists' anticompetitive behavior. Second, the reliance on procedure elides substantive injustice below the surface and, therefore, leaves in place the inequities of data-extractive capitalism. Finally, and perhaps most importantly, the practical application of compliance-based governance is internally inconsistent, performatively creating public institutions that are incapable of holding industry accountable.

1. Dominant Practices and Underinclusive Law

The performativity of privacy law practices means that the law may be constructed by the repeated practices of the most dominant actors—namely, those with money, power, and the risk tolerance that comes with both. There are several reasons for this. These companies' wealth, status, and market share allow them to take on greater litigation risks than their smaller competitors.[254] As such, dominant companies can afford to act first, and establish new compliance practices without clear guidance from regulators, just as envisioned by compliance-based governance. And perhaps because smaller competitors cannot afford the risks of investigation and litigation that come with improper compliance practices, industry standards and customs will coalesce around the performances of dominant players.[255]

---

252. Appellee's Brief at 28, Davis v. Facebook, Inc., 956 F.3d 589 (9th Cir. 2020) (No. 17-17486) (arguing that users themselves had to "take[] steps to keep their browsing histories private").

253. Solove, *supra* note 157, at 1880.

254. *E.g.*, George B. Shepherd & Morgan Cloud, *Time and Money: Discovery Leads to Hourly Billing*, 1999 U. ILL. L. REV. 91, 103–04 (1999).

255. *See, e.g.*, Eric A. Posner, *Law, Economics, and Inefficient Norms*, 144 U. PA. L. REV. 1697, 1727 (1996) ("Highly unequal endowments of group members may be evidence of inefficient norms. The more powerful members may prefer and enforce norms that redistribute wealth to them, even when those norms are inefficient."); Lloyd L. Weinreb, *Custom, Law and Public Policy: The INS Case as an Example for Intellectual Property*, 78 VA. L. REV. 141, 146–47 (1992) (arguing that relying on custom will mean that "the better financed private interest" will win, "rather than a careful, systematic" rule that "will serve the community as a whole").

This coalescing behind the practices of the most dominant actors also happens organically. In many industries, professionals share their experiences and advice through formal outlets—namely, industry conferences, convenings, and publications, where the views of industry leaders are usually of keen interest to the rank-and-file.[256] The privacy industry has several large networking conferences, including several hosted by the International Association of Privacy Professionals (IAPP), attracting thousands of attendees worldwide, and the Privacy+Security Forum, which happens twice a year and brings together hundreds of professionals for panels, networking, and idea exchange.[257] Researchers have also shown that privacy professionals take advantage of their overlapping social networks to learn from colleagues at leading companies.[258] This effectively spreads the compliance performances of a small subset of industry actors across the field, reinforcing privacy law "isomorphism."[259] Therefore, the most powerful corporations are able to entrench their compliance practices in the same way that a first entrant can claim a monopolistic position in a market.[260]

Wealthier companies also have the resources to build larger in-house privacy departments that can dedicate time, money, and labor to compliance practices.[261] They can even offer compliance support to their customers.[262] By contrast, smaller companies are forced to outsource more of their compliance to privacy technology vendors, many of which make dubious claims about proprietary automated systems that purport to achieve compliance with pre-filled

256. *See* EDELMAN, *supra* note 47, at 78–79 (discussing the impact of professional organizations and information resources in the human resources field).

257. *Upcoming IAPP Conferences*, IAPP, https://iapp.org/conferences/ [https://perma.cc/TFW9-7DAQ]; PRIV. & SEC. ACAD., https://www.privacysecurityacademy.com/ [https://perma.cc/795Z-VCHY].

258. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 126, at 80, 142.

259. *See* Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOCIO. REV. 147 (1983) (explaining how and why businesses in an industry evolve to look and behave in similar ways); Mark S. Granovetter, *The Strength of Weak Ties*, 78 AM. J. SOC. 1360, 1363–66 (1973) (discussing how information is spread through the connections that link individuals within their networks and to other networks).

260. This is called the "first-mover advantage." *See, e.g.*, Rajshree Agarwal & Michael Gort, *First-Mover Advantage and the Speed of Competitive Entry, 1887-1986*, 44 J. L. & ECON. 161, 173 (2001); William T. Robinson & Sungwook Min, *Is the First to Market the First to Fail? Empirical Evidence for Industrial Goods Businesses*, 39 J. MKTG. RSCH. 120, 126–27 (2002).

261. Indeed, as the IAPP and TrustArc recently found, budgetary constraints likely explain why many companies have not hired anyone to help with data mapping, data inventories, or privacy impact assessments, despite GDPR requirements. IAPP & TRUSTARC, GETTING TO GDPR COMPLIANCE: RISK EVALUATION AND STRATEGIES FOR MITIGATION 8–10 (2018), https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf [https://perma.cc/W4JF-P5QA].

262. *See* Liam Tung, *Struggling to Comply with GDPR? Microsoft 365 Rolls Out New Privacy Dashboards*, ZDNET (Jan. 30, 2019), https://www.zdnet.com/article/struggling-to-comply-with-gdpr-microsoft-365-rolls-out-new-privacy-dashboards/ [https://perma.cc/6H3Z-BLGB].

documents and paper trails.[263] Therefore, a long list of performative compliance practices almost exclusively come from the internal processes of companies that can afford to develop them.

Dominant companies also have more influence over regulators and regulations. In addition to their multi-billion-dollar direct lobbying campaigns aimed at weakening privacy law,[264] the wealthiest technology companies have funded several trade organizations to research and publish policy white papers that reflect their interests.[265] Plus, representatives from the most powerful technology companies have been the most common invitees at congressional hearings on privacy.[266] And, given the revolving door between government service and lucrative positions representing technology companies, regulators have a serious incentive to develop stronger relationships with companies like Facebook and Google than with their far smaller competitors.[267]

This is not merely a theoretical possibility. It is, in fact, precisely how many interactions play out between regulators and industry. The FTC routinely cites the views of the information industry's largest players in its staff reports. For example, the FTC relied on statements from Google's Director of Public Policy when it emphasized transparency and control in its mobile privacy guidance.[268] The report followed from the advice of the Retail Industry Leaders Association and the App Association, an industry trade organization funded by wealthy software development interests that calls for "limited government involvement

263. Ari Ezra Waldman, *Outsourcing Privacy*, 96 NOTRE DAME L. REV. REFLECTION 194, 196 (2021).

264. *See, e.g.*, THOMAS M. LENARD & PAUL H. RUBIN, TECH. POL'Y INST., THE BIG DATA REVOLUTION: PRIVACY CONSIDERATIONS 3, 26 (2013), https://techpolicyinstitute.org/wp-content/uploads/2013/12/the-big-data-revolution-privac-2007594.pdf [https://perma.cc/275M-V77Y]; April Dembosky & James Fontanella-Khan, *US Tech Groups Criticized for EU Lobbying*, FIN. TIMES (Feb. 4, 2013), https://www.ft.com/content/e29a717e-6df0-11e2-983d-00144feab49a [https://perma.cc/95KA-VKA8].

