PRIVACY LAW'S FALSE PROMISE

ARI EZRA WALDMAN*

ABSTRACT

Privacy laws have never seemed stronger. New international, national, state, and local laws have been passed with the promise of greater protection for consumers. Courts across the globe are reclaiming the law's power to limit collection of our data. And yet, our privacy seems more in danger now than ever, with frequent admissions of nefarious data use practices from social media, mobile apps, and e-commerce websites, among others. Why are privacy laws, seemingly more comprehensive than ever, not working to protect our privacy? This Article explains.

Based on original primary source research—interviews with engineers, privacy professionals, and vendor executives; product demonstrations; webinars, blogs, industry literature; and more—this Article argues that privacy law is failing to deliver its promised protections because it is undergoing a process of legal endogeneity: mere symbols of compliance are standing in for real privacy protections. Toothless trainings, audits, and paper trails, among other symbols, are being confused for actual adherence to privacy law, which has the effect of undermining the promise of greater privacy protection for consumers.

* Microsoft Visiting Professor of Information Technology Law, Princeton University, Center for Information Technology Policy. Professor of Law and Director, Innovation Center for Law and Technology, New York Law School. Affiliate Fellow, Yale Law School Information Society Project. PhD, Columbia University; J.D., Harvard Law School. This Article received the Best Paper Award at the 2019 Privacy Law Scholars Conference. The Article benefited from feedback from faculty and students at the Privacy Research Group at New York University School of Law, Cornell Law School, New York Law School's Faculty Colloquium, Yale Law School's Information Society Project, and Fordham Law School. Special thanks, in alphabetical order, to Vigjilenca Abazi, Philip Bender, Jody Blank, Joseph Calendrino, Celine Castets-Renard, Danielle Keats Citron, Julie Cohen, Rebecca Crootoff, John Duffy, Lauren Edelman, Sue Glueck, Nikolas Guggenberger, Woodrow Hartzog, Joris van Hoboken, Chris J. Hoofnagle, Ariel Fox Johnson, Thomas Kadri, Mike Kwet, Karen Levy, Asaf Lubin, Mason Marks, Emily McReynolds, James A. Mourey, Frank Munger, Peter Omerod, Przemyslaw Palka, Jon Penney, Ed Purcell, Priscilla Regan, Joel Reidenberg, Neil Richards, Ira Rubinstein, Paul Schwartz, Eli Seims, Andrew Selbst, Jake Sherkow, Richard Sherwin, Liron Shilo, Priscilla Smith, Daniel J. Solove, Kathy Strandburg, Olivier Sylvain, Michael Veale, Christopher Wolf, and Felix Wu. Essential research assistance was provided by Lauren Davenport, Monica Meiterman, and Maverick James. Funding for this research was provided by New York Law School's Summer Research Grant.

TABLE OF CONTENTS

INTRODUCTION

The people we trust with our data are putting our privacy at risk. Facebook has long been cavalier about protecting personal information from third parties.[1] Mobile app platforms routinely sweep in user data merely because they can.[2] Manufacturers of toasters,[3] toothbrushes,[4] and sex toys[5] are wiring up everything to the Internet of Things, tracking

1. *See* Josh Constine & Taylor Hatmaker, *Facebook Admits Cambridge Analytica Hijacked Data on Up to 87M Users*, TECHCRUNCH (Apr. 4, 2018, 1:30 PM), https://techcrunch.com/2018/04/04/cambridge-analytica-87-million/ [https://perma.cc/L54K-3X7U].

2. *See* Robert McMillan, *The Hidden Privacy Threat of ... Flashlight Apps?*, WIRED (Oct. 20, 2014, 6:30 AM), https://www.wired.com/2014/10/iphone-apps/ [https://perma.cc/28K9-7J9Z].

3. *See Die-Cast 2-Slice Smart Toaster*, BREVILLE, https://www.breville.com/us/en/products/toasters/bta820.html [https://perma.cc/4AK6-GWTP].

4. *See Why Switch to a Bluetooth Electric Toothbrush?*, ORAL-B, https://oralb.com/en-us/products/compare/bluetooth [https://perma.cc/Z3V6-E9ZY].

5. *See* Cory Doctorow, *The Internet of Connected Sex Toys Is Every Bit as Horrifyingly Insecure and Poorly Thought Out as You Imagine*, BOINGBOING (Feb. 2, 2018, 9:28 AM), https://boingboing.net/

intimate behaviors while giving hackers countless opportunities for mischief.[6] Facial recognition technology proliferates despite its Orwellian dangers.[7] Even academic researchers are mining intimate data without our consent.[8] Our privacy is in danger. And the laws that are supposed to protect us do not seem to be working. This Article explains why.

Privacy law—a combination of statutes, constitutional norms, regulatory orders, and court decisions—has never seemed stronger. The European Union's General Data Protection Regulation (GDPR)[9] has been called "comprehensive"[10] and "one of the strictest privacy laws in the world."[11] California's Consumer Privacy Act (CCPA)[12] stakes out similar ground.[13] The Federal Trade Commission's (FTC's) broad regulatory arsenal is putting limits on the collection, use, and manipulation of personal information.[14] The U.S. Supreme Court has started to reclaim the Fourth Amendment's historical commitment to curtailing pervasive police surveillance by requiring warrants for cell-site location data.[15] And the E.U.

2018/02/02/sarah-jamie-lewis.html [https://perma.cc/W2ZJ-TTHW]; *see also* THE INTERNET OF DONGS PROJECT, https://internetofdon.gs/ [perma.cc/F5EN-PSRW].

6. See Scott R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 TEX. L. REV. 85 (2014).

7. *See* Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/X55V-FAG5].

8. *See* Woodrow Hartzog, *There Is No Such Thing as "Public" Data*, SLATE (May 19, 2016, 9:15 AM), http://www.slate.com/articles/technology/future_tense/2016/05/okcupid_s_data_leak_shows_there_s_no_such_thing_as_public_data.html [https://perma.cc/47PT-8Z9A]; Taylor Hatmaker, *In 2006, Harvard Also Conducted a Facebook Study that Went Too Far*, DAILY DOT (July 12, 2014, 10:55 AM), https://www.dailydot.com/debug/facebook-t3-study-tastes-ties-time/ [perma.cc/SV6K-SBTW].

9. *See* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, May 4, 2016, 2016 O.J. (L 119) [hereinafter GDPR].

10. William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 963 (2016).

11. Daniel Solove, *Beyond GDPR: The Challenge of Global Privacy Compliance—An Interview with Lothar Determann*, TEACHPRIVACY (Nov. 13, 2017), https://teachprivacy.com/challenge-of-global-privacy-compliance/ [https://perma.cc/4956-Q6TK].

12. *See* CAL. CIV. CODE § 1798.100 (West 2018).

13. *See* Lydia de la Torre, *GDPR Matchup: The California Consumer Privacy Act 2018*, IAPP PRIVACY TRACKER (July 31, 2018), https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/ [https://perma.cc/53CF-B3JJ] (comparing the GDPR and the CCPA and showing how the latter is broader than the former in certain respects). Almost every media outlet reporting on the CCPA has called it the "toughest" or "strictest" privacy law in the United States. *See, e.g.*, April Glaser, *California Just Passed the Strictest Online Privacy Bill in the Country*, SLATE (June 28, 2018, 6:34 PM), https://slate.com/technology/2018/06/california-just-passed-the-strictest-online-privacy-bill-in-the-country.html [https://perma.cc/LC54-B98V].

14. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 145–192 (2016) (describing the origins and multiple ways the FTC protects the privacy of U.S. consumers); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 627–48 (2014) (arguing that the FTC's privacy jurisprudence should be understood as an emerging common law that grows and adapts with new technologies and challenges).

15. Carpenter v. United States, 138 S. Ct. 2206 (2018) (requiring the government to obtain a warrant before acquiring cell-site location data); *see also* Riley v. California, 134 S. Ct. 2473 (2014)

Court of Justice has challenged the cross-border transfer of European citizens' data, signaling that American companies need to do far more to protect personal information.[16]

This seems remarkably comprehensive. But the law's veneer of protection is hiding the fact that it is built on a house of cards. Privacy law is failing to deliver its promised protections in part because the corporate practice of privacy reconceptualizes adherence to privacy law as a compliance, rather than a substantive, task. Corporate privacy practices today are, to use Julie Cohen's term, managerial.[17] They prioritize innovation over regulation, efficiency over social welfare, and paperwork over substance. They also rely on new technologies to automate legal decisions. This Article provides the first picture of this growing privacy compliance market. Based on original primary source research into the ecosystem of privacy compliance, I argue that privacy law is experiencing a process of *legal endogeneity*: mere symbols of compliance are standing in for real privacy protections.

This development is new for privacy, but not new for the law. Legal endogeneity, as theorized by the socio-legal scholar Lauren Edelman,[18] describes how the law, rather than constraining or guiding the behavior of regulated entities, is actually shaped by ideas emerging from the space the law seeks to regulate.[19] It occurs when compliance professionals on the ground have significant power to define what the law means in practice. When given that opportunity, compliance professionals often frame the law in accordance with managerial values like operational efficiency and reducing corporate risk rather than the substantive goals the law is meant to achieve, like consumer protection or equality. This opens the door for companies to create structures, policies, and protocols that comply with the law in name only.[20] As these symbolic structures become more common, judges and policymakers defer to them as paradigms of best practices or as evidence for an affirmative defense or safe harbor, mistaking mere symbols

(declaring warrantless search of an arrestee's cell phone unconstitutional); United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) ("[L]onger term GPS monitoring . . . impinges on expectations of privacy.").

16. *See* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650 (declaring the Safe Harbor arrangement, which allowed the transfer of data to the United States, unconstitutional because it did not adequately protect the privacy of EU citizens).

17. *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 7, 143 (2019); *see also id.* at 143–47 (arguing that managerialization of law is a product of the neoliberal project focused on governmental efficiency, nonintervention, and innovation at all costs).

18. *See* LAUREN B. EDELMAN, WORKING LAW: COURTS, CORPORATIONS, AND SYMBOLIC CIVIL RIGHTS (2016) (developing the theory of legal endogeneity in the context of Title VII and workplace sex discrimination law).

19. *Id.* at 12, 22.

20. *Id.* at 14.

of compliance with adherence to legal mandates.[21] When this happens, law fails to achieve substantive goals because the compliance metric—the adoption of symbols, processes, procedures, and policies within a corporate environment—may be orthogonal to actual progress. Edelman discussed legal endogeneity in the context of race and sex discrimination in the workplace, where the equality goals of Title VII of the Civil Rights Act were being frustrated by the ineffectual trainings, toothless policies, checklists, and disempowered diversity offices that compliance professionals created on the ground.[22] As this Article shows, the problem is far more pervasive than even Edelman suggested.

I present original research showing that privacy standards are being co-opted into corporate compliance structures that provide little to no protection. Each of the stages of legal endogeneity that Edelman noted is evident. Some of privacy law's most important tools—including privacy by design, consent requirements, and FTC consent decrees—are so unclear that professionals on the ground have wide latitude to frame the law's requirements, kicking endogeneity into high gear. Where rules are clear, they are so process-oriented that technological tools can create paper trails that may take the place of actual adherence to the law. And because those determining privacy law's meaning often reflect corporate or managerial—rather than consumer—interests, consumers more often than not lose out.

Scholars have documented the role that chief privacy officers (CPOs)[23] and engineers[24] play in implementing privacy law. But they are not alone.[25] Compliance professionals, marketing officers, outside auditors, human resource experts, and in-house and firm lawyers, just to name a few, "managerialize" privacy law, bringing in and prioritizing neoliberal values of efficiency and innovation in the implementation of privacy law.[26] They help shift the locus of legal decision-making from the legislature to the C-

21. *Id.* at 12–13.

22. *Id.* at 11.

23. *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015) (describing how nine leading privacy professionals at multinational corporations fill in gaps left open by privacy law); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011) (similar).

24. *See* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659 (2018) (arguing that engineers integrate a narrow vision of privacy law into the designs of technology products they create).

25. As the sociologists of technology Wiebe Bijker and Trevor Pinch have shown, there are many social groups influencing the use, perceptions of, and social construction of new technologies. Trevor J. Pinch & Wiebe E. Bijker, *The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other*, *in* THE SOCIAL CONSTRUCTION OF TECHNOLOGICAL SYSTEMS 11 (Wiebe E. Bijker et al. eds., 2012) (describing the authors' social construction of technology, or SCOT, model).

26. *See* COHEN, *supra* note 17, at 143–47.

suite, think about privacy in managerial terms, and often create symbolic structures of compliance—from paper trails to formalistic, but insubstantial privacy checklists—with the goal of minimizing the risk of privacy litigation, investigation, and exogenous shocks, not of enhanced privacy protection for consumers.

There are, indeed, many privacy professionals working hard to protect consumer privacy. But they are pushing against a powerful tide. If left unabated, privacy's managerialization will have profound and troubling implications for privacy law, the technology industry, users, and society. As more technology companies paint creative pictures of their legal compliance, lawyers and judges become more likely to defer to the toothless structures companies create by either accepting them as evidence of substantive adherence to the law[27] or actually incorporating them into statutes, thereby undermining the capacity for law to achieve more robust privacy protections for users.[28] This does real damage to our quest for more privacy.

It also undermines the rule of law. The rise of merely symbolic structures neuters the ability of legislation to enact social policy: why pass a law to achieve positive social change if its goals are going to be frustrated in practice? Moreover, as the locus of legal decision-making shifts further away from policymakers to corporate managers, the substantive and procedural protections in the laws on the books may dissipate.[29]

This is a critical moment in the fight against the false hegemony of symbolic compliance in privacy law. Laws like the GDPR and the CCPA are still new, the FTC's agile approach to consumer protection can be redirected away from blind deference to corporate structures, and consumers have a chance to make their collective voices heard. We can still reverse course. There are roles for compliance and compliance professionals to play, but the use of process to undermine substance is not one of them. All levels of the consumer privacy ecosystem—from lawmakers to civil society to academics—can aid in this effort. Crafting an approach to privacy law that advances both corporate and consumer interests will require understanding how we got here; how lawyers, consultants, and technology vendors can do better; and how the social process of law can honestly

27. *See* Ian Kerr & Carissima Mathen, Chief Justice John Roberts Is a Robot (Apr. 1, 2014) (working paper) (on file with University of Ottawa), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3395885 (discussing the difference between mere compliance and actual adherence to the law).

28. *See* EDELMAN, *supra* note 18, at 153–96 (describing how law has deferred to and incorporated the symbolic structures of Title VII compliance).

29. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008) (arguing that decision-making via algorithm eviscerates traditional due process protections afforded to agency decision-making).

translate privacy's laws on the books to real privacy protections on the ground. These are the goals of this Article.

Part I pushes back against the temptation to talk about law in a vacuum. Rather, this Part describes the ecosystem of what I call the social practice of privacy law, including the lawyers, regulators, state attorneys-general, CPOs, privacy professionals, in-house engineers, and vendors, among other social groups, that play critical roles in implementing privacy law on the ground. Part II describes the narrative of legal endogeneity and argues that some compliance approaches can undermine substantive privacy protections for consumers by facilitating the creation of merely symbolic structures of compliance. This section relies on new primary source material, qualitative and quantitative research, and insights into privacy compliance inside technology companies never before discussed in the literature. I demonstrate for the first time how different social groups within a corporate organization and their approaches to privacy law contribute to the problem. Finally, Part III addresses the dangers of legal endogeneity head on, identifying ways in which companies can actually support substantive, pro-consumer privacy law, and recommending changes to the law and how we can better translate the promise of privacy law into practice. I conclude with a summary of my findings, responses to potential objections, and a discussion of next steps in this research agenda.

Before I begin my analysis, I would like to briefly discuss my research methods. Because the different social actors involved in privacy compliance are underexplored, I conducted primary source research to identify market players and analyze the ways in which they, and their relationships to privacy professionals, engineers, and lawyers, are affecting privacy law. I attended privacy industry conferences, including the International Association of Privacy Professionals (IAPP) national conference, "Privacy. Security. Risk. 2017"; the 2018 and 2019 International Privacy+Security Fora; the 2018 Privacy+Security Forum, organized by leading privacy scholars Dan Solove and Paul Schwartz; the Annual Forum of the European School of Management and Technology (ESMT); and CyberWeek 2018, organized by the University of Tel Aviv.[30] At these conferences, I met and either scheduled or conducted semi-structured interviews with privacy professionals in various industries, including high technology, aerospace, retail, finance, and travel.

Based on this work, desk research, industry profiles, and advice from leading privacy scholars, I identified third-party compliance vendors in the

30. The author was invited to speak at the IAPP conference, the ESMT Annual Forum, CyberWeek 2018, and the 2019 International Privacy+Security Forum. Funding for travel to the IAPP conference, the ESMT Annual Forum, and CyberWeek 2018 was provided by the organizers of those conferences.

privacy space. I distributed a survey and conducted interviews with individuals at technology companies and their vendors to elicit themes in their conceptualization of privacy and their responsibilities to their clients. I used interviews with representatives to follow up on and fill gaps in publicly available information about their services. Many were eager to speak about their work. To varying degrees, interviewees either received permission to speak on the record as a representative of their employer or preferred to speak anonymously pursuant to confidentiality agreements. Public comments in news outlets and research conducted by other scholars also informed my research.

In order to determine how privacy professionals, lawyers, and compliance vendors understood privacy law and how they conceptualized their responsibilities and goals, and to minimize response biases from surveys,[31] I participated in webinars hosted by companies and the IAPP, read their and law firm blogs, and reviewed articles in industry journals geared toward privacy professionals. This research supplemented a twenty-month-long project of interviewing leading figures in the privacy and design space, including privacy professionals, in-house and firm lawyers, and engineers engaged in design.[32] Primary source fieldwork also supplemented traditional legal research into privacy statutes, cases, and regulatory orders, both in the United States and in Europe. European privacy law was included because of the outsized impact the GDPR is already having on technology companies worldwide.

I. THE SOCIAL PRACTICE OF PRIVACY LAW

Most scholars approach privacy law as a top-down phenomenon, studying how constitutional law, legislation, and court decisions affect the collection and use of our data.[33] Though undoubtedly essential, this fertile

31. Response bias refers to a series of tendencies in which survey respondents do not answer questions honestly. I was particularly concerned with what social scientists call social desirability bias, where survey respondents answer questions in ways that make them appear more favorable to the experimenter. *See, e.g.*, Anton J. Nederhof, *Methods of Coping with Social Desirability Bias: A Review*, 15 EUR. J. SOC. PSYCHOL. 263 (1985) (collecting the literature).

32. This series of interviews included those conducted for a related research project. *See* Waldman, *supra* note 24, at 678–79 (discussing research methodology). Those interviewees were originally identified via snowball sampling, but biases of the data set were limited by use of more randomized interview recruitment (at engineering conferences and through listservs). *See* James S. Coleman, *Relational Analysis: The Study of Social Organizations with Survey Methods*, HUM. ORG., Winter 1958–1959, at 28, 28–29 (discussing methodologies).

33. For example, Orin Kerr has studied the Fourth Amendment in a long research agenda too voluminous to cite here. *See, e.g.*, Orin S. Kerr, *Cross-Enforcement of the Fourth Amendment*, 132 HARV. L. REV. 471 (2018); Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 MICH. L. REV. 1117 (2017). Neil Richards has explored the interaction between privacy and the First Amendment. *See, e.g.*, Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005). So has Margot Kaminski. *See, e.g.*, Margot E. Kaminski, *Privacy and the*

research agenda is incomplete. Insufficient attention has been paid to the social structures on the ground—the people, professional organizations, and corporations—that not only turn law into action, but do far more work than legislators and judges in determining what the law means in practice.

A. The Legal Experts

That is starting to change. Several scholars have studied how real people affect privacy law. Chris Hoofnagle, Daniel Solove, and Woodrow Hartzog have shown how FTC commissioners assumed the role of de facto privacy regulators under their authority to police "unfair and deceptive" business practices.[34] It did not have to be that way. By the late 1990s, FTC commissioners recognized that digital and internet technologies were changing the commercial relationship between producers and consumers, saddling the latter with privacy risks while gifting the former opportunities for predation and manipulation.[35] The FTC's assertion of regulatory power has been so successful that lawyers and privacy professionals treat FTC consent decrees as a kind of common law from which to learn details about their legal obligations.[36]

Danielle Citron recognized that practitioners on the ground can also affect the implementation of privacy laws when she explored the agile privacy work of state attorneys general (AGs), long active but overlooked privacy enforcers.[37] Citron found that state AGs can effectively implement the privacy laws their legislatures pass and can set policy through enforcement activity because they benefit from a combination of broad legal authority, local knowledge, office specialization, and coordination with colleagues across the country.[38] They are also less constrained by the politics that can paralyze federal agencies.[39] As a result, state AGs have become the "front line[] of privacy enforcement."[40] In 2017, for example,

---

Right to Record, 97 B.U. L. REV. 167 (2017); Margot E. Kaminski et al., *SIRI-OUSLY 2.0: What Artificial Intelligence Reveals About the First Amendment*, 101 MINN. L. REV. 2481 (2017).

34. *See* 15 U.S.C. § 45(a)(1) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."). The FTC was given the authority to prevent such practices in subsection (a)(2). 15 U.S.C. § 45(a)(2); *see also* Solove & Hartzog, *supra* note 14, at 599–600; HOOFNAGLE, *supra* note 14, at 119–23.

35. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 1–3 (2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [https://perma.cc/5K3U-55YR].

36. *See* Solove & Hartzog, *supra* note 14, at 607.

37. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016) (showing how state attorneys general can be more effective than federal regulators at privacy enforcement, but also face certain hurdles and employ ineffective policies).

38. *See id.* at 786–95.

39. *See id.* at 750, 786.

40. *Id.* at 749.

state AGs, alone or in concert, reached settlements on data breach and privacy claims with Target,[41] Lenovo,[42] Hilton,[43] VIZIO,[44] and a handful of other corporations, and initiated actions against Equifax.[45]

They have also had a substantial impact on defining what the law means and how it will be implemented. Guidance documents like California's mobile privacy-focused *Privacy on the Go* provide examples of what companies should and should not do to comply with various state privacy laws.[46] And *Making Your Privacy Practices Public* takes the vague requirement in the California Online Privacy Protection Act that privacy policies should be "conspicuous"[47] and translates that into specific recommendations on readability and design.[48] The Texas AG's office took generalized language in the Children's Online Privacy Protection Act and concluded that collecting location data from anyone under thirteen years old violates the law.[49] And the California AG has convened working groups with Silicon Valley technology companies and persuaded them to adopt certain practices, not explicitly required by state law, on mobile privacy and nonconsensual pornography.[50] State AGs may not have written the privacy laws.[51] However, as Citron showed, they infuse the law with pro-consumer

41. In re Investigation by Eric T. Schneiderman, Att'y Gen. of the State of N.Y., of Target Corp.,, No. 17-094 (May 15, 2017), https://ag.ny.gov/s ites/default/files/nyag_target_settlement.pdf [perma.cc/927E-U5GN].

42. Press Release, Office of the Att'y Gen., Attorney General Becerra Announces $3.5M Settlement with Lenovo for Preinstalling Software that Compromised Security of Its Computers (Sept. 5, 2017), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-35m-settlement-lenovo-preinstalling-software [https://perma.cc/C9PT-7VWJ].

43. Press Release, Office of the Att'y Gen., A.G. Schneiderman Announces $700,000 Joint Settlement with Hilton After Data Breach Exposed Hundreds of Thousands of Credit Card Numbers (Oct. 31, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-700000-joint-settlement-hilton-after-data-breach-exposed [https://perma.cc/AEV5-PDCV].

44. Stipulated Order for Permanent Injunction and Monetary Judgment, Fed. Trade Comm'n. v. VIZIO, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), http://nj.gov/oag/newsreleases17/Vizio-Order.pdf [perma.cc/U6NZ-HQGJ].

45. Memorandum in Support of Plaintiffs' Motion for Transfer of Actions to the Northern District of Georgia and for Consolidation Pursuant to 28 U.S.C. § 1407, *In re* Equifax, Inc. Data Breach Litig., MDL No. 2800 (J.P.M.L. Sept. 11, 2017), http://www.almcms.com/contrib/content/uploads/sites/292/2017/09/Equifax-MDL-motion.pdf [perma.cc/K4ZC-W6VN].

46. *See, e.g.*, KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf [perma.cc/VDZ5-VZJ2]; Citron, *supra* note 37, at 760.

47. CAL. BUS. & PROF. CODE § 22575(a) (West 2018).

48. *See* KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, MAKING YOUR PRIVACY PRACTICES PUBLIC: RECOMMENDATIONS ON DEVELOPING A MEANINGFUL PRIVACY POLICY 9–10 (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf [perma.cc/QMZ6-2G7U].

49. *See* Citron, *supra* note 37, at 780.

50. *See id.* at 759 n.60, 774.

51. As Citron noted, however, "state AGs have proposed and endorsed . . . privacy and data security laws" and "routinely testify" on Capitol Hill to influence federal policy. *Id.* at 758–59; *see also* Colin Provost, *State Attorneys General, Entrepreneurship, and Consumer Protection in the New*

values and play a critical role in their construction and practical implementation.

Kenneth Bamberger and Deirdre Mulligan studied how chief privacy officers (CPOs) also fill gaps left open by privacy law.[52] Through a series of interviews with privacy professionals recognized as leaders in their fields,[53] Bamberger and Mulligan concluded that CPOs saw their companies' responsibilities as more than just compliance; rather, legal rules provided a floor.[54] Several American CPOs talked about their jobs in fiduciary terms: they were "steward[s]" of data and "responsibl[e]" to consumers.[55] In short, some CPOs saw their primary objective as creating and maintaining "the company's trusted relationship" with customers, employees, and society.[56] And their profile is increasing. The position of CPO emerged in the 1990s in the financial and health sectors and expanded to other industries over the following ten years.[57] Today, 47,164 people on LinkedIn list "chief privacy officer," "deputy chief privacy officer," or other upper- or middle-management level privacy positions as their current employment.[58]

B. Shifting Privacy Responsibilities

FTC commissioners and state AGs share one essential quality: they are charged with public governance and social welfare functions.[59] But, in reality, many legal policy decisions are made by social groups far from those charged to protect citizens. Online platforms employ armies of content

Federalism, PUBLIUS: J. FEDERALISM, Spring 2003, at 37, 39 (discussing the legislative role of attorneys general).

52. *See* BAMBERGER & MULLIGAN, *supra* note 23; Bamberger & Mulligan, *supra* note 23.