265. David Dayen, *An Advocacy Group for Startups Is Funded by Google and Run by Ex-Googlers*, INTERCEPT (May 30, 2018), https://theintercept.com/2018/05/30/google-engine-advocacy-tech-startups/ [https://perma.cc/67EM-R6VA].

266. *See Examining Safeguards for Consumer Data Privacy, Hearing Before the S. Comm. on Com., Sci., & Transp.*, 115th Cong., 2d Sess. (2018) (including testimony from Keith Enright, Google's Chief Privacy Office at the time, and Damien Kieran, Global Data Protection Officer and Associate General Counsel at Twitter, Inc.).

267. For example, former FTC Commissioner Jon Leibowitz left the FTC to co-chair the 21st Privacy Coalition, an industry-funded, anti-regulatory advocacy group, and became counsel at the law firm Davis Polk & Wardwell LLP, where he represented large corporations on antitrust and privacy matters. *See* Press Release, Brian E. Frosh, Maryland Attorney General, *Former FTC Chair Jon Leibowitz to Join Office of Attorney General* (Oct. 14, 2021), https://www.marylandattorneygeneral.gov/press/2021/101421.pdf [https://perma.cc/5Y3D-7RCK].

268. *See, e.g.*, FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 3 n.13 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [https://perma.cc/Y3E4-5AVR].

in technology."[269] The FTC also explicitly endorsed Facebook's, Apple's, and Google's use of icons to communicate privacy information.[270] It adopted industry's recommendation for self-regulation and an opt-in "Do Not Track" mechanism.[271] And regulators sided with leading technology companies to support self-regulation of the "Internet of Things."[272] It stands to reason that these powerful interests will also have an advantage when they seek to certify their compliance practices and have their versions of best practices adopted as the industry standard.

Therefore, wealthy corporations' performances are more likely to construct the compliance landscape. But what is good for a monopolist is not usually good for society.[273] Entrenched powers have an interest in cementing their market positions, and many have used the law to do so.[274] Performative compliance practices can do the same.

2. Procedures and Substantive Injustice

The enforcement toolkit in recent U.S. privacy proposals is largely procedural: impact assessments, privacy officers, and internal policies. That means that laws will rely on internal organizational structures to protect the individual rights guaranteed on the face of the laws.[275]

But these legitimizing procedures disaggregate legitimacy from substantive justice. Procedures offer "no framework for thinking systematically about the interrelationships between political and economic power."[276] They substitute the "political judgment" of traditional regulation and government intervention with

269. *Id.* at 13 n.62; *see About*, APP ASS'N, https://actonline.org/about/ [https://perma.cc/U9R9-8UH2]

270. FED. TRADE COMM'N, *supra* note 268, at 17 & n.81.

271. *Id.* at 21 & n.92.

272. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 48–49 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/J7CM-NQFF]. The "Internet of Things" refers to a growing collection of electronic devices connected to the internet over Wi-Fi. Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#4a6ee29b6828 [https://perma.cc/22V7-EN2C].

273. Google and Facebook are being investigated as monopolists. *See* Plaintiffs' Complaint, U.S. v. Google, Inc., Case 1:20-cv-03010 (D.D.C. Oct. 20, 2020); Complaint for Injunctive and Other Equitable Relief, F.T.C. v. Facebook, Inc., No. 1:20-cv-03590 (D.D.C. Dec. 9, 2020) (public redacted version of document filed under seal).

274. COHEN, *supra* note 9, at 2–10.

275. This is part of a long research agenda on legitimizing procedures. *See, e.g.*, Tom R. Tyler, *Procedural Justice, Legitimacy, and the Effective Rule of Law*, 30 CRIME & JUST. 283, 314–18 (2003); Jason Sunshine & Tom R. Tyler, *The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing*, 37 L. & SOC'Y REV. 513, 514 (2003); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1305, 1308–13 (2008) (calling for procedural governance mechanisms in administrative agency use of algorithmic systems).

276. Britton-Purdy, Grewal, Kapczynski & Rahman, *supra* note 22, at 1790.

"technical management" of the market, thereby leaving unanswered and unresolved vexing questions of inequality, subordination, manipulation, and asymmetrical power.[277] After all, data can be a tool of oppression, whether it is exploited to train totalitarian facial recognition models, surveil protestors, incarcerate people, or subjugate vulnerable populations.[278] For those people society pushes to the margins, privacy is particularly important and data-extraction is particularly dangerous. Disclosures, data breaches, and industry negligence with pornography sites, WiFi-enabled sex toys, and femtech products undermine a core human right of sexual privacy for everyone, but the people who are most hurt by such privacy breaches are also the most marginalized in society.[279] Compliance practices do little to ameliorate or stop these harms other than to encourage companies to put their policies down on paper. There are, however, some practices that no amount of procedural due process can fix.[280]

Worse yet, focusing on procedural safeguards may discourage policymakers from taking more robust actions. As Paul Butler argued in the context of the right to counsel, guaranteeing a procedural right—in that case, providing lawyers to indigent defendants—obscured the fact that the criminal justice and carceral systems are systemically racist and unjust to the poor.[281] Process, Butler argued, "invest[ed] the criminal justice system with a veneer" of legitimacy and discouraged reformers from digging any deeper.[282] Compliance practices open up privacy law to the same problem. Compliance governance only tries to address certain problems, such as the need to integrate privacy into every step of the design process, the complexity of the technology, and the rapid pace

277. *Id.* at 1793.

278. *See, e.g.*, RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE 42–52 (2019); SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 1–2, 29 (2018); Rashida Richardson, Jason M. Shultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. 192, 218 (2019).

279. *See* Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1770 (2021) ("These risks are not evenly distributed across society. Women and marginalized communities disproportionately bear the burden of private-sector surveillance of intimate life . . . [f]or people with intersecting marginalized identities, the harm is compounded.").

280. There is increasing recognition that the procedural safeguards that characterized much of privacy and technology scholarship are insufficient. *See, e.g.*, Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L.J. 797 (2021) (distinguishing previous scholarship that sought to reimpose due process on administrative processes that use algorithms to make policy from more structural concerns about algorithms' fundamental legitimacy); Frank Pasquale, *The Second Wave of Algorithmic Accountability*, L. & POL. ECON. (Nov. 25, 2019), https://lpeblog.org/2019/11/25/the-second-wave-of-algorithmic-accountability/ (distinguishing between algorithmic accountability scholarship that seeks to ameliorate harms and assign responsibility and structural deficiencies of automated decision-making in government, generally).

281. Paul D. Butler, *Poor People Lose:* Gideon *and the Critique of Rights*, 122 YALE L.J. 2176, 2201 (2013) ("[P]rocedural rights may be especially prone to legitimate the status quo, because 'fair' process masks unjust substantive outcomes and makes those outcomes seem more legitimate.").