53. BAMBERGER & MULLIGAN, *supra* note 23, at 11–12, 40–43, 59 (discussing the authors' research methodology, including the focus on corporate executives).

54. *Id.* at 60, 64.

55. *Id.* at 66.

56. *Id.* at 67.

57. Bamberger & Mulligan, *supra* note 23, at 261.

58. Based on a LinkedIn Premium Advanced Search conducted on December 6, 2018 filtered by "job titles" using the search terms "chief privacy officer." This is an imperfect metric for measuring reach of privacy professionals today, but it does give a flavor for how the market has grown since the first CPOs in the 1990s.

59. Every attorney general is a lawyer. Every FTC commissioner since 1989, the earliest date available on the FTC's webpage, has been a lawyer. *See Former Commissioners*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/biographies/former-commissioners [https://perma.cc/JLP2-JGBP]. And although CPOs do not always have to have J.D. degrees, the IAPP recently found that six in ten privacy professionals at large companies have law degrees. IAPP, BENCHMARKING PRIVACY MANAGEMENT AND INVESTMENTS OF THE FORTUNE 1000: REPORT ON FINDINGS FROM 2014 RESEARCH 10, https://iapp.org/media/pdf/resource_center/2014_Benchmarking_Report.pdf [perma.cc/ZKK8-NJG4].

moderators to negotiate internal speech rules[60] and make fair use determinations in copyright law.[61] We outsource constitutional responsibilities to police officers, who make practical interpretations of search and seizure law in the moment.[62] Catherine Crump argues that surveillance policy is made by vendors hired by the government.[63] We are increasingly outsourcing judicial decision-making to mediators and arbitrators who hear evidence, consider legal arguments, and issue binding orders.[64] And CPOs, lawyers, and compliance personnel create an internal "company law" of privacy.[65]

Privacy decisions on the ground are similar. Elsewhere, I explored how engineers employed by technology companies instantiate a particular vision of privacy law in the products they create.[66] Because of the networks they sit in and their proximity to the design process,[67] engineers have outsized

60. *See generally* TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET (2018) (profiling the content moderation industry, its practices, and effects); *see also* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018) (describing how online platforms like Facebook employ, train, and deploy large teams of content moderators to make decisions about hate speech and copyright infringement).

61. *See* Lenz v. Universal Music Corp., 801 F.3d 1126 (9th Cir. 2015) (holding that online platforms engaged in content moderation must consider fair use before removing material).

62. *See* GREGORY HOWARD WILLIAMS, LEGAL AND POLITICAL PROBLEMS OF POLICE DISCRETION 5 (1982) (calling attention to police discretion because law enforcement officers are architects of policy in society); *see also* JOHN L. COOPER, YOU CAN HEAR THEM KNOCKING 106 (1981) ("Police interpretation of the law helps to operationalize its legal authority, and to that degree the legality of the criminal justice system, in terms of all the laws that are administered. For this reason, it can be said that the police become the embodiment of the law . . . .").

63. *See* Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595 (2016) (arguing that advanced technology is often obtained by local law enforcement through the procurement process without meaningful input from citizens and political leaders).

64. *See, e.g.*, CHARLES GARDNER GEYH, COURTING PERIL: THE POLITICAL TRANSFORMATION OF THE AMERICAN JUDICIARY 16–43 (2016); Jean R. Sternlight, *The Rise and Spread of Mandatory Arbitration as a Substitute for the Jury Trial*, 38 U.S.F. L. REV. 17, 20 (2003) (binding arbitration takes away the opportunity for a trial); Jean R. Sternlight, *Rethinking the Constitutionality of the Supreme Court's Preference for Binding Arbitration: A Fresh Assessment of Jury Trial, Separation of Powers, and Due Process Concerns*, 72 TUL. L. REV. 1, 5 (1997).

65. *See* BAMBERGER & MULLIGAN, *supra* note 23.

66. *See* Waldman, *supra* note 24 (arguing that theory, law, corporate organization, and the social experience and education of engineers hamper the diffusion of privacy norms throughout a company and into products).

67. This argument reflects actor-network theory (ANT), developed by the science and technology studies scholars Michel Callon and Bruno Latour. *See, e.g.*, Michel Callon, *The Sociology of an Actor-Network: The Case of the Electric Vehicle*, *in* MAPPING THE DYNAMICS OF SCIENCE AND TECHNOLOGY: SOCIOLOGY OF SCIENCE IN THE REAL WORLD 19 (Michel Callon, John Law & Arie Rip eds., 1986). ANT generally posits that artifacts (like machines) do not just emerge out of nowhere; rather, they come into existence as products of social relations, or actor-networks, like those that exist within a technology company. BRUNO LATOUR, REASSEMBLING THE SOCIAL: AN INTRODUCTION TO ACTOR-NETWORK THEORY 9–16 (2005); Albena Yaneva, *Making the Social Hold: Towards an Actor-Network Theory of Design*, 1 DESIGN & CULTURE 273 (2009). *But see* Susan Leigh Star, *Power, Technology and the Phenomenology of Conventions*, *in* TECHNOSCIENCE: THE POLITICS OF INTERVENTIONS 79, 88–99 (Kristin Asdal, Brita Brenna & Ingunn Moser eds., 2007) (criticizing ANT as focusing too much on the efforts of (mostly male) designers and marginalizing the contributions of others).

power to translate privacy law into design. Through first-person interviews, observations of corporate design processes, and analyses of internal privacy standards and protocols, I found that, at least for some engineers in the high technology sector, the kind of consumer privacy they considered during design differed from the more robust conception of privacy coming out of CPOs' offices. Where CPOs may think about privacy in terms of trust, many engineers think about choice architecture.[68] Where privacy professionals create company-wide protocols and trainings to help integrate privacy into design, many engineers make privacy decisions ad hoc and often prioritize efficiency, speed, and other engineering values over privacy.[69] Where corporate privacy teams may work hard to persuade their bosses that privacy is important and even good for business, engineers fall back on their education and social experiences with other technologists at work to shift the focus elsewhere.[70] This means that in some cases, privacy law[71] and the visions of earnest and hardworking privacy professionals are not being fully realized; the engineers whose job it is to translate internal privacy rules into design have different, sometimes contradictory, priorities, backgrounds, and views.

Frustrating the integration of robust privacy protections into technology design is just one effect of shifting the locus of privacy law decision-making from policymakers to corporate actors. Such a shift can undermine substantive and procedural safeguards, replace transparency with opacity, and short circuit deliberative decision-making with quick compliance-based answers.[72] There is another risk, one which this Article explores: the managerialization of privacy law compliance by compliance professionals

68. *See* Waldman, *supra* note 24, at 681–85.

69. *Id.* at 685–89, 711–16.

70. *Id.* at 716–25.

71. This includes the principle of privacy by design. Privacy by design is the idea that the privacy of consumers should be considered from the beginning and throughout the design process of new technologies rather than tacked on at the end. The idea has been around since at least the European Union's Privacy Directive, which the GDPR replaced. *See* Directive 95/46/EC, 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) 31, 46; *see also* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE SEVEN FOUNDATIONAL PRINCIPLES (2009), http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf [perma.cc/7UM3-PGCE]. It has more recently received more systematic scholarly attention. *See* HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY (Batya Friedman ed., 1997) (challenging the idea that efficiency and functionality are the central foci of design and showing how values are integrated into new products); WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018); MARY FLANAGAN & HELEN NISSENBAUM, VALUES AT PLAY IN DIGITAL GAMES (2014); Katie Shilton, *Technology Development with an Agenda: Interventions to Emphasize Values in Design*, 47 PROC. AM. SOC'Y FOR INFO. SCI. & TECH. 1 (2010).

72. Danielle Citron identified similar implications of the increasing use of automated tools in public agency decision-making. *See* Citron, *supra* note 29, at 1254–55.

and engineers can threaten to replace real pro-consumer progress with mere symbols of compliance, undermining the promise of pro-privacy laws.

II. UNDERMINING PRIVACY LAW

FTC commissioners, AG offices, and corporate CPOs impact the framing of privacy law. But the center of gravity is still unsettled. Privacy law is being defined, negotiated, and practiced by an army of compliance professionals, auditors, and engineers. Many of them put form over substance to frame privacy law in narrow, compliance-based, and managerially focused ways. They are, in other words, putting privacy on a path to what Lauren Edelman called legal endogeneity and symbolic compliance.[73]

This Part describes legal endogeneity and traces the endogeneity of privacy law, teasing out four related implications. First, although many privacy professionals and their lawyers earnestly want to help their companies comply with the letter and spirit of privacy law, their framing of corporate privacy obligations as minimizing risk to the company and their reliance on paper trails and checklists can undermine that commitment.[74] Second, many compliance professionals create symbolic structures of compliance that often—though certainly not always—ossify into compliance in name only.[75] Third, this emerging legal endogeneity reflects neoliberal managerialization and exemplifies the dangers such an approach poses to the rule of law.[76] Fourth, and finally, although legal endogeneity is taking hold in privacy law, with statutes and regulatory orders already incorporating the mere presence of symbolic structures as evidence of compliance with privacy law, this process is incomplete.[77] We can change course.

A. Legal Endogeneity

In her book, *Working Law*, Edelman showed how form over substance in corporate compliance with civil rights law was having a deleterious effect on real progress toward workplace equality. Edelman wanted to understand why, fifty years after the passage of the Civil Rights Act and the establishment of the Equal Employment Opportunity Commission (EEOC), "substantial workplace inequality on the basis of race, sex, and other

73. *See* EDELMAN, *supra* note 18, at 12, 14.
74. *See infra* Part II.B.2.
75. *See infra* Part II.B.2–II.B.5.
76. *See infra* Part II.C.
77. *See infra* Part II.B.6.

protected categories persist[ed]."[78] Although there could be many reasons for failure, her research suggested that rather than enforcing the substance of civil rights laws, courts and the EEOC were deferring to the in-house structures—trainings, anti-discrimination policies, complaint procedures, and diversity officers, just to name a few—companies had developed in the wake of the Civil Rights Act as evidence that they were actually complying with the law, even when those companies still failed to hire or promote minorities.[79]

Sometimes, these structures have important expressive effects:[80] a policy of nondiscrimination is a first step toward embedding nondiscrimination in the ethos of a company.[81] But they can also be a glossy veneer for noncompliance. For example, a company can have a nondiscrimination policy, but never enforce it; it can hire a diversity officer, but give her office no power; it can develop extensive internal hearing procedures to deal with alleged bias, but use review boards to deny all claims.[82] These symbols were nevertheless accepted by the courts as evidence that companies were not violating civil rights laws; when an alleged victim of discrimination sues her employer, both the lawyers and judges turn to these systems and sometimes confuse the existence of compliance structures with actual compliance.[83]

Edelman also found that legal deference to mere symbols of compliance with civil rights laws was not accidental. Rather, it was part of the endogenous development of law, a process in which compliance professionals played a starring, yet frustrating, role. Sociologists of law argue that law is a product of social relations: lobbying, social movements, bureaucracies, arguments in adversarial proceedings, and the organized

78. EDELMAN, *supra* note 18, at 6–10 (providing statistical evidence for ongoing racial and gender inequality in the workplace).

79. *Id.* at 11, 153–96.

80. *See, e.g.*, Danielle Keats Citron, *Law's Expressive Value in Combatting Cyber Gender Harassment*, 108 MICH. L. REV. 373, 404–14 (2009) (discussing how the law is necessary for persuading individuals, platforms, and the law to take seriously that cyber harassment is gender discrimination); Deborah Hellman, *The Expressive Dimension of Equal Protection*, 85 MINN. L. REV. 1, 3 n.10 (2000) (law is coercive and expressive of norms); Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2022, 2031 (1996) (law tells people what is socially harmful and signals appropriate behavior).

81. Adopting Bruno Latour's distinction between the "ostensive" and the "performative" aspects of behavior, Martha Feldman and Brian Pentland argue that executives are responsible for the "ostensive" aspect of routines: setting the tone for action, laying out a mission, and creating policies that form best practice guides. Martha S. Feldman & Brian T. Pentland, *Reconceptualizing Organizational Routines as a Source of Flexibility and Change*, 48 ADMIN. SCI. Q. 94, 100–102 (2003). Then, routines are "performed" by workers on the ground: real people doing real work translating the mission into action, products, and widgets. *Id.*; *see also* Bruno Latour, *The Powers of Association*, 32 SOC. REV. 264, 266–68, 271–73 (1984).

82. *See* EDELMAN, *supra* note 18, at 14.

83. *See id.* at 168–73.

legal profession, to name just a few.[84] Indeed, it is even the product of the environment it seeks to regulate; judges and legislators often come from industry or have experience representing industry players.[85] This, combined with a professional tendency among compliance officers to fully document their work, lends itself to reliance on shorthand heuristics to prove compliance with the law.[86] The result can be a perverse practice of law: instead of looking for evidence of substantive progress or adherence to legal principles, courts end up deferring to the veneer of compliance that companies create.

In particular, Edelman noticed six stages of legal endogeneity that ultimately undermined workplace antidiscrimination law, illustrated in Figure 1.[87]

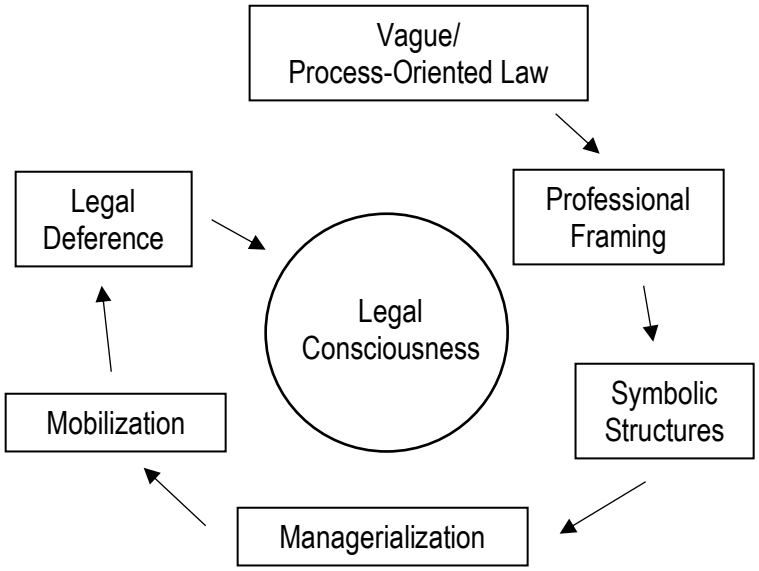

Figure 1

84. *Id.* at 21.

85. *See* David Freeman Engstrom, *Agencies as Litigation Gatekeepers*, 123 YALE L.J. 616, 674–80 (2013) (noting how regulatory capture impairs agencies' ability to serve as litigation gatekeepers); *see also* Lee Fang, *The Reverse Revolving Door: How Corporate Insiders Are Rewarded Upon Leaving Firms for Congress*, NATION (May 4, 2013), https://www.thenation.com/article/reverse-revolving-door-how-corporate-insiders-are-rewarded-upon-leaving-firms-congres/ [https://perma.cc/24D9-FULM] (providing examples of industry players moving into policymaking roles).

86. *See* EDELMAN, *supra* note 18, at 170–71.

87. *Id.* at 28.

Edelman argues that the process starts when a legislature passes a law with ambiguous or vague requirements.[88] Title VII and the other statutes that constitute the ecosystem of employment discrimination law do not specify the meaning of discrimination or "equal employment opportunity."[89] Nor do they specify how courts should determine if an employer is engaging in discrimination. These ambiguities may be the result of the legislative drafting process,[90] but regardless of their origin, they leave the door open to wildly different interpretations from those responsible for compliance on the ground.

But vagueness is not the only problem. Title VII's prohibition on sex discrimination in the workplace sets a goal of nondiscrimination, but does not state how to get there. Other laws require specific actions. For example, a rule could mandate safe driving or reasonableness, or it could set a fifty-five MPH speed limit or define specific responsibilities to others. Edelman's focus on Title VII's vagueness—the statute's failure to define discrimination or equality—implies that vague standards are susceptible to legal endogeneity.[91] But she also notes that Title VII cases like *Meritor Savings Bank v. Vinson*,[92] which suggested that a functional anti-harassment policy and grievance procedure could shield a corporate defendant from sexual harassment liability,[93] and *Faragher v. City of Boca Raton*,[94] which established *Meritor*'s suggestion as an official affirmative defense,[95] gave employers a process-oriented escape hatch from substantive adherence to a law that prohibits sexual harassment.[96] This suggests vagueness is not the

88. This is an endogenous process in itself, which suggests that the process of legal endogeneity and symbolic compliance may be more of a loop than a continuum. *See id.* at 28 (conceptualizing the stages of legal endogeneity in a spiral).

89. 42 U.S.C. § 2000e (2012) (as amended).

90. *See, e.g.*, PAUL BURSTEIN, DISCRIMINATION, JOBS, AND POLITICS: THE STRUGGLE FOR EQUAL EMPLOYMENT OPPORTUNITY IN THE UNITED STATES SINCE THE NEW DEAL (1985); *see also* Victoria F. Nourse & Jane S. Schacter, *The Politics of Legislative Drafting: A Congressional Case Study*, 77 N.Y.U. L. REV. 575, 594–96 (2002) (documenting "deliberate ambiguity" in statutes); Joseph A. Grundfest & A.C. Pritchard, *Statutes with Multiple Personality Disorders: The Value of Ambiguity in Statutory Design and Interpretation*, 54 STAN. L. REV. 627, 640–41 (2002) (arguing that ambiguity in statutes serves legislative purposes like compromise even though the law has developed a variety of interpretive techniques to derive meaning out of ambiguity).

91. *See* EDELMAN, *supra* note 18, at 42–55 (focusing on Title VII's vagueness).

92. 477 U.S. 57 (1986).

93. *Id.* at 72–73 (rejecting the view that the mere presence of a grievance procedure is enough to escape liability, but recognizing the potential for such procedures to insulate companies from liability if the "procedures were better calculated to encourage victims of harassment to come forward").

94. 524 U.S. 775 (1998).

95. *Id.* at 777–78 ("[A] defending employer may raise an affirmative defense to liability or damages, subject to proof by a preponderance of the evidence. . . . The defense comprises two necessary elements: (a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise." (citation omitted)).

96. *See Meritor*, 477 U.S. at 73.

only culprit. *Meritor* and *Faragher* legitimized protocols, policies, and paper trails, even if they hid underlying resistance to Title VII's goal of gender equality. Therefore, Edelman focused not just on vague standards, but on what happens when they combine with process-oriented performance rules.

Legislative ambiguity and process-oriented rules give corporate professionals—lawyers, consultants, and compliance experts, for example—the chance to define what the law means and protect their employers. This, after all, is their job: they act as the filter between the law and the company. In the civil rights context, human resource professionals and in-house counsel play central roles in this process because they design, monitor, and administer personnel policy.[97] And they used the leeway they were given by ambiguous law to conclude that their goal was to minimize the risk of litigation for their employer, not actually eliminate bias, discrimination, and inequality.[98]

These professionals then used the process-oriented parts of the law to develop compliance-oriented solutions in response to legal requirements as they saw them. Ambiguity in the law allows these professionals to get creative, to do their best to comply with their framing of the law without substantially interfering with their chief goal—the continued productivity and profiting of the company.[99] To comply with Title VII in the wake of *Meritor* and *Faragher*, for example, companies drafted policies, created new offices and positions, developed dispute resolution mechanisms and reporting structures, hired consultants to craft new approaches, and kept detailed paper trails, to name just a few steps.[100] And these systems spread rapidly through industry as professionals shared their innovations with their colleagues.[101]

With these systems in place, the law gets managerialized. Managerialization refers to the way in which corporate compliance structures become the sites at which the law is actually applied and its meaning negotiated on a regular basis.[102] Julie Cohen has appropriately described managerialization of law as a natural outgrowth of a neoliberal project that seeks to constrain government regulation aimed at social welfare by emphasizing efficiency and innovation in the service of

97. *See* EDELMAN, *supra* note 18, at 30–31.
98. *Id.* at 31.
99. *Id.* at 31–33.
100. *Id.* at 32.
101. *See* Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOC. REV. 147, 147–49, 153 (1983).
102. *See* COHEN, *supra* note 17, at 143.

industrial and capital production.[103] The process helps companies avoid the costs of litigation and outsources what they see as cumbersome and analog procedures to in-house representatives and even technologies with corporate interests in mind. For example, when an employee has a discrimination claim, she does not immediately go to a judge or even a lawyer. She tells her diversity officer, a corporate employee, who may ask for proof, at which point the allegation may be transferred to an in-house review team. In-house lawyers will get involved and companies will use processes that look very much like adversarial proceedings or dispute resolution, yet with few of a court's protections and rights for aggrieved plaintiffs. Instead, at each point, the professionals determining what the law means and how to apply it in any given circumstance are the in-house lawyers and compliance professionals who developed the structures in the first place.[104]

Corporations then mobilize these structures to push back when employees try to vindicate their rights. In the Title VII context, research has shown that companies erect procedural barriers for discrimination victims. Management lawyers also discourage them from going through internal processes even as those same lawyers leverage those structures to quash employee attempts to use the courts.[105] Edelman found that this had three negative effects on the law's capacity to create real change: it discouraged individuals from taking action in response to rights violations,[106] allowed compliance structures to enter into the legal consciousness as evidence of real progress,[107] and transformed the few workplace discrimination proceedings into debates over structures rather than civil rights.[108]

The final stage of legal endogeneity is deference to symbolic structures, or when corporate compliance systems become embedded in institutional interpretations of law. This happens in three progressive steps. In workplace discrimination cases, judges will start by mentioning that corporate

103. *See* Corinne Blalock, *Neoliberalism and the Crisis of Legal Theory*, 77 LAW & CONTEMP. PROBS. 71, 72–73, 83–90 (2014) (reconceptualizing neoliberalism and its relation to legal theory); *see also* COHEN, *supra* note 17, at 143–47.

104. *See* EDELMAN, *supra* note 18, at 33–39.

105. *Id.* at 158–67.

106. *Id.* at 37; *see also* KRISTIN BUMILLER, THE CIVIL RIGHTS SOCIETY: THE SOCIAL CONSTRUCTION OF VICTIMS (1992) (arguing, among other things, that companies actively discourage employees from turning to the courts to vindicate their rights).

107. *See* EDELMAN, *supra* note 18, at 37–38. By "legal consciousness," Edelman was referring to "the set of shared beliefs and ideas that both draw on and constitute the meaning of law." *Id.* at 154. Susan Silbey, one of the leading scholars who helped develop the concept, has called it "conceptually tortured" and recommended abandoning it entirely. Susan S. Silbey, *After Legal Consciousness*, 1 ANN. REV. L. & SOC. SCI. 323, 324 (2005). That said, the idea remains relevant as a path for understanding the connection between, on the one hand, how people tend to experience and understand the law, and how people behave under the law, on the other. *See, e.g.*, PATRICIA EWICK & SUSAN S. SILBEY, THE COMMON PLACE OF LAW: STORIES FROM EVERYDAY LIFE (1998); *see also* LAURA BETH NIELSEN, LICENSE TO HARASS: LAW, HIERARCHY, AND OFFENSIVE PUBLIC SPEECH (2004).

108. *See* EDELMAN, *supra* note 18, at 38.

defendants have systems in place, including diversity officers and internal dispute resolution processes. Over time, these mentions become evidence in the factual question of whether discrimination actually occurred. Finally, some compliance structures become so closely associated with the legal consciousness, that judges simply take their mere presence as sufficient evidence that a company did not engage in discrimination.[109] There are many reasons why this has happened in Title VII cases: judicial preference for heuristics in decision-making, specific decisions in which federal courts noted that compliance structures would have helped a defendant's case,[110] the increasingly common tendency for lawyers on both sides of discrimination cases to refer to these structures in their briefs,[111] and judicial politics,[112] among other factors.

All this has the effect of conflating a tool of compliance with actual adherence to the substantive requirements of law. And the more that happens, the more these structures of compliance enter our collective consciousness about what the law requires. But symbols of compliance and actual compliance are two different things. When we conflate the two, the result is the frustration of Title VII's goal of a more equal workplace and a collective impression that law, and the system it supports, is ineffective.

B. Legal Endogeneity in Privacy Law

A similar narrative is playing out in privacy law today. Ambiguous privacy rules, from the GDPR to FTC consent decrees, with process-oriented regulatory levers open the door for companies to frame the law in ways that serve corporate, rather than consumer, interests. The compliance ecosystem, from lawyers to privacy professionals to engineers, dominates the social practice of privacy law because these compliance professionals, not legislators or regulators, embed their vision into corporate practice and technology design. And these groups create structures that proliferate throughout the privacy compliance market, thus impacting the legal consciousness; judges, regulators, lawyers, and even consumers are starting to assume that the mere presence of compliance structures is evidence of substantive adherence with the law. But this narrative may not be as

109. *See id.* at 173.

110. *See, e.g.*, Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 765 (1998) (creating an explicit affirmative defense that would allow employers to escape liability if they tried to respond to harassment allegations and had a grievance procedure that the employee declined to pursue); Meritor Sav. Bank v. Vinson, 477 U.S. 57, 72–73 (1986) (holding that although the mere presence of a grievance procedure and nondiscrimination policy did not insulate it from liability, the defendant's argument and position could have benefited from a more specific policy and a more streamlined procedure).

111. *See* EDELMAN, *supra* note 18, at 170–72.

112. *Id.* at 190.

indelible as Edelman fears it is for Title VII and workplace equality.[113] This Part establishes the narrative of legal endogeneity in privacy law and maps the ways in which different groups in the social practice of privacy law are contributing to the erosion of substantive privacy protection.

1. Ambiguity and Process in Privacy Law

Privacy law's flexible definitions[114] and standards,[115] sometimes challenging even in the hands of lawyers, are particularly vulnerable to being weakened and undermined by symbolic structures. Whenever a new

113. *Id.* at 223–25 (explaining why, despite providing recommendations for reversing the endogeneity of civil rights law, material success will be difficult and unlikely).