282. *Id.* at 2178–79.

of development. Even at its best, compliance-based governance ignores more structural questions of power, justice, and human flourishing.

3. Undermining the Public-Private Partnership

For it to work the way it is supposed to, compliance-based governance assumes that regulators' toolkits and expertise are insufficient.[283] A traditional regulator might use a command-and-control approach where the state can ban products outright, place limits on behaviors, and hold industry accountable through court orders and litigated claims.[284] But a compliance-based model, where industry is responsible for its own ongoing monitoring, suggests this approach is ineffectual and limited. The private sector, proponents say, has technical expertise that government does not.[285] A command-and-control approach also raises a "pacing problem" where top-down regulation cannot keep up with fast-changing technologies.[286] Therefore, compliance-based governance purports to bring "private sector expertise in[to] governance."[287] It is also supposed to bring new enforcement mechanisms to regulators' command-and-control toolkits of rules and government enforcement agents.[288] The compliance model implies that if toolkits were sufficient, there would be no need for the nimbleness, flexibility, and speed—not to mention the input and expertise from private industry—that compliance-based governance brings to the information economy.

Compliance-based practices—impact assessments, compliance structures, self-audits and self-assessments, codes of conduct, industry self-certifications, settlements, and consultations—are performative because they construct regulatory institutions that require those practices. The expectation that industry will bring its own experts to the table disincentivizes the government to fund the FTC's own experts. If regulated entities are hiring assessors and conducting audits by executive attestation on their own, the FTC does not need its own army of auditors and monitors to do the same job. And if most cases settle, Congress has an excuse to withhold the funding and staffing the FTC might need to litigate more claims. By making industry a partner in regulation, the compliance model explicitly and intentionally redistributes regulatory duties, relieving government of burdens, but also normalizing the idea that government does not and should

283. Kaminski, *supra* note 4, at 1564 (noting that collaborative governance adds "soft" law mechanisms like negotiated settlements, legal safe harbors, and incorporation of industry standards to traditional regulatory modalities).

284. *See, e.g.*, David A. Dana, *The New "Contractarian" Paradigm in Environmental Regulation*, 2000 U. ILL. L. REV. 35, 44–51 (comparing command-and-control to a site-specific negotiated form of governance).

285. Kaminski, *supra* note 4, at 1560.

286. *Id.* at 1560–61.

287. *Id.* at 1562.

288. *Id.*

not have to perform traditional regulatory responsibilities. Industry is there to help.

Many other legal institutions are transforming themselves in the image of the compliance model. Industry input is engrained in modern environmental, health, and safety law,[289] with regulators often considering market costs in regulatory decision-making.[290] Financial regulation in the wake of the 2008 Financial Crisis relies on audits, independent committees, and other internal structures that amount to outsourcing regulation to regulated entities themselves.[291] Compliance-based regulation and managerialization have similarly expanded the importance of employer-friendly arbitration and played a crucial role in justifying forced arbitration clauses in employment contracts.[292] And, as Lauren Edelman has shown, the corporate practices associated with Title VII—policy statements, diversity offices, bias training, and internal appeals—have performatively constructed what courts perceive anti-discrimination law to be.[293]

Scholars have argued this kind of hollowing out of traditional regulatory functions is the product of neoliberal hegemony.[294] That is undoubtedly true. Procedural governance in environmental, health, and financial regulation law may also reflect the performativity of compliance practices on the ground. Put another way, we have come to expect that regulation is a public-private partnership in which industry manages much of its own compliance. Therefore, the compliance model has created legal institutions in its own image.

But this erosion of public institutional power undermines the very mechanisms that are supposed to help compliance-based governance guard against its own devolution into regulatory capture and self-regulation. As the compliance model's proponents concede, compliance-based governance is subject to the risk of capture, because regulated companies themselves are

289. *See* DOUGLAS A. KYSAR, REGULATING FROM NOWHERE: ENVIRONMENTAL LAW AND THE SEARCH FOR OBJECTIVITY 100–05 (2010); Martha C. Nussbaum, *The Costs of Tragedy: Some Moral Limits of Cost-Benefit Analysis*, 29 J. LEGAL STUD. 1005, 1029–30 (2000); Amartya Sen, *The Discipline of Cost-Benefit Analysis*, 29 J. LEGAL STUD. 931, 936 (2000); Thomas O. McGarity, *The Goals of Environmental Legislation*, 31 B.C. ENV'T AFF. L. REV. 529, 551 (2004) (describing the Risk Assessment and Cost-Benefit Act of 1995, which would have required cost-benefit analyses in all regulatory programs); Cary Coglianese, *The Managerial Turn in Environmental Policy*, 17 N.Y.U. ENV'T L.J. 54, 55–60 (2008) (describing managerialism in environmental law).

290. *See* Britton-Purdy, Grewal, Kapczynski, & Rahman, *supra* note 22, at 1811–12.

291. *See* Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467, 485–86 (2020) (demonstrating how CFPB regulators outsource regulation of third parties to banks); Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 COLUM. L. REV. 369, 397–98 (2019) (describing the role of internal compliance departments in financial regulation as a form of "collaborative governance").

292. *See* Judith Resnick, *Diffusing Disputes: The Public in the Private of Arbitration, the Private in Courts, and the Erasure of Rights*, 124 YALE L.J. 2804, 2836–47 (2015).

293. *See* EDELMAN, *supra* note 47, at 13 ("Thus the meaning of law evolves over time in a way that is fundamentally influenced by the institutions that law is meant to regulate.").

294. *See* Britton-Purdy et al., *supra* note 22, at 1801–13.

creating compliance tools and participating in their own regulation.[295]Accordingly, effective governance presupposes the existence of a robust and effective regulator that is capable and prepared to act as a "backdrop threat" to ensure that industry is an honest partner as it works with public institutions to achieve social goals.[296] But, as noted above, one of the performative aspects of the model is the construction of public regulatory institutions that depend on industry expertise, input, capital, and workers to fulfill regulatory responsibilities. This dependence not only creates managerialized public institutions, but it also weakens the ability of government regulators to adequately function as enforcers ready to bring down the hammer of command-and-control if industry's compliance programs fail to rein in data-extractive practices.

However, the prospect of tethered regulatory agencies is far more likely than proponents suggest. When scholars describe the compliance model's diverse toolkit—from impact assessments to trainings and audits—they again make the epistemic error of considering the toolkit in a vacuum, divorced from the social context in which that toolkit is used. But compliance practices are not theories; they operate within organizational bureaucracies created to routinize productivity and profit.[297] Those bureaucracies can subordinate privacy structures to undermine accountability in any number of ways. Many companies push their CPO down the corporate hierarchy or subordinate them within risk management or compliance departments, forcing privacy to fight within systems focused on achieving substantially different goals.[298] Companies also shift control of privacy budgets to legal, compliance, or technology departments.[299] They also sideline privacy work. In self-reported surveys, privacy leaders report the greatest control over trainings, drafting policies, publications, communications, and travel, but far less responsibility for the practices that really matter in compliance-based governance: audits, data inventory, and

295. *See, e.g.*, Lobel, *Renew Deal*, *supra* note 125, at 385 (conceding that collaborative governance tools may be "used by management merely as mechanisms for monitoring, controlling, and exerting additional pressures on workers").