114. There is a rich tradition of scholars exploring the meaning of privacy. Almost all of them recognize its malleability. *See, e.g.*, ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971) (finding privacy "difficult to define because it is exasperatingly vague and evanescent"); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 234 (1977) (noting that privacy has a "protean capacity to be all things to all lawyers"); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) (noting that "[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings" that it is difficult to define it at all). That has not stopped scholars from trying. Privacy has been defined as a right to be left alone, the capacity to control what others know about us, the ability to protect intimate information, the liberty-affirming need to develop new ideas free of social pressure, controlling the appropriate flow of information, protecting our bodily and sexual integrity, and the negotiation of disclosure in relationships of trust, just to name a few. *See* JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010); NEIL M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015); JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2000); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 90, 94, 102–04 (2004); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019); Jean L. Cohen, *The Necessity of Privacy*, 68 SOC. RES. 318, 319 (2001); Robert S. Gerstein, *Intimacy and Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 265 (Ferdinand David Schoeman ed., 1984); Charles Fried, *Privacy*, 77 YALE L.J. 475, 484 (1968); Steve Matthews, *Anonymity and the Social Self*, 47 AM. PHIL. Q. 351, 351 (2010); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Howard B. White, *The Right to Privacy*, 18 SOC. RES. 171, 180–81 (1951); Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1203 (2000); *see also* ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988); JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012); ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018).

115. Discussions about the relative merits of rules versus flexible standards are beyond the scope of this Article. Duncan Kennedy originally described rules and standards as setting up a dialectical form of argument. *See* Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685, 1689–90 (1976). Ronald Dworkin emphasized the role standards play in realizing substantive legal principles. *See* Ronald M. Dworkin, *The Model of Rules*, 35 U. CHI. L. REV. 14, 22–29 (1967) (distinguishing between principles and rules in order to explain the important role of standards that are not rules); *see also, e.g.*, MARK KELMAN, A GUIDE TO CRITICAL LEGAL STUDIES 15–63 (1987); RICHARD A. POSNER, THE PROBLEMS OF JURISPRUDENCE 42–53 (1990); FREDERICK SCHAUER, PLAYING BY THE RULES: A PHILOSOPHICAL EXAMINATION OF RULE-BASED DECISION-MAKING IN LAW AND IN LIFE (1991); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992); Pierre Schlag, *Rules and Standards*, 33 UCLA L. REV. 379, 383–420 (1985) (examining the form and rhetoric of the rules versus standards debate).

law comes into effect, decision makers on the ground are empowered to adapt, consider changes in context, and assess what is best under the circumstances,[116] especially before a court of law has a chance to have its say. But vague laws can be particularly problematic. The "staggeringly complex" and "ambiguous"[117] GDPR lays out several of these broad standards that need to be given "specific substance over time."[118] Until that happens, regulated companies have room to determine what the law means.

Consider just a few examples: Article 25 of the GDPR calls for privacy "by design and by default."[119] But beyond a general understanding that it refers to making privacy part of the design process for new technologies, what privacy by design means in practice is far from clear.[120] Even guidance documents from the Article 29 Working Party, an advisory group of data protection authorities from across Europe,[121] add little clarity, noting only that companies that "place privacy and data protection at the forefront of product development will be well placed to ensure that their goods and services respect the principles of privacy by design."[122] And scholars have suggested a variety of definitions, ranging from vague privacy principles[123]

116. *See* Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1744–45 (1995).

117. Alison Cool, *Europe's Data Protection Law Is a Big, Confusing Mess*, N.Y. TIMES (May 15, 2018), https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html [https://perma.cc/ST82-9STL].

118. *See* Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 195 (2019).

119. *See* GDPR, *supra* note 9, art. 25, at 48.

120. *See* Ari Ezra Waldman, *Privacy's Law of Design*, 9 U.C. IRVINE L. REV. 1239 (2019) (noting that Article 25 has failed to articulate foundational elements of how to achieve privacy by design in practice). The word "design" can mean many different things, from intentions (something is done "by design") to aesthetics (a room can be designed to be visually appealing). But for the purposes of this Article, I follow the broad definition outlined by Woodrow Hartzog, who defines design as the "processes that create consumer technologies and the results of their creative process instantiated in hardware and software." HARTZOG, *supra* note 71, at 11.

121. Since 1997, the Working Party, now, with some minor changes, called the European Data Protection Board, has issued 240 statements, reports, opinions, and recommendations to help companies comply with European data protection rules. *See Opinions and Recommendations*, EUR. COMMISSION, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [https://perma.cc/K6V9-AR4V].

122. ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 8/2014 ON THE RECENT DEVELOPMENTS ON THE INTERNET OF THINGS 3 (2014), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [https://perma.cc/5T7T-KRNR]. Its advice to companies working in the Internet of Things marketplace was to "apply the principles of Privacy by Design and Privacy by Default." *Id.* at 21.

123. Ann Cavoukian, the former Information & Privacy Commissioner of Ontario, Canada, has argued that privacy by design is the "philosophy . , , of embedding privacy into the design specifications of technology itself." ANN CAVOUKIAN, PRIVACY BY DESIGN: FROM RHETORIC TO REALITY 1 (2009), http://www.ipc.on.ca/images/Resources/privacybydesign.pdf [perma.cc/B8JN-YTF8]; *see also* ANN CAVOUKIAN, *supra* note 71.

and privacy-enhancing technologies[124] to sets of values[125] or "boundaries and goals" for design[126] to norms based on products liability for design defects.[127] This ambiguity will persist until we have clear rules.

The GDPR's consent requirements are also unclear. If companies want to collect ordinary, non-sensitive data, user consent must be "unambiguous."[128] If the data is sensitive, including physical and mental health information, race, ethnicity, or sexual orientation, for example, consent must be "explicit."[129] The two concepts are not the same,[130] but neither the GDPR itself nor any interpretive document clarify what steps make consent explicit rather than just unambiguous. For example, although the European Data Protection Board has stated that "it should be made clear that the use of default options which the data subject is required to modify in order to reject the processing (consent based on silence) does not in itself constitute unambiguous consent," it never makes clear what kind of positive action is required.[131]

Alongside the GDPR, privacy professionals in the United States must incorporate FTC consent decrees into the legal context in which their companies operate.[132] But despite a growing agenda as the de facto federal

124. *See, e.g.*, Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1341–42 (2013) (arguing that privacy by design requires translating privacy principles into code, both in the back-end infrastructure of data collection and front-end user interfaces).

125. *See, e.g.*, FLANAGAN & NISSENBAUM, *supra* note 71 (discussing the way in which game designers integrate values into their products).

126. HARTZOG, *supra* note 71, at 7.

127. *See* Waldman, *supra* note 120 (applying several analogies from the law of products liability for design defects to specify what privacy by design should mean in practice).

128. GDPR, *supra* note 9, art. 6, at 36 (requiring consent); *id.* art. 4, at 34 (consent must be unambiguous).

129. *Id.* art. 9, ¶ 2(a), at 38.

130. *See* Note from Presidency to Permanent Representatives Comm., Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation): Analysis of the Final Compromise Text with a View to Agreement 3 (Dec. 15, 2015), http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf [https://perma.cc/GH75-UM2L] ("On the final outstanding issues that were discussed in trilogue, the following balance was achieved. The way in which consent is to be given by data subjects remains 'unambiguous' for all processing of personal data, with the clarification that this requires a 'clear affirmative action', and that consent has to be 'explicit' for sensitive data.").

131. ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 15/2011 ON THE DEFINITION OF CONSENT 36 (July 13, 2011), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/ 2011/wp187_en.pdf [perma.cc/GJ4U-DYE7]. The Article 29 Working Party is now called the European Data Protection Board.

132. As part of their research on the FTC's privacy jurisprudence, Solove and Hartzog interviewed leading privacy attorneys who noted that FTC consent decrees are scrutinized by practitioners for insight into the current state of the law. *See, e.g.*, Solove & Hartzog, *supra* note 14, at 607, 621 (quoting Chris Wolf, then-director of Hogan Lovells LLP's privacy and information management practice group). Indeed, the FTC intends for its consent orders to have a norm-setting impact. *See id.* at 622 (quoting Toby Levin, a senior attorney with the FTC from 1984 to 2005).

privacy regulator,[133] the FTC often includes vague requirements in its consent decrees, giving professionals on the ground wide latitude to determine what the law means in practice.

For example, the FTC ostensibly requires companies to provide "adequate" notice to consumers. In *FTC v. Frostwire, LLC*,[134] for example, the agency alleged that the company failed to "*adequately* inform[] consumers that [an Android file sharing] application" required several steps to protect the privacy of some files.[135] In *FTC v. Echometrix*,[136] the FTC found that broad statements in its privacy policy were too vague and "failed to disclose *adequately*" the company's data collection regime.[137] And in *In re Sears Holdings Management Corp.*,[138] the FTC concluded that Sears's long, legalese licensing agreement "failed to disclose *adequately* that the software application, when installed," would monitor a long list of consumer behavior.[139] The FTC has never clarified the meaning of adequacy, instead choosing a step-by-step common law approach. Indeed, arguably the only piece of the FTC's privacy jurisprudence that is not left open to interpretation on the ground is the FTC's baseline and clearest rule: do not lie.[140]

In addition to ambiguity in the law, international privacy law offers data collectors a series of process-oriented escape hatches to avoid liability. Each route requires a paper trail, thus incenting processes over substance. Under the traditional notice-and-consent regime, data collectors can escape liability as long as they post their data use practices in a privacy policy.[141] Under the GDPR, data processing records are required,[142] and data protection impact assessments can protect companies from liability even

133. 15 U.S.C. § 45(a)(1) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

134. Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Frostwire, LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 7, 2011), http:// www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf [perma.cc/G964-4NU2].

135. *Id.* at 16 (emphasis added).

136. Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Echometrix, Inc., No. CV10-5516 (E.D.N.Y. Nov. 30, 2010), http://www.ftc.gov/sites/default/files/documents/cases/2010/11/101130echometrixcmpt.pdf [perma.cc/4G79-C962].

137. *Id.* at 4, 5 (emphasis added).

138. Complaint, *In re* Sears Holdings Mgmt. Corp., FTC File No. 082 3099, No. C-4264 (F.T.C. Aug. 31, 2009), http:// www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf [https://perma.cc/3C49-LRLC].

139. *Id.* at 5 (emphasis added).

140. That is not to say that the FTC only engages in broken promises litigation. However, most scholars agree that broken promises not only constitute the lion's share of FTC actions, but it is also the agency's clearest requirement of industry. *See* Solove & Hartzog, *supra* note 14, at 629–38 (reviewing the FTC's deception jurisprudence focusing on incidents of lying and misleading statements in privacy policies).

141. Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 41 (2015).

142. *See* GDPR, *supra* note 9, at 50–51.

when engaging in data processing that carries a "high risk to the rights" of data subjects.[143]

Ambiguous laws and process are nothing new. The limitations of language and the legislative drafting process often result in statutes and rules that leave their meaning and details to those interpreting them.[144] And the debate over standards and rules is as old as the common law.[145] Margot Kaminski argues that seemingly vague terms in the GDPR become clear when we combine the GDPR with interpretive tools, including reports from the European Data Protection Board. That is, she argues, how it is supposed to work.[146] Dan Solove and Woodrow Hartzog argue that lawyers and privacy professionals may be able to piece together what does and does not constitute "adequate" notice from the sum total of FTC consent decrees.[147]

But interpretations of the GDPR and FTC actions neither emerge in a vacuum nor necessarily take on the color the Board or the FTC intend. Rather, interpretations are made by real people affected by biases, social influences, and institutional pressures.[148] And by the FTC's own count, the agency averages only ten privacy-related cases per year, limiting the sources lawyers have from which to glean lessons and find clarity.[149] Even if clarity is to come in the future, the FTC and data protection authorities will only have the opportunity to issue official judgments after protracted investigations and litigation. Until then, corporate actors on the ground can use their first-mover advantage to entrench their interpretations of the law before any court has its say,[150] interpreting vague terms in light of corporate,

143. *See id.* art. 35, at 53.

144. *See, e.g.*, Kenneth A. Bamberger, *Normative Canons in the Review of Administrative Policymaking*, 118 YALE L.J. 64, 75–76 (2008); Grundfest & Pritchard, *supra* note 90, at 640; Nourse & Schacter, *supra* note 90, at 594–96 (documenting "deliberate ambiguity" in statutes); *see also* REED DICKERSON, THE INTERPRETATION AND APPLICATION OF STATUTES 43–53 (1975) (discussing how the inherent limitations of language create ambiguity in statutes).

145. *Compare, e.g.*, Balt. & Ohio R.R. Co. v. Goodman, 275 U.S. 66 (1927) (establishing a rule of contributory negligence in rail crossing cases if the driver does not get out of the car to check for an oncoming train), *with* Pokora v. Wabash Ry. Co., 292 U.S. 98 (1934) (holding that the issue of the driver's negligence is a question for the jury, based on a standard of reasonableness); *see also, e.g.*, KELMAN, *supra* note 115, at 15–63; SCHAUER, *supra* note 115, at 149–55; Duncan Kennedy, *supra* note 115, at 1689–90.

146. *See* Kaminski, *supra* note 118, at 195.

147. *See* Solove & Hartzog, *supra* note 14, at 658–61; *see also id.* at 650–56 (arguing that, when taken together, the FTC's "adequate security" jurisprudence may have started with a vague standard, but has come to include a series of specific rules).

148. This is one of the core insights of the fields of the sociology of law—namely, that law is a social system made up of people and behaviors and a social institution that has an impact on social life. *See, e.g.*, JOHN R. SUTTON, LAW/SOCIETY: ORIGINS, INTERACTIONS, AND CHANGE 8–20 (2001).

149. *See* Solove & Hartzog, *supra* note 14, at 600.

150. The first-mover advantage refers to the benefits that accrue to a company that is first in the market. *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) (noting that a first mover enjoys a kind of monopoly that ultimately ebbs with time); William T. Robinson & Sungwook Min, *Is the First to Market the First to Fail? Empirical Evidence for Industrial Goods Businesses*, 39 J. MARKETING RES.

rather than consumer, values. They leverage their size and resources to shape the law in ways that, both in the short and long term, benefit them and their interests.[151] This is where the real work of the social practice of privacy law happens; somewhere between lawmaking and adjudication, the regulated have the chance to frame the debate.[152] And as the responsibilities for legal interpretations increasingly shift to compliance professionals with interests not necessarily aligned with their customers, the GDPR's and the FTC's intent becomes more distant.

2. *Framing Corporate Obligations Narrowly in Terms of Risk Avoidance*

Recognizing the ambiguity and process in privacy law, privacy professionals on the ground have the opportunity (and responsibility) to translate the law's requirements for their employers in a way that makes compliance possible.[153] As Edelman describes, these professionals "make certain laws or norms visible or invisible to employers and frame those laws' relevance to organizational life."[154] In so doing, they shape the "aesthetic of law," determining not just what laws make it through the filter, but what those legal obligations look like.[155] Human resources professionals and lawyers figure prominently in Edelman's work on the implementation (or lack thereof) of civil rights laws; they frame the work compliance with Title VII as minimizing the risk of a lawsuit from an employee, rather than actually eradicating sex discrimination in the workplace.[156] In the privacy space, lawyers,[157] CPOs,[158] consultants,[159] and their staffs should assume the

120, 126 (2002). In this context, I am arguing that companies have the chance to be first movers when it comes to interpreting what the law means in practice because courts and regulatory agencies can only respond later.

151. *See* COHEN, *supra* note 17, at 139 (describing how patterns of institutional and legal change tilt toward advantages for wealthy corporate interests because, as repeat players in the legal system, they can argue for positive outcomes in any given case or prospective rule changes that work in their favor).

152. *Id.* at 186.

153. Bamberger & Mulligan, *supra* note 23, at 271, 291.

154. EDELMAN, *supra* note 18, at 82.

155. *Id.*

156. *See id.* at 78–80.

157. In-house counsel operate as the chief filters or "gatekeepers" between the law and corporate organizations. *See* Robert L. Nelson & Laura Beth Nielsen, *Cops, Counsel, and Entrepreneurs: Constructing the Role of Inside Counsel in Large Corporations*, 34 LAW & SOC'Y REV. 457, 470 (2000). Nelson and Nielsen found that in-house counsel routinely used their legal expertise to advance their employers' financial interests, allowing their companies to make more money, pay fewer taxes, escape liability, and reach new markets. *Id.* at 474–76. Lawyers also needed to maintain their seat at the table by "mak[ing] their advice more palatable to businesspeople." *Id.* at 477.

158. *See* BAMBERGER & MULLIGAN, *supra* note 23.

159. Consultants provide advice and counseling. They can design an internal privacy structure or work with in-house teams to build systems to comply with specific laws. They can also serve as outsourced privacy leads. Protiviti, for example, "designs holistic and comprehensive approaches to

principal legal filter role and should ideally frame corporate legal obligations in terms of the laws' underlying purposes—namely, to create more robust privacy protections, to protect consumers from predatory data collection practices, and to minimize privacy risks to consumers.[160]

But that is not always what happens. Although there are many privacy professionals advocating strongly and effectively for privacy prioritization inside technology companies, some professionals frame privacy law compliance as a means of minimizing the risk to the *company*, not protecting consumers from data use harms.

This risk framing pervades the privacy compliance landscape. When the National Institute of Standards and Technology (NIST) published its *Privacy Risk Management Framework*, it focused on developing standards for an organization-wide "program that involves the *management of organizational risk*—that is, the risk to the organization or to individuals associated with the operation of a system."[161] In the Journal of Data Protection and Privacy, an industry journal offering analysis of international privacy developments,[162] several articles in the Journal's first five volumes focus on minimizing corporate risk. In *The Risk-Based Approach to Privacy: Risk or Protection for Business?*, for example, the authors recognize the GDPR's requirement that privacy protection mechanisms be proportional to the risk data processing poses to users. But the lion's share of the article focuses on how privacy impact assessments (PIAs) can be used to mitigate corporate exposure to GDPR penalties.[163] Two practical

GDPR compliance" and helps companies with "[r]egulation interpretation[;] . . . [c]ompliance solutions—people, process and technology execution for an effective cybersecurity and privacy program[; and] [c]ompliance management—monitoring and maintaining controls going forward." *GDPR Is Here—Now What?*, PROTIVITI, https://www.protiviti.com/US-en/technology-consulting/general-data-protection-regulation [https://perma.cc/7UPE-NPEH]. Galexia helps companies "understand their legal, regulatory and best practice requirements," and "develop[s] compliance tools, manage[s] stakeholder consultation and architect[s] solutions." *Services*, GALEXIA, http://www.galexia.com/public/services/ [https://perma.cc/X4N5-J7EF].

160. The GDPR's first stated goal is "protection of natural persons with regard to the processing of personal data." GDPR, *supra* note 9, art. 1, at 32; *see also* Assemb. B. 375, 2017-18 Reg. Sess., § 2 (Cal. 2018) (finding that "[t]he unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals" and "California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information").

161. *Risk Management*, NAT'L INST. STANDARDS & TECH., https://csrc.nist.gov/Projects/Risk-Management/rmf-overview [https://perma.cc/DZR5-FFYL].

162. *See Journal of Data Protection and Privacy*, HENRY STEWART PUBLICATIONS, https://www.henrystewartpublications.com/jdpp [https://perma.cc/2WZZ-7XG4] ("Essential reading for Presidents, CEOs, CTOs, CFOs, COOs and CIOs in private and public sectors, Government Departments and membership/trade bodies . . . .").

163. *See* Giulio Coraggio & Giulia Zappaterra, *The Risk-Based Approach to Privacy: Risk or Protection for Business?*, 1 J. DATA PROTECTION & PRIVACY 339 (2018).

guidebooks do the same.[164] But although PIAs are supposed to help companies "identif[y] and evaluate[] potential threats to individual privacy, discuss[] alternatives and identif[y] the appropriate risk mitigation measures for each,"[165] a company merely looking to avoid risk to itself could see a PIA as a convenient paper trail documenting a check-the-box approach to privacy.[166]

Law firms run risk minimization Continuing Legal Education programs that focus entirely on risks to the company.[167] Privacy trade groups also frame compliance as a means of minimizing corporate risk. For example, the IAPP and TrustArc published a study focusing on prioritizing different parts of the GDPR based on the risks of noncompliance to the company.[168] And the organization has also framed data minimization as a way of reducing corporate risk,[169] and hosted several webinars in which experts have said that the "heart" of data protection compliance is doing what "you can to manage the risk to the company" posed by new privacy laws.[170] This focus ultimately encourages many companies to house their privacy officers within their risk management departments, and puts a decidedly corporate spin on privacy law itself.[171] In other words, only collecting as much data as is necessary for a particular purpose does reduce the risk of litigation or investigation because data minimization is required by the GDPR. But the purpose of the requirement is to reduce privacy risks *to consumers* associated with the collection and processing of personal data.[172] Skilled

164. *See, e.g.*, IT GOVERNANCE PRIVACY TEAM, EU GENERAL DATA PROTECTION REGULATION (GDPR): AN IMPLEMENTATION AND COMPLIANCE GUIDE 14–58 (2d ed. 2017) (framing obligations in terms of risk management for the company); ARDI KOLAH, THE GDPR HANDBOOK: A GUIDE TO IMPLEMENTING THE EU GENERAL DATA PROTECTION REGULATION (2018).

165. Kenneth A. Bamberger & Deirdre K. Mulligan, *PIA Requirements and Privacy Decision-Making in US Government Agencies*, *in* PRIVACY IMPACT ASSESSMENT 225, 228 (David Wright & Paul De Hert eds., 2012).

166. Raphaël Gellert highlighted this problem before. *See* Raphaël Gellert, *Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative*, 5 INT'L DATA PRIVACY L. 3 (2015).

167. *See, e.g.*, *Privacy and Data Protection: Managing Your Litigation Risk*, PERKINS COIE, https://email.perkinscoie.com/9/765/october-2018/you-re-invited--lessons-learned-from-the-us--privacy-and-data-protection---managing-your-litigation-risk(2).asp?sid=5bc613d8-81d3-49bc-840d-eed68e1ccf98 [https://perma.cc/3W6S-5KZJ].

168. IAPP & TRUSTARC, GETTING TO GDPR COMPLIANCE: RISK EVALUATION AND STRATEGIES FOR MITIGATION (2018), https://iapp.org/media/pdf/resource_center/GDPR-Risks-and-Strategies-FINAL.pdf [https://perma.cc/52LP-UXYE].

169. *Reducing Risk Through Data Minimization*, IAPP (Sept. 6, 2016), https://iapp.org/store/webconferences/a0l1a000002hDCIAA2/ [https://perma.cc/KW54-FYFW].

170. *See, e.g.*, *The Role of Risk Management in Data Protection*, IAPP (Jan. 23, 2015), https://iapp.org/store/webconferences/a0l1a000000SKCzAAO/ [https://perma.cc/6KMB-RHVS].

171. See Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 LAW & POL'Y 477, 488, 493–94 (2011).

172. *See, e.g.*, GDPR, *supra* note 9, recital 75, at 15 ("The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead

privacy lawyers recognize this.[173] Framed narrowly, however, data minimization means doing the least possible to shield a company from liability.

I spoke with a small group of privacy professionals and corporate privacy lawyers about this at the IAPP's "Privacy. Security. Risk." conference in 2017 and the Privacy+Security Forum in 2018. To their credit, each interviewee recognized that the GDPR and other risk-based approaches to privacy defined "risk" in terms of privacy risks to the individual consumer. But two additional themes came through. A deputy general counsel who had previously worked at an AmLaw Top 100 firm noted that "many of the privacy risk programs [he has] seen are more based on organizational risks, like the risk of a fine or lawsuits or the kind of reputational harm that comes with a data breach or having to testify before Congress."[174] A lawyer at a large international law firm agreed, noting that "for better or for worse, that's what risk programs often turn into: the company is obviously interested in keeping itself out of the papers, and of course out of court."[175] R. Jason Cronk, a certified privacy professional and privacy consultant, noted that companies assess risk based on "how big a footprint the company has and how big a target they are."[176] These and other professionals suggest that risk framing creates incentives to orient compliance programs around corporate risk avoidance rather than substantive adherence to the law much in the same way standardized testing can incent "teaching to the test" rather than holistic learning.[177]

Framing the data privacy landscape as one based on corporate risk is not surprising. Risk framing can actually encourage compliance with the law by persuading executives to treat it as a high priority,[178] especially since some

---

to physical, material or non-material damage . . . ."); *see also* Michael Birnhack, Eran Toch & Irit Hadar, *Privacy Mindset, Technological Mindset*, 55 JURIMETRICS 55, 65 (2014) (nothing that "[t]he current GDPR text adopts a risk assessment consideration, namely, that the data controller should apply technological measures that are proportionate to the risk; it requires the data controller and processor to implement 'appropriate and proportionate' technical and organizational measures throughout the entire lifecycle of the system").

173. *See* CTR. FOR INFO. POLICY LEADERSHIP, HUNTON & WILLIAMS LLP, RISK, HIGH RISK, RISK ASSESSMENTS AND DATA PROTECTION IMPACT ASSESSMENTS UNDER THE GDPR 14 (Dec. 21, 2016), https://iapp.org/media/pdf/resource_center/cipl_gdpr_risk_21_dec_2016.pdf [perma.cc/NQ7V-FFJU] (noting that "the GDPR clearly focusses on one type of risk: adverse risk to the individual").

174. Interview with deputy general counsel in Silicon Valley, in San Diego, Cal. (Oct. 17, 2017) (notes on file with author).

175. Interview with partner at AmLaw Top 100 firm, in San Diego, Cal. (Oct. 17, 2017) (notes on file with author).

176. E-mail from R. Jason Cronk to author (July 25, 2019) (on file with author).

177. *See* Cary Coglianese & Jennifer Nash, *The Law of the Test: Performance-Based Regulation and Diesel Emissions Control*, 34 YALE J. ON REG. 33, 79–89 (2017) (challenging performance-based standards in part because they encourage regulated industries to design "for the test" rather than improve safety holistically).

178. *See* EDELMAN, *supra* note 18, at 98.

executives still see privacy as inconsistent with corporate profit goals. The risk of a fine of 4 percent of global revenue goes a long way to making privacy compliance a central corporate mission.[179] Risk framing also makes sense from an endogenous political perspective. By emphasizing the dangers of noncompliance, privacy professionals stake out important territory at the highest levels of corporate decision-making, giving them seats at the table and the capacity to influence policy.[180] And third-party vendors follow suit because it allows them to increase their market share and emphasize the importance of their services.[181]

But risk framing is problematic if the goal is adherence to the substantive goals of privacy law. First, it is too narrow, focusing on the avoidance of a problem rather than the achievement of an affirmative goal—namely, greater user control, privacy, and safety. Second, it is incomplete. There is more to privacy than managing risk. Privacy also involves managing users' expectations, their desire for obscurity,[182] their need for trust,[183] and their consistent distaste for transfers of data to third parties.[184] Operating along narrow risk-mitigation paths distracts corporate attention from more important, substantive mandates. And, third, a risk-based approach is myopic. By enhancing user trust, privacy can be good for business,[185] especially if companies innovate and market around making privacy an essential aspect of their business model.