296. Kaminski, *supra* note 4, at 1561.

297. ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 210–31 (2021); *see generally* MAX WEBER, ECONOMY AND SOCIETY: AN OUTLINE OF INTERPRETIVE SOCIOLOGY (Guenther Roth & Claus Wittich eds., 1922) (describing the corporate bureaucracy as effective at channeling work toward capitalistic ends).

298. *See* WALDMAN, *supra* note 297, at 144–48; IAPP, BENCHMARKING PRIVACY MANAGEMENT AND INVESTMENTS OF THE FORTUNE 1000: REPORT ON FINDINGS FROM 2014 RESEARCH 23 (2014), https://iapp.org/media/pdf/resource_center/2014_Benchmarking_Report.pdf [https://perma.cc/99J8-YT7Z] (showing that Fortune 1000 privacy leaders ranked "compliance" as the most important priority for the company).

299. *Id.* at 32 (finding that 80 percent of privacy budgets are spent on salaries, legal counsel, software, and overhead, whereas other budget items like incident response, privacy-related monitoring, and privacy-related investigations comprise only 1-2 percent each); *see also* Andrew C. Inkpen & Eric W. K. Tsang, *Social Capital, Networks, and Knowledge Transfer*, 30 ACAD. MGMT. REV. 146, 147–150 (2005) (demonstrating that budget shifting can undermine a corporate department's authority).

technology.[300] Management also creates siloed privacy departments that appear robust, but have little impact on the company's work.[301] Therefore, privacy law's reliance on privacy professionals—even those who consider themselves privacy advocates—doing work in the public interest is misplaced. Companies are already exercising their financial and structural power to co-opt internal privacy advocates and turn their efforts away from meaningful privacy work.[302]

The information industry also routinely fires dissident employees, creating a chilling effect on others trying to push against the data-extractive tide. In August 2020, for example, Buzzfeed reported that Facebook punished a senior engineer for collecting evidence showing the company gave preferential treatment to conservative accounts.[303] Another Facebook employee who gathered evidence that the social network protected right-wing websites from the company's policies on misinformation had their internal access revoked, as well.[304] Google took the same approach to its employees who blew the whistle on the company's efforts to suppress unionization, its cozy relationship with outside advisers with long histories of homophobic and racist comments, and its entanglement with Customs and Border Protection.[305] Google even fired the prominent AI researcher Timnit Gebru for trying to publish a paper on language algorithms that threatened the company's bottom line.[306] This job insecurity has a chilling effect on tech-sector managers, dissuading them from speaking privacy truths to data-extractive power.[307]

Any one of these constraints—weakened privacy offices, precarity of employment, and siloization, alone, or in concert—weaken privacy law. Privacy departments that are siloed, starved for cash, and organizationally subservient to business units with independent or contrary interests have weaker voices in making policy. When advocates for accountability are fired, others may go silent. As a result, corporate obligations are framed in terms dictated by more powerful organizational actors, whether that is the general counsel, whose job it is to minimize legal risks to the company, or the vice president for technology, whose

300. IAPP, *supra* note 298, at 5, 23.

301. Ari Ezra Waldman, *supra* note 142, at 709–19 (2018).

302. WALDMAN, *supra* note 297, at 210–31.

303. Craig Silverman & Ryan Mac, *Facebook Fired an Employee Who Collected Evidence of Right-Wing Pages Getting Preferential Treatment*, BUZZFEED NEWS (Aug. 6, 2020), https://www.buzzfeednews.com/ article/craigsilverman/facebook-zuckerberg-what-if-trump-disputes-election-results [https://perma.cc/P94C-LX6J].

304. *Id.*

305. Noam Scheiber & Kate Conger, *The Great Google Revolt*, N.Y. TIMES (Feb. 18, 2020), https://www.nytimes.com/interactive/2020/02/18/magazine/google-revolt.html [https://perma.cc/8Z9D-YVXN.

306. Cade Metz & Daisuke Wakabayashi, *Google Researcher Says She Was Fired over Paper Highlighting Bias in A.I.*, N.Y. TIMES (Dec. 3, 2020), https://www.nytimes.com/2020/12/03/technology/google-researcher-timnit-gebru.html [https://perma.cc/L9F9-ZDFG].

307. *E.g.*, Robert A. Gorman & Matthew W. Finkin, *The Individual and the Requirement of "Concert" Under the National Labor Relations Act*, 130 U. PA. L. REV. 286, 344 (1981).

job it is to define the technical aspects of corporate practice. Neither of these actors is necessarily an active and overt anti-privacy voice. But the perspectives, goals, and metrics on which they are judged by their company are orthogonal to privacy and far more managerial. This makes it more likely that internal compliance practices will be framed and cabined to serve corporate interests rather than social and policy goals.

This creates a downward spiral. Compliance governance practices hollow out regulatory institutions by normalizing the expectation that industry will fill in gaps left open by underfunded, slow-moving, and untrained public regulators. At the same time, it relies on internal corporate structures that are not independent of industry, but rather entirely controlled and subordinated by industry bureaucracies that can easily game the system. In this world, there are no honest partners and no backdrop threats. There is only self-regulation and symbolic compliance.

IV.
A FRAMEWORK FOR RESISTANCE

Privacy law's social practices, including many that long predate the GDPR and the CCPA, should be understood as expressive performances that have socially constructed what we think privacy law is and should be.[308] Surfacing the performative aspects of privacy law practices may help explain why so many recent privacy proposals look so similar and why most of them will likely prove ineffective at protecting our privacy. Ever since the FTC started requiring privacy offices and programs alongside notice-and-consent, internal compliance and self-governance have socially constructed the category of *privacy law* and crowded out other options. But this status quo is insufficient to adequately serve privacy interests. It is too reliant on corporate goodwill and destructive to public governance. It is susceptible to gaming and internally inconsistent. And it perpetuates a misleading vision of the autonomous capacities of individual subjects to protect their privacy in a data-extractive economy. The world it creates is detrimental to privacy.

This Section suggests a radical alternative. Because it is difficult to escape the normalizing capacities of performative practices,[309] this Section provides a framework for thinking about, and developing, new discursive and behavioral performances that destabilize existing routines and generate democratic institutions of privacy governance.[310] By democratic, I mean that the information economy should be accountable "to those who live" within it.[311] And we should

308. *See supra* Part II.

309. *See, e.g.*, BUTLER, *supra* note 16, at x-xi (suggesting that identity only emerges from performance).

310. *See* Christine Overdevest, *Toward a More Pragmatic Sociology of Markets*, 40 THEORY & SOC'Y 533, 539 (2011) (discussing reforms to economic models using destabilizing techniques).