179. *See* GDPR, *supra* note 9, art. 58, 83, at 70, 82 (providing the powers to levy fines and the factors to consider when assessing fines).

180. *See* EDELMAN, *supra* note 18, at 97.

181. *Id.* at 98.

182. *See* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013); HARTZOG, *supra* note 71, at 110–11.

183. *See* HARTZOG, *supra* note 71, at 97–107 (discussing various aspects of trust in privacy law); WALDMAN, *supra* note 114, at 1–10, 47–75 (arguing that privacy is based on relationships of trust between individuals and thus can protect the value of trust); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1308–10 (2000) (noting that we entrust our data to web platforms); Kirsten Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online*, FIRST MONDAY, Dec. 2, 2013, http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802 [https://perma.cc/F3P7-FFPW]; Richards & Hartzog, *supra* note 114, at 451–56 (protecting privacy can build trust between online platforms and consumers); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008).

184. *See, e.g.*, Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J.L. & TECH. 111, 131–34 (2017) (noting consistent consumer rejection of corporate practices that involve data collection through data brokers).

185. *See* Kirsten Martin, *Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online*, 45 J. LEGAL STUD. S191 (2016) (showing how better transparency and privacy protections can enhance user trust while the opposite will erode user trust).

3. Symbols of Compliance

Having interpreted privacy law for their corporate employers and framed corporate privacy obligations in terms of risk rather than substantive privacy protections for users, compliance professionals create structures, services, and technologies to comply with their version of the law.[186] Some of these structures are tied to specific provisions of privacy law. For example, because the FTC often requires regulated companies to implement a "comprehensive privacy program"[187] and because the GDPR requires the designation of a data protection officer (DPO),[188] many companies have to hire a DPO. Similarly, because the GDPR gives consumers a right to access their information and a right to erase irrelevant, incorrect, and outdated information,[189] data collectors have to develop systems to find and categorize user data. And laws like the California Online Privacy Protection Act (CalOPPA) require privacy notices that describe data use practices.[190] But where legal requirements are flexible—What is a CPO/DPO supposed to do? How do companies have to present their data use practices to users? How are companies supposed to design products with privacy in mind?—compliance structures often become *merely symbolic*.

Symbolic structures are those that carry with them an instant perception of legitimacy because they resemble pre-existing forms already having the imprimatur of the law. A nondiscrimination policy, with legal-sounding terms of art, or internal dispute resolution systems are examples of symbolic structures that resemble legal processes.[191] As is the process of online content moderation, where rules reflect neoliberal First Amendment principles[192] and questions are adjudicated with quasi-judicial proceedings.[193] Notably, symbolic structures can be helpful. An equal

186. I follow Edelman and define *structure* as any corporate office, program, policy, or practice that exists independently of a particular person. *See* EDELMAN, *supra* note 18, at 101. A privacy office is a structure, as are internal data access rules, mission statements, organizational structures, privacy teams, in-house training systems, compliance protocols, and so forth.

187. *See, e.g.*, Agreement Containing Consent Order at 4, *In re* Google, Inc., FTC File No. 102 3136, No. C-4336 (F.T.C. Mar. 30, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf [https://perma.cc/34LE-35N8] [hereinafter Google Consent Decree] (requiring a "comprehensive privacy program").

188. *See* GDPR, *supra* note 9, arts. 37–39, at 55–56.

189. *Id.* arts. 15, 17, at 43–44.

190. CAL. BUS. & PROF. CODE § 22575 (West 2018).

191. *See* EDELMAN, *supra* note 18, at 101. Other examples in the employment discrimination context include formal job descriptions that include language of EEO compliance, salary classification systems, personnel and diversity offices, formal job ladders, performance evaluations, and maternity leave policies. *See id.* at 117.

192. *See* Klonick, *supra* note 60, at 1618–22, 1658–62 (arguing that content moderation policies have a baseline in free speech norms); *see also* GILLESPIE, *supra* note 60, at 17, 24–25, 45–49, 51, 56.

193. *See* Klonick, *supra* note 60, at 1638–47 (showing how the process of content moderation bears some resemblance to judicial process).

opportunity employment policy can have both expressive and substantive effects when companies take it seriously, and a fair dispute resolution system can give victims of discrimination an opportunity to make their voices heard and seek equal treatment.[194] But when these structures become *merely* symbolic, when they offer just the veneer or the trappings of compliance with no substance, then they can frustrate the goals of the law. This is what is happening in privacy law.

Over the last ten years, many companies have developed increasingly complex privacy structures, hired CPOs and downstream privacy professionals, and created protocols to manage access to personal data, among many other steps.[195] In many companies, these structures are taken seriously and employees at all levels work with privacy offices to meet their responsibilities to their users. But these structures can also ossify into symbols. One of the best examples of this may be corporate privacy policies. Though privacy policies developed first as industry's way to stave off regulation,[196] they are now required by many state and federal mandates.[197] Many of those laws require that privacy policies be sufficiently "conspicuous" to users, and yet privacy policies today are a confusing mess of legalese jargon.[198] No one reads them because they are long and difficult to understand. [199] And they are designed and presented to us in ways that

194. *See* TOM R. TYLER, WHY PEOPLE OBEY THE LAW 96, 116–20, 137–38, 149 (2006) (finding that popular perceptions of the legitimacy of authorities depends, at least in part, on the existence of procedural safeguards and the opportunity to be heard). The effect of fair procedure on legitimacy is more pronounced in contexts where procedure matters more, like a trial. *Id.* at 105.

195. *See* BAMBERGER & MULLIGAN, *supra* note 23, at 83–86.

196. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PA. ST. L. REV. 587, 593 (2007) ("Online privacy policies have appeared . . . as a voluntary measure by websites . . . ." (footnote omitted)); *see also* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046–47 (2000) (noting that an FTC threat for greater regulation resulted in a substantial increase in the number of websites offering privacy policies); Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 726 (2001) ("[S]elf-regulation and technical tools have proven to be more public relations than meaningful information privacy for citizens."); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 774 (1999) [hereinafter Reidenberg, *Restoring*] ("[U.S. policy on] fair information practices has historically been predicated on the philosophy that self-regulation will accomplish the most meaningful protection of privacy without intrusive government interference, and with the greatest flexibility for dynamically developing technologies."); Solove & Hartzog, *supra* note 14, at 593–94.

197. *See* Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 90–95 (2018) (showing how state and federal statutes require privacy policies).

198. *See* Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. LEGAL STUD. S163, S163–64 (2016) ("Privacy policies often contain ambiguous language describing website practices for data processing activities . . . . Ambiguity regarding these practices undermines the purpose and value of a privacy policy for website users."); Reidenberg et al., *supra* note 141, at 40, 87–88 ("[A]mbiguous wording in typical privacy policies undermines the ability of privacy policies to effectively convey notice of data practices to the general public.").

199. George R. Milne, Mary J. Culnan & Henry Greene, *A Longitudinal Assessment of Online Privacy Notice Readability*, 25 J. PUB. POL'Y & MARKETING 238, 243 (2006). Lorrie Cranor estimates that it would take a user an average of 244 hours per year to read the privacy policy of every website she

make them manipulative of our behavior.[200] As such, they are merely symbolic structures: they technically comply with the law in that they are lists of data use practices, but they do not fulfill the law's purpose of actually providing sufficient transparent notice to users to inform privacy decision-making.

Privacy compliance programs can also become merely symbolic when they are reduced to flow charts, check lists, and templates. Interviews with in-house lawyers and privacy professionals at three major U.S. technology companies reveal that checklists are frequent compliance tools because they "help people in their jobs simplify responsibilities and make sure they're following the rules set down for them by the GC [general counsel] office, [the CPO,] or their manager."[201] Other scholars have found similar internal tools at work at other companies.[202] Third-party technology vendors provide checklists and templates, as well. For example, Nymity offers an automated "privacy program . . . made up of policies, procedures, and other accountability mechanisms."[203] Data collectors snap up these tools with alacrity.

These structures are not, by themselves, problematic. But extensive qualitative research at technology companies suggests that many of these policies are policies in name only. As one former engineer put it, "we would need to run our design by privacy, legal, and marketing."[204] But the process was "compliance-style. I remember being told by my manager that 'privacy checked the boxes, so we can go ahead.'"[205] And there was a sense among three interviewees that even though it was a privacy professional's job to audit new designs, the privacy team did not really want to get in the way. "Nobody wants to stop creativity," one former engineer at Google said.[206]

---

visited. Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 274 (2012). This translates to about fifty-four billion hours per year for every U.S. consumer to read all the privacy policies she encountered. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 563 (2008); *see also* Mark A. Graber, Donna M. D'Alessandro & Jill Johnson-West, *Reading Level of Privacy Policies on Internet Health Web Sites*, 51 J. FAM. PRAC. 642, 642 (2002) (noting how difficult privacy policies are to read).

200. *See* Waldman, *supra* note 197, at 107–17.

201. Telephone Interview with senior privacy manager at leading technology company (Aug. 8, 2017) (notes on file with author).

202. *See* BAMBERGER & MULLIGAN, *supra* note 23, at 83–86.

203. NYMITY, 2018 PRIVACY COMPLIANCE SOFTWARE BUYER'S GUIDE 9 (2018), https://info.nymity.com/hubfs/2018%20Privacy%20Compliance%20Software%20Buyers%20Guide/Nymity-Buyers-Guide-GDPR-Edition.pdf [perma.cc/HUU3-HU4X] (suggesting that its templating software will allow clients to create their privacy programs).

204. Telephone Interview with former engineer at Google and Microsoft (Oct. 4, 2016) (notes on file with author).

205. Telephone Interview with former Google employee (Apr. 18, 2016) (notes on file with author).

206. Telephone Interview with former engineer at Google and Microsoft, *supra* note 204.

"I can't say for sure, but I'm sure privacy didn't want to, either. They didn't stop us from doing our work."[207] This narrow, compliance focus reduced internal compliance rules into a merely symbolic structure.

FTC-required assessments have also become merely symbolic structures that can impede the substantive implementation of privacy law. The FTC requires companies operating under consent decrees to submit assessments roughly every two years for the life of the order.[208] Assessments have to be completed by a "qualified, objective, independent third-party" auditor with sufficient experience. And they must describe specific privacy controls, evaluate their adequacy given the size and scope of the company, explain how they meet FTC requirements, and certify they are operating effectively.[209] That seems specific enough, without much opportunity for error. Assessments, like those required of Google[210] and Facebook,[211] are often the only real weapons in the FTC's arsenal[212] because they ostensibly require a qualified, independent third party to verify corporate compliance. And they have been heralded as game changers.[213]

In reality, assessments have failed to achieve that goal because some of them have become mere symbols of compliance. The FTC requires *assessments*, and assessments are not the intense, independent, under-the-hood investigations we think of when we think of audits. They leave wiggle room for regulated companies. Audits are independent third-party analyses, where the auditor herself reviews evidence and makes conclusions independent of the audit subject.[214] Assessments are based on assertions

207. Telephone Interview with former Google employee, *supra* note 205.

208. *See, e.g.*, Decision and Order, *In re* Google, Inc., FTC File No. 102 3136, No. C-4336 (F.T.C. Oct. 13, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf [perma.cc/4X8V-UBLM] [hereinafter Google Order]; Decision and Order at 4, *In re* Twitter, Inc., FTC File No. 092 3093, No. C-4316 (F.T.C. Mar. 2, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf [perma.cc/8WD7-4H4Z].

209. *See* Google Order, *supra* note 208, at 5.

210. *See* Google Consent Decree, *supra* note 187, at 5–6.

211. *See* Agreement Containing Consent Order at 6–7, *In re* Facebook, Inc., FTC File No. 092 3184, No. C-4365, (F.T.C. Nov. 29, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf [https://perma.cc/RHW6-LL3V].

212. The FTC's authority to impose administrative fines is severely limited. *See* HOOFNAGLE, *supra* note 14, at 166; Solove & Hartzog, *supra* note 14, at 605. Companies that violate settlement orders are subject to civil penalties up to $16,000 for each violation. *See Commission Approves Federal Register Notice Adjusting Civil Penalty Amounts*, FED. TRADE COMMISSION (Dec. 23, 2008), http://www.ftc. gov/opa/2008/12/civilpenalty.shtm [https://perma.cc/9R6T-A948].

213. 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/K7QT-HTC3] (quoting David Vladeck, former Director of the FTC's Consumer Protection Bureau); *see also* Kashmir Hill, *So, What Are These Privacy Audits That Google and Facebook Have to Do for the Next 20 Years?*, FORBES (Nov. 31. 2011, 2:29 PM), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-auditsthat-google-and-facebook-have-to-do-for-the-next-20-years/ [https://perma.cc/TZ3V-HXZG].

214. *See, e.g.*, Jonathan Macey & Hillary A. Sale, *Observations on the Role of Commodification, Independence, and Governance in the Accounting Industry*, 48 VILL. L. REV. 1167, 1173 (2003) (laying

from management rather than wholly independent analyses from auditors, and are usually framed by goals set by management.[215] That means that the company that is supposed to be the subject of the assessment is, in fact, determining the bases upon which it gets evaluated, thus giving companies some power to predetermine the results. For example, the FTC wanted an assessment to ensure that Google had a privacy team, an ongoing and flexible privacy assessment process, relationships with vendors capable of protecting data, and a few other related requirements.[216] But based on a redacted version of the report, the assessment used conclusory language that was based almost entirely on Google proffers. For example, the report states that "Google has implemented a privacy risk assessment process in order to identify reasonably foreseeable, material risks, both internal and external," tracking the language of the FTC order explicitly.[217] As evidence for this conclusory statement, the report refers the reader to Google's responses to the auditor's questions, not any actual evidence.[218] Later, the report concludes that "Google's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information" based only on "the Google Privacy Program set forth in Attachment A of Management's Assertion in Exhibit I."[219] In other words, the only evidence showing that Google met FTC requirements was Google's statements to that effect. The fact that these assessments can be fulfilled through rough conclusory statements without independent investigation shows how assessments can become mere symbols of compliance.