311. Britton-Purdy, Grewal, Kapczynski & Rahman, *supra* note 22, at 1827.

recognize that privacy law is not simply an exogenous institution that sets rules of the game for data use. As the economist Robert Hale noted, "the law confers on each person a wholly unique set of liberties with regard to the use of material goods and imposes on each person a unique set of restrictions with regard thereto."[312] In other words, the legal constructions of informational capitalism allocate market power, choosing winners and losers along the way.[313] By disclaiming any interest in the substantive rights and burdens of the information economy, the rights/compliance model has chosen industry over individuals, market actors over market subjects, and capital over consumers.

Following the work of the social philosopher André Gorz, I propose alternative performances focused not on protecting the current "needs, criteria, and rationales" of informational capitalism, but rather on "what should be," and the "fundamental political and economic changes" needed to turn what *ought* to be into what *is*.[314] In other words, I propose a series of "non-reformist reforms" or, non-reformist performances: practices on the ground that aim not at mere tinkering with the rights/compliance model, but rather aim at fundamentally transforming the relationship between individuals and technology companies.[315] I also borrow from the law and political economy literature to define this new framework in terms of three overlapping values: power, equality, and democracy.[316] Notably, there is no magic bullet or single set of proposals that will inevitably move us toward a fairer future. Progress is contingent, halting, and uncertain. But we must start somewhere.

A. Non-Reformist Performances

Gorz saw non-reformist reforms as a way to build a better world today, while preparing for the world we want tomorrow. Reforms are "non-reformist" when they help bring about radical change.[317] Popular social movements could wait for structures of oppression to collapse under their own contradictions, shying away from incremental reforms within current systems of power for fear of legitimizing the systems and delaying real social transformation. Or, they could build both better lives and greater consciousness for the people along the way to structural change. Non-reformist reforms do the latter.

312. ROBERT L. HALE, FREEDOM THROUGH LAW: PUBLIC CONTROL OF PRIVATE GOVERNING POWER 15 (1952).

313. COHEN, *supra* note 9, at 3–8.

314. GORZ, *supra* note 23, at 7–8.

315. Amna A. Akbar, *Demands for a Democratic Political Economy*, 134 HARV. L. REV. F. 90, 112 (2020).

316. Britton-Purdy, Grewal, Kapczynski & Rahman, *supra* note 22, at 1821, 1824, 1827.

317. Mark Engler & Paul Engler, André Gorz's Non-Reformist Reforms Show How We Can Transform the World Today, JACOBIN MAG. (July 22, 2021), https://www.jacobinmag.com/2021/07/andre-gorz-non-reformist-reforms-revolution-political-theory [https://perma.cc/6MP7-C3RC].

Amna Akbar's three essential characteristics of non-reformist reforms explain how to achieve this better world.[318] First, non-reformist reforms are never end goals; they are means to a transformative future. They are based not on a technocrat's assessment of what industry, or those in power, think is possible under the current regime. Rather, non-reformist reforms are meant to take us closer to what should be possible.[319] Second, non-reformist reforms are always pathways for "building ever-growing organized popular power."[320] This is as much about process as it is about substance. Non-reformist reforms come from social movements fighting for them, rather than being meted out by those in power.[321] The latter strengthens the system that disenfranchises social movements and ordinary people, while the former recenters power. Finally, non-reformist reforms are never singular answers to discrete policy questions.[322] They always aim at building popular power and, therefore, are part of a "broader array of strategies . . . for political, economic, [and] social transformation."[323] Non-reformist reforms are about "deepening consciousness, building independent power and membership, and expanding demands" all at the same time.[324] They are not about targeting a single issue at the expense of other social demands, values, and visions.[325]

Consider a pay raise for union workers. A reformist reform is a raise granted by management, at their behest and by their largesse; a non-reformist reform is a raise won through struggle, protest, and activism, a process that awakens workers to their own power. A reformist reform is a raise that results when raises, however high, are the workers' ultimate goal; a non-reformist reform is a raise that opens the door for more demands, more struggles against power, and greater consciousness among workers of the system's subordination of its workforce. And a reformist reform is a raise that stands on its own; a non-reformist reform, by contrast, is a raise that is part of a larger ecosystem of structural change aimed at empowering workers.

Gorz saw non-reformist reforms as ways of changing how the disempowered behave both amongst themselves and toward those in power. That focus on behavioral change surfaces a connection between non-reformist reforms and performativity. As discussed, our practices can be performative and habituating, locking the disempowered into non-existent, unsuccessful, or short-lived struggles against power. Therefore, non-reformist *performances* seek to empower individuals, materially improve the people's position vis-à-vis technology companies, and raise collective consciousness about data-driven

318. Akbar, *supra* note 315, at 112–17.
319. *Id.* at 115–16.
320. *Id.* at 116.
321. *Id.* at 115–16.
322. *Id.* at 118.
323. *Id.*
324. *Id.* at 106.
325. *Id.* at 118.

oppression and the rights/compliance model's complicity in the public's subordination to informational capitalism. And, like Judith Butler's theory of performativity itself, non-reformist performances start with discourse.[326]

B. Privacy Discourse

The theory of privacy-as-control embedded in the rights/compliance model maintains current structures of power. That is, although it seems empowering to be told that we should have control over when, how, and to whom we disclose our information, the reality is darker. As we have seen, performing individual rights of control habituates us into a false sense of control while technology companies weaponize our exercise of individual rights to immunize themselves from legal accountability.[327] New discursive performances can start the process of advancing social values over industry interests and raise popular consciousness in the process.

There is already a rich body of privacy scholarship eschewing the individual-focused discourses of control and choice. For example, some scholars talk about privacy in terms of loyalty.[328] Others argue that privacy is about the flow of information through and among social networks.[329] Helen Nissenbaum has focused privacy around "context-relative informational norms" that "govern[] the flows of personal information" in distinct social contexts, such as education, health care, and politics.[330] Julie Cohen has offered an even more robust conception of privacy. She argues that "[p]rivacy . . . protects the situated practices of boundary management through which the capacity for self-determination develops."[331] Neil Richards argued that "privacy is about the rules governing the extent to which human information is detected, collected, used, shared, and stored and how those activities can be used to affect our lives."[332]

But we can go further. Although these approaches to privacy are not centered solely on the individual and, therefore, do not perpetuate the idea that privacy is something we must govern ourselves, they are still agnostic as to ends. Some privacy scholarship is taking this next step. Danielle Citron has called for giving special weight to, and protection for, sexual privacy, pushing back against corporate surveillance of our sexuality, bodies, and intimate selves.[333] Her work takes an explicitly normative turn by elevating sexual privacy as far more worthy

326. Kenji Yoshino, *Covering*, 111 YALE L.J. 769, 868–69 (2002).

327. *See supra* Part III.A.2.

328. Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. (forthcoming 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3921799. *See also* DATA § 207 (duty of care); COPRA § 101 (duty of loyalty).

329. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919–88 (2005).

330. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 141 (2010).

331. Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1905 (2013).

332. NEIL RICHARDS, WHY PRIVACY MATTERS 3 (2021).

333. *See generally* Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019).

of legal protection than the profit-making whims of a company that thinks extracting data from intimate applications and pornography websites is the path to wealth.[334] For sexual privacy, procedure is not enough. Virginia Eubanks called for special attention to protecting the privacy of those on public assistance, in the child welfare system, and those who are unhoused.[335] Scott Skinner-Thompson argued that privacy law should adopt an anti-subordination approach that would protect the rights of the most vulnerable.[336] And Khiara Bridges expressed that privacy law should address structural socioeconomic inequality.[337] We could also think about privacy as a necessary element of human flourishing, or the realization of the whole person, including our physical well-being, happiness, self-determination, and more.[338] We need to quit thinking and talking about privacy in terms of choice and control, full stop. By leveraging the performative capacities of discourse—which is well underway in legal academia—we can change baseline assumptions about what privacy is for.

What if scholars and advocates started talking about privacy almost exclusively in terms of emancipation? Privacy is more than just a set of rules or a series of processes or even a set of norms. Privacy is a state of freedom from overlapping forms of subordination: corporate, institutional, and social. Privacy's emancipatory capacities underly Professor Citron's call for sexual privacy, which, if fully protected, would liberate women, LGBTQ+ people, and sexual minorities from oppressive social and institutional structures.[339] Emancipation sits at the center of Salomé Viljoen's call for democratizing data governance to liberate people from a system of datafication that enacts, reifies, and amplifies unjust and unequal social relations.[340] Scholars and advocates should adopt this language when speaking and thinking about privacy. Doing so will contribute to new ways of thinking about the role of privacy law, privacy litigation, and privacy wrongs.

C. Power and Policy

New discourses are important, but they only begin a process of countering privacy law's pro-industry performances. We should think about the kind of privacy performances we want in terms of power: to whom do they allocate power, from whom do they take power, and against whom is the law weaponized? To date, privacy law discourses and behaviors have empowered

334. *Id.* at 1874–75.

335. *See, e.g.*, VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018).

336. SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS 139–79 (2021).

337. *See generally* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017).

338. *See* MARTHA C. NUSSBAUM, CREATING CAPABILITIES: THE HUMAN DEVELOPMENT APPROACH (2011).

339. Citron, *supra* note 333, at 1874 ("We are free only insofar as we can manage the boundaries around our bodies and intimate activities.").

340. Viljoen, *supra* note 223, at 584.

industry to extract our data for profit with limited accountability. We can change that by redistributing power to the rest of us.[341]

Redistributing power means regulators will have to undertake different performances. Instead of partnering with industry, conceptualizing their regulatory role as industry partners, and occasionally requiring companies to pay compensatory fines, regulators must recognize that the data-extractive harms caused by industry are metastatic.[342] For example, Amazon agreed to pay $61.7 million in a settlement with the FTC, a number derived from adding up the precise amounts of tips the company stole from its delivery drivers over two years.[343] At less than 0.015 percent of the company's revenue in a single year, the fine is neither likely to have any material effect on Amazon nor deter future mischief.[344] But the harm Amazon caused to workers exceeds the lost compensation. Amazon's growth and profit stem from a business model that places impossible demands on underpaid workers while maintaining strict surveillance of worker life. Amazon workers cannot leave their posts to use the restroom; the company pays particularly low wages.[345] An investigation into Amazon's employment practices demonstrated that the company engages in a series of tactics, like siphoning tips, not simply to nickel-and-dime workers, but to encourage employees to leave, keeping wages down.[346] Surveillance keeps employees afraid. Stealing tips is part of a patchwork of strategies subordinating workers.[347]

Data processing harms also metastasize for users. The FTC fined Facebook $5 billion for its role in the Cambridge Analytica scandal, but it has had little effect.[348] Individual users were subject to manipulation by Cambridge Analytica because of how social networks function, the lack of regulation over what it means to "consent" to terms of service, and the capacity of data processing to create relational harms.[349] Facebook's fine was accompanied by marginal

341. *See* Britton-Purdy, Grewal, Kapczynski, & Rahman, *supra* note 22, at 1821; *see also* Akbar, *supra* note 315, at 112–17 (arguing for a "democratic political economy" where power is returned to "everyday people" and away from elites that "monopolize wealth and power").

342. *See* Paul Ohm, *Regulating at Scale*, 2 GEO. L. TECH. REV. 546, 546–47 (2018) (arguing that the exponential scale of some harms requires an approach different from linear regulation).

343. Agreement Containing Consent Order, *In re* Amazon.com, Inc., File No. 1923123 (F.T.C. Feb 2, 2021).

344. Shelley E. Kohan, *Amazon's Net Profit Soars 84% with Sales Hitting $386 Billion*, FORBES (Feb. 2, 2021), https://www.forbes.com/sites/shelleykohan/2021/02/02/amazons-net-profit-soars-84-with-sales-hitting-386-billion/?sh=429340591334 [https://perma.cc/46ED-5NCD].

345. David Leonhardt, *The Amazon Customers Don't See*, N.Y. TIMES (June 15, 2021), https://www.nytimes.com/2021/06/15/briefing/amazon-warehouse-investigation.html [https://perma.cc/F53M-TQT7].

346. *Id.*

347. *Id.*

348. Nilay Patel, *Facebook's $5 Billion FTC Fine Is an Embarrassing Joke*, VERGE (July 12, 2019), https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke [https://perma.cc/NHV6-MMA4].

349. *Id.*

changes in what third-party apps can do, but the company has not changed the underlying data processing mechanisms that subjected millions of users to Cambridge Analytica's data misuse.[350]

Regulators need new performances, ones that regulate business models based on subordinating workers and users rather than individual practices of oppression and data-extraction in isolation. Regulators will then be habituated into seeing their role as working on behalf of individuals to counter corporate power. The Department of Justice (DOJ) should be empowered to hold industry executives personally liable when they lie or mislead regulators in corporate privacy assessments.[351] In terms of new regulatory practices, many privacy advocates, and at least one current FTC Commissioner, have called on the FTC to litigate claims more often.[352] Congress must also empower the FTC to pursue more robust remedies, including disgorgement, to deter wrongful conduct by forcing defendants to give up profits derived from their illegal behavior.[353] Amazon did not just steal $61.7 million from its drivers; it also derived enormous profits from a booming delivery market during the COVID-19 pandemic in which it underpaid its workers while promising otherwise.[354] A percentage of customers likely used Amazon's services based on that promise.[355]

Since disgorgement of ill-gotten profits may have a stronger effect on corporate behavior, a similar model could rein in data misuse. Indeed, disgorgement need not only apply to money. Data collection feeds algorithmic processes that target individuals with advertisements; behavioral targeting, in fact, is at the core of the Internet business model. If microtargeted algorithms are the products of improper data collection, then the algorithms themselves are ill-gotten gains, and should be similarly disgorged. FTC Commissioner Rebecca Slaughter has already hinted that this would be a welcome shift in regulators' practices.[356]

---

350. *Id.*

351. MYOBA § 1352.

352. *Dissenting Statement of Commissioner Rohit Chopra, at 7, Regarding Zoom Video Communications, Inc., Commission File No. 1923167*, FED. TRADE COMM'N (Nov. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1582914/final_commissioner_chopra_dissenting_statement_on_zoom.pdf [https://perma.cc/5XEH-3W98] (stating that previous FTC litigation contributed to "strong outcomes and important development of the law").

353. *See* AMG Capital Mgmt., LLC v. F.T.C., 141 S. Ct. 1341, 1344 (2021) (holding that the FTC Act does not entitle the FTC to seek disgorgement and other equitable remedies). *See also* Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMEND. INST. (Mar. 23, 2021) https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/J2YT-ENDP].

354. Karen Weise, *Amazon's Profit Soars 220 Percent as Pandemic Drives Shopping Online*, N.Y. TIMES (May 12, 2021), https://www.nytimes.com/2021/04/29/technology/amazons-profits-triple.html [https://perma.cc/RGM5-99SN].

355. *See* Coxon v. S.E.C., 137 F. App'x 975, 976 (9th Cir. 2005) (stating the government need show "only a 'reasonable approximation of profits causally connected to the violation'" and could do that with the help of expert testimony).

356. Rebecca Kelly Slaughter, *Protecting Consumer Privacy in a Time of Crisis, Remarks of Acting Chairwoman Rebecca Kelly Slaughter*, 2 FED. TRADE COMM'N (Feb. 10, 2021),

We must also redistribute power away from the information industry by facilitating critical research about data-extractive technologies. Making radical changes in trade secrecy laws is an obvious first step.[357] But given industry's current monopoly over the raw data necessary to assess technology's social effects, the mass unionization of technology researchers employed by industry can shift power to those seeking to pull back the veil on corporate misdeeds. Google's summary firing of Timnit Gebru suggests that corporate-funded information research is not independent.[358] In Gebru's situation, a union could have acted as a check against retaliation, discrimination, or forcing internal technology researchers to "strike a positive tone" in their work.[359] Organized and empowered employees could push back on corporate development of technologies that harm marginalized populations. The rights/compliance model assumes that in-house compliance and privacy professionals will play the role of the privacy advocate. That is unlikely, given ordinary workplace pressures facing in-house compliance professionals.[360] A union for technology workers doing important research on information economy harms may help. In the spirit of non-reformist performances, the activism and struggles of unionization can also awaken technology company workers to their exploitation within organizational structures and their role in designing products explicitly aimed at extracting data and profits from subordinated consumers.[361]

The rights/compliance model of governance provides "rules of the game" without committing companies or society to any particular ends.[362] A radically different approach would create performances based on the principle of equality, or the basic notion that information systems should not create or entrench "social subordination."[363] That can start with changing how we make privacy law.

---

https://www.ftc.gov/public-statements/2021/02/remarks-commissioner-rebecca-kelly-slaughter-future-privacy-forum [https://perma.cc/WMD6-7NQS].

357. *See, e.g.*, Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018) (arguing for an end to trade secrecy protections for algorithmic systems used in sentencing).

358. Karen Hao, *We Read the Paper that Forced Timnit Gebru out of Google. Here's What It Says.*, MIT TECH. REV. (Dec. 4, 2020), https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/ [https://perma.cc/4EHC-PU7A].

359. Paresh Dave & Jeffrey Dastin, *Google Told Its Scientists to 'Strike a Positive Tone' in AI Research—Documents*, REUTERS (Dec. 23, 2020), https://www.reuters.com/article/us-alphabet-google-research-focus/google-told-its-scientists-to-strike-a-positive-tone-in-ai-research-documents-idUSKBN28X1CB [https://perma.cc/5XEN-ZYTM].

360. *See* Lauren B. Edelman, Stephen Petterson, Elizabeth Chambliss & Howard S. Erlanger, *Legal Ambiguity and the Politics of Compliance: Affirmative Action Officers' Dilemma*, 13 L. & POL'Y 73, 78 (1991) ("Tension . . . is often found in enforcement positions in organizations" where agents are subject to "conflicting pressures.").

361. WALDMAN, *supra* note 298, at 210–31.

362. Jones & Kaminski, *supra* note 229, at 110. Importantly, Kaminski and Jones do not claim that the GDPR is value-neutral or lacks substantive goals. *See, e.g.*, GDPR, *supra* note 3, at art. 9; rec. 71.

363. Britton-Purdy, Grewal, Kapczynski, & Rahman, *supra* note 22, at 1824.

Today, regulators and policymakers seek industry input.[364] They should instead give advocacy organizations representing marginalized populations, and not corporations, a seat at the table. Groups focused on the cyber civil rights of women, the poor, communities of color, survivors of intimate partner violence and nonconsensual pornography, sex workers, those living with disabilities, HIV+ individuals, and those who identify as LGBTQ+, among many others, may have unique perspectives on data use, its dangers, and its downstream consequences.[365] Those most likely to be subordinated by data practices should be in the room; those most likely to subordinate others should not be.[366] They may not always agree or have a single message, but they certainly have claims to seats at the table that are currently given to industry by default.

One of the results of decentering the needs of industry in privacy law is an emphasis on cyber civil rights.[367] Senator Sherrod Brown's bill, the Data Accountability and Transparency Act (DATA) of 2020, comes closest among recent proposals to doing this. Although the draft bill retains some of the rights/compliance framework, it creates an office of civil rights that would ensure data collection and use is "fair, equitable, and nondiscriminatory."[368] The proposal would prohibit any data aggregation that results in discrimination in housing, employment, credit, insurance, and public accommodations, or that has a disparate impact on marginalized populations.[369] It also makes it easier for victims to prove, and obtain justice for, disparate impact.[370] Of course, DATA is not immune from any of the problems discussed throughout this Article. But non-reformist reforms are consciously imperfect. DATA nods to the population-level harms that are endemic to business models dependent upon data-driven behavioral targeting. It is worth noting that in drafting his proposal, Senator Brown consulted exclusively with representatives of civil society and not with

364. *See supra* Part II.A.1.

365. *See, e.g.*, CYBER C.R. INITIATIVE, www.cybercivilrights.org [https://perma.cc/R6AN-Q4DR]; DETROIT CMTY. TECH. PROJECT, https://www.detroitcommunitytech.org/ [https://perma.cc/XT3J-84LU]; DATA 4 BLACK LIVES, https://d4bl.org/ [https://perma.cc/3V76-B5E4]; NAT'L NETWORK TO END DOMESTIC VIOLENCE, https://nnedv.org/ [https://perma.cc/DC5V-PNYS].

366. I recognize the complexity in identifying specific groups. Many groups that are subordinated by structures of power are also part of structures of power that oppress others. This is not only true because individuals possess intersectional identities that connect them to different positions in power relations, but also because data processing empowers some and not others. Suffice it to say, policymakers' goal should not be to do what industry thinks is possible or preferable, but to listen to those who are harmed.

367. Danielle Citron proposed a cyber civil rights agenda more than a decade ago. *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 61 (2009).

368. DATA § 301(b)(1).

369. *Id.* at § 104 (shifting the burden of proof to the data aggregator to show absence of discrimination or other alternatives to discrimination).

370. *Id.*

industry.[371] Senator Brown's decision to focus on equality, rather than on what corporations would accept, is a welcome model for new privacy performances.

Frank Pasquale also has a provocative proposal for "ex ante licensing of large-scale data collection . . . in jurisdictions committed to enabling democratic governance of personal data."[372] Pasquale proposes a stricter version of Senator Brown's DATA that would require data brokers to obtain a license from the government in order to process large data sets of personal information.[373] This proposal sounds radical, but the notion that some information is too sensitive to use for business purposes is commonplace. For instance, we criminalize the dissemination of a person's bank account information, and universities require researchers to obtain approval before engaging in any human-subject research.[374] In other words, we place limits on gathering and sharing information about real people all the time because we are concerned about both the downstream effects and social values that are lost if we did not. Pasquale argued that an *ex ante* licensing regime would be the only way to protect the population, particularly the most marginalized, from "systematic efforts to typecast individuals, to keep them monitored in their place, or to ransack databases for ways to manipulate them."[375] Managerialized compliance cannot do this, nor does it even try. It is content with managing data collection and trying to regulate it *ex post*, after it is used and after it likely has already had an effect on social life.

D. Democracy and Protest

Non-reformist reforms come from the people, through struggle, and via the power of social movements. Therefore, alternative privacy performances must be part of broader social movements for structural change. The rights/compliance model for privacy law is the opposite. As this Article has shown, the model is the product of the practices of industry, designed to keep corporations in power while providing the veneer of accountability to silence and demoralize advocates for change.[376] Successful non-reformist reforms hinge on people power. Real change in our relationship with the information industry can only come if we fight for it, raising consciousness about our collective power in the process.

---

371. *Brown Releases New Proposal that Would Protect Consumers' Privacy from Bad Actors*, SHERROD BROWN: U.S. SENATOR OF OHIO (June 18, 2020), https://www.brown.senate.gov/newsroom/press/release/brown-proposal-protect-consumers-privacy [https://perma.cc/HG6L-933M]; *Statements by Privacy Experts and Civil Rights and Consumer Organizations*, U.S. SENATE COMM. BANKING, HOUS. & URBAN AFFS. (2020), https://www.banking.senate.gov/imo/media/doc/DATA%202020%20-%20statements%20by%20organizations2.pdf [https://perma.cc/8JRS-9AJN].

372. Frank Pasquale, *Licensing Big Data Analytics in an Era of Invasive and Contested AI*, at *1 (unpublished manuscript on file with author).

373. *Id.*

374. *Id.*

375. *Id.* at *12.

376. *See supra* Part III.B.3.

Informational capitalism does not make that easy. Our economy is built to hide its horrors. Industrial capitalism left scars—soot, illness, death; informational capitalism leaves few scars as visible on the surface, but the wounds are still deep.[377] Privacy and data breach harms are often intangible,[378] and the law's entanglements with industry are invisible.[379] The closest social movements have come to a galvanizing ground-up campaign for data justice is "Fuck the Algorithm," a slogan used by a group of high school students in the United Kingdom whose algorithmically-determined final grades were lower than their performance suggested they should be.[380] The intangible nature of privacy harms and the entanglements of industry make it harder for privacy to galvanize popular movements for structural reform. That must change. Advocacy groups of all sorts must make privacy a centerpiece of their activist platforms. After all, privacy has always been a matter of gender equality,[381] racial justice,[382] and LGBTQ+ liberation.[383]

That these ideas—cyber civil rights, data licensing, research funding, unionization, and "egalitarian" free speech—do not seem to fit within privacy law's traditional purview speaks to the myopia that has characterized privacy law to date. Privacy law is not merely about data. It is also about the effects on society of data and data use. The narrowness of the rights/compliance model has benefited industry at our expense by disaggregating values from data governance. By focusing primarily on data collection and data management, traditional privacy law is siloed from the social contexts affected by data collection and use. New performances can help us find a different way.

CONCLUSION

This Article challenges a growing conventional wisdom in privacy scholarship. That narrative—namely, that the E.U.'s or California's legal entrepreneurship explains today's interest in privacy legislation among U.S. policymakers—is fundamentally flawed. It elides the fact that many privacy law practices codified in these new laws predate both the GDPR and the CCPA. It is

377. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 94, 195, 345–47 (2019).

378. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. (forthcoming 2022) (manuscript at 3), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222 [https://perma.cc/8W7H-TX8E].

379. COHEN, *supra* note 9.

380. Karen Hao, *The UK Exam Debacle Reminds Us that Algorithms Can't Fix Broken Systems*, MIT TECH. REV. (Aug. 20, 2020), https://www.technologyreview.com/2020/08/20/1007502/uk-exam-algorithm-cant-fix-broken-system/ [https://perma.cc/E5FG-ER42].

381. *See, e.g.*, ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1998); Citron, *supra* note 333, at 1890–1897; Citron, *supra* note 367; Daniele Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014).

382. *See, e.g.*, BRIDGES, *supra* note 337; NOBLE, *supra* note 278, at 1, 27–28; BENJAMIN, *supra* note 278.

383. *See, e.g.*, SKINNER-THOMPSON, *supra* note 336.

also based on a fundamental misconception of law as autonomous from its social context.

In place of this top-down narrative, this Article relies on sociological and critical studies literatures to argue that recent proposals for comprehensive privacy law adopt roughly similar rights/compliance approaches because long-standing privacy law practices are performative. The routinized performance of internal privacy offices, impact assessments, audits, record-keeping, regulatory-industry partnerships, and privacy self-management has socially constructed privacy law from the ground up. Put another way, we think privacy should look a certain way because we are accustomed to doing it that way. Unfortunately, we are acculturated to a privacy regime that actually undermines privacy. Following the emerging law and political economy research agenda, the Article proposes a framework based on principles of power, equality, and democracy. The framework offers some alternative performances that can tear down barriers to accountability, break up conventional routines, and destabilize industry's asymmetrical power.

This Article has also made independent contributions to legal theory and has implications beyond privacy law. Performativity in legal scholarship has been exclusively used in the traditional sense of performing identity. This Article suggests that we can also perform—and, therefore, socially construct—entire legal regimes through our actions and discourses. That has important implications for a variety of legal fields. It also gives us a path forward. Privacy advocacy may sometimes seem like tilting at windmills, but all we need are new performances. Given the centrality of privacy in today's political debates, we now have a unique opportunity to shift the course of privacy law from its inadequate past to a new, democratic future.