4. Managerialization of Privacy Law

Despite sometimes elevating mere form over substance, checklists, compliance templates, assessments, and other symbolic tools have diffused through the privacy ecosystem.[220] Professionals share their experiences and

out the requirements of audits under federal securities law); *see also* Melvin A. Eisenberg, *The Board of Directors and Internal Control*, 19 CARDOZO L. REV. 237, 254–55 (1997) (describing the responsibilities of independent auditors under Section 10A of the Securities Exchange Act).

215. *See* Megan Gray, *Understanding and Improving Privacy "Audits" Under FTC Orders*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y 6 (Apr. 18, 2018, 1:10 PM), https://cyberlaw.stanford.edu/files/blogs/white%20paper%204.18.18.pdf [perma.cc/L99D-7LVG].

216. *See* Google Consent Decree, *supra* note 187, at 5–6.

217. *See* FED. TRADE COMM'N, INITIAL ASSESSMENT REPORT ON GOOGLE'S PRIVACY PROGRAM FOR THE PERIOD OCT. 29, 2011 – APR. 25, 2012, at 9 (June 22, 2012), https://epic.org/privacy/ftc/googleb uzz/FTC-Initial-Assessment-09-26-12.pdf [perma.cc/9M9L-YNDY].

218. *Id.*

219. *Id.* at 14.

220. *See* 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).

recommendations with each other through both formal and serendipitous interactions at workshops and conferences.[221] I witnessed this first hand at the IAPP's national conference and at smaller professional gatherings of privacy professionals, including the Privacy+Security Fora. This can be helpful; professionals can learn from each other, offer suggestions based on experiences, and improve their own protocols. The spread of these programs through social networks can also contribute to what organizational sociologists Paul DiMaggio and Walter Powell have called "isomorphism," or the tendency of companies in the same market to function, hire, and structure themselves in similar ways.[222] That is why we see similar privacy compliance checklists and similar privacy organizational structures in many companies.

Another consequence is that these structures—and their designers—become the loci at which privacy law is negotiated, addressed, and implemented on a regular basis. When Edelman discussed the managerialization of antidiscrimination law, she noted that compliance professionals interpreting policies and running internal review processes had become the center of legal interpretation and implementation.[223] What is happening in privacy law is similar. Even where in-house privacy professionals are doing their best, the tendency to managerialize compliance can shift the locus of privacy law to compliance professionals and engineers at privacy technology vendors, and shift the goal of compliance from substantive adherence to procedural box-checking.[224]

Compliance professionals inside companies contribute to the managerialization of privacy law by talking about privacy in managerial terms. In the employment discrimination context, Edelman noticed that despite the fact that the Civil Rights Act specifically spoke to race and sex discrimination, compliance professionals on the ground tended to couch their work in terms of diversity, generally,[225] and offered managerial (i.e.,

221. *See* EDELMAN, *supra* note 18, at 78-79 (discussing the impact of professional organizations and information resources in the human resources field). The IAPP hosts the largest of these conferences, attracting thousands of privacy professionals to several events per year. *See Conferences*, IAPP, https://iapp.org/conferences/ [https://perma.cc/5R2X-4QMT]. The Privacy+Security Forum (PSF) runs domestic and international conferences for privacy professionals each year, attracting hundreds of attendees to each event. *See* PRIVACY+SECURITY ACAD., https://privacyandsecurityforum.com/ [https://perma.cc/HF6S-QEQS]. In Europe, the Française de Correspondants à la Protection des Données à Caractère Personnel and the CPDP conferences in Brussels attract members of the privacy professional class, as well. *See* FRANÇAISE DE CORRESPONDANTS À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL (AFCDP), https://www.afcdp.net/ [https://perma.cc/7HEL-GW6Y]; COMPUTERS, PRIVACY & DATA PROTECTION (CPDP), https://www.cpdpconferences.org/ [https://perma.cc/ND4Y-KYNN].

222. *See* DiMaggio & Powell, *supra* note 101, at 147–49, 153.

223. *See* EDELMAN, *supra* note 18, at 124–50.

224. *See* COHEN, *supra* note 17, at 143–47.

225. *See* EDELMAN, *supra* note 18, at 140–42 (concluding that "[d]iversity rhetoric subtly but dramatically reshaped the focus of civil rights compliance by de-emphasizing the focus on race and sex

profit), rather than social, justifications for increased diversity.[226] This has the effect of incenting even those executives who care about racial and gender equality to think about diversity in more nebulous terms and through a corporate profit lens.[227] Some privacy professionals and technology vendors[228] are doing the same thing to privacy. They see privacy as one part of a compliance ecosystem focused on enhancing efficiency, speed, and productivity, while reducing the risk of debilitating fines. They see privacy structures in marketing terms: users are more likely to continue to share information with data collectors if users feel their privacy is protected.[229] The IAPP has hosted web conferences and published blogs focused on the efficiency and productivity benefits of privacy technology vendors.[230] And although consumers can benefit when companies start thinking about privacy as good for business,[231] the value proposition is nevertheless shifted from what helps consumers to what helps corporations.[232]

When that happens, those responsible for compliance advance managerial, rather than substantive, privacy goals.[233] Corporate goals like

---

and replacing it with a broad set of dimensions on which organizations could achieve diversity" based on quantitative and qualitative research of management literature and executives and compliance professionals).

226. *See id.* at 142–46 (showing how executives argued for greater diversity because it would increase profits and be good for business).

227. *Id.* at 149–50; *see also* Lauren B. Edelman, Sally Riggs Fuller & Iona Mara-Drita, *Diversity Rhetoric and the Managerialization of Law*, 106 AM. J. SOC. 1589, 1609–21 (2001); *id.* at 1621 ("[D]iversity rhetoric subtly alters formal legal ideas of diversity by advocating diversity on a variety of dimensions that go well beyond those specified by civil rights law."). This can have a negative effect on equality and civil rights. As Edelman, Fuller, and Mara-Drita note, managerial models of "diversity" elevate categories of diversity—"geographic location, organizational rank, dress style, communication style, and attitudes"—as equally as important as race and gender, thus de-emphasizing the law's focus on "discrimination, injustice, and historical disenfranchisement." *Id.* at 1632.

228. AuraPortal, for example, offers a GDPR compliance tool actually called "GDPR Accelerator" and markets the product as a way to "accelerate compliance in record time." *GDPR: Accelerate Compliance in Record Time*, AURAPORTAL, https://www.auraportal.com/product/gdpr/ [https://perma.cc/MF9U-3R4E].

229. *See, e.g.*, Timothy Morey, Theodore "Theo" Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV., May 2015, at 96, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust [perma.cc/2SKT-XWHL].

230. *See, e.g.*, *Operationalizing Privacy Tech—A Privacy Pro's Perspective*, IAPP (Apr. 13, 2017), https://iapp.org/store/webconferences/a0l1a000003gUuyAAE/ [perma.cc/AM9P-GPWA].

231. *See* ANN CAVOUKIAN, PRIVACY BY DESIGN: STRONG PRIVACY PROTECTION—NOW, AND WELL INTO THE FUTURE 18 (2011), https://www.ipc.on.ca/wp-content/uploads/Resources/PbDREport.pdf [perma.cc/2NYF-LHVM]; *see also* Reidenberg, *Restoring*, *supra* note 196, at 771–72 ("Privacy is a critical issue for the growth of electronic commerce. . . . The fair treatment of personal information and citizen confidence are each necessary conditions for electronic commerce over the next decade.").

232. *See also* COHEN, *supra* note 17, at 145 (discussing how managerializing internal dispute resolution tilts the scales away from individuals seeking to effectuate their privacy rights and toward corporate interests of efficiency and eliminating disruptions to innovation).

233. In the employment discrimination context, Edelman described how human resources offices, internal dispute mechanisms, mandatory arbitration, and other structures that developed after the Civil Rights Act contributed to the "managerialization" of civil rights law, or where structures become the

efficiency, productivity, and profit are often thought to be in tension with the substantive legal goals of regulatory legislation, like equality, nondiscrimination, or, in this case, consumer privacy.[234] Even though, as Julie Cohen and others have noted,[235] there is no such conflict, corporate interests and their vendors on the ground are contributing to a narrative that regulation is antithetical to innovation and, more specifically, that consumer privacy rights have to take a back seat to corporate goals. Granted, there are many privacy professionals that are strong internal advocates for personal privacy and deep, substantive adherence to legal norms;[236] however, merely symbolic structures are often being used to advance management goals to the detriment of consumers.

5. Managerialization and the Perception of Compliance

This happens because the use of managerial rhetoric around privacy and the proliferation of compliance structures influences the perception of adherence. That is, if we understand privacy law in managerial terms—as focused on managing corporate risk, balancing regulation and profit, and enhancing innovation—instead of protecting individuals, we tend to see merely symbolic structures developed in line with those terms as constituting compliance with the law. They get so engrained in our legal consciousness[237] that, over time, no one bothers to look under the hood and

---

setting for advancing managerial goals rather than the substantive legal goals the legislation intended. *See* EDELMAN, *supra* note 18, at 124–25.

234. *See, e.g.*, *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 11 (2012) (statement of Rep. Marsha Blackburn, Member, H. Comm. on Energy & Commerce) ("And what happens when you follow the European privacy model and take information out of the information economy? . . . [R]evenues fall, innovation stalls, and you lose out to innovators who chose to work elsewhere."); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 7, 15, 26–28 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [perma.cc/6ZL4-PPPC] (noting the comments from industry that privacy regulation would increase costs and decrease profits).

235. *See, e.g.*, Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1, 29–30 (2019); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1919–20 (2013) (noting that the "simplistic" view of privacy as antithetical to innovation and profit "fails to take into account either the nature of innovative practice or the dynamic function of privacy"); *see also* Katherine J. Strandburg & Yafit Lev-Aretz, *Better Together: Privacy Regulation and Innovation Policy* (forthcoming 2019) (demonstrating that little evidence exists for the argument that privacy regulation will stifle technology innovation).

236. The IAPP recognizes that persuading executives to take action on privacy is one of a CPO's top priorities. *See* Michael Spadea, *Getting Your Board on Board, Part II*, IAPP (Sept. 1, 2012), https://iapp.org/news/a/getting-your-board-on-board-part-ii/ [https://perma.cc/S8LW-3QTA]; Chris Pahl, *Getting Your Board on Board, Part III*, IAPP (Sept. 1, 2012), https://iapp.org/news/a/getting-your-board-on-board-part-iii/ [https://perma.cc/A2S8-SQCV].

237. *See* EDELMAN, *supra* note 18, at 154–55 (arguing that in the employment discrimination context, the managerialization of civil rights law encouraged many social groups—from employees to

see the hollow shell inside.[238] The effect is the frustration of consumer privacy rights because users assume the law cannot help them.

This is already happening in privacy law. Joe Turow has shown that we assume websites with privacy policies actually protect our privacy,[239] even though a privacy policy is merely a statement of data use practices rather than a promise of confidentiality.[240] And Woodrow Hartzog has argued that users and policymakers too often confuse structures of user control over privacy—consent buttons, left-to-right toggles, cookie consents, and even opt-in buttons, to name a few—with actual user empowerment and privacy.[241] The problem, as Hartzog insightfully notes, is that "control doesn't scale. The sheer number of choices that inundate users under a control regime is overwhelming to the point of futility."[242] Choice, though technically required by even supposedly strict laws like the GDPR, becomes an easy tactic for shifting the burden of privacy management from the technology company, which is actually well-situated to address privacy issues efficiently, to the user, who is not.[243] No wonder Facebook CEO

judges—to perceive the mere presence of an anti-discrimination policy, for example, as proof that the company was following Title VII).

238. John Meyer and Brian Rowan called this the "rationalized myth" of formal structures. John W. Meyer & Brian Rowan, *Institutional Organizations: Formal Structure as Myth and Ceremony*, 83 AM. J. SOC. 340, 343 (1977).

239. *See* Joseph Turow, Michael Hennessy & Nora Draper, *Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003-2015*, at 62 J. BROADCASTING & ELECTRONIC MEDIA 461, 463 (2018) (finding that more than half of Americans surveyed believe that a company with a privacy policy does not share customer information with anyone); *see also* Aaron Smith, *What Internet Users Know About Technology and the Web*, PEW RES. CTR. (Nov. 25, 2014), http://www.pewresearch.org/wp-content/uploads/sites/9/2014/11/PI_Web-IQ_112514_PDF.pdf [perma.cc/UMX3-HEW7] (making similar findings across age and educational groups).

240. *See* EDELMAN, *supra* note 18, at 155 (using the phrase "managerialization of legal consciousness" to describe when individuals tend to see the presence of symbolic structures as not merely tools to achieve compliance but as actually achieving substantive legal goals).

241. *See* HARTZOG, *supra* note 71, at 62–63.

242. *Id.* at 64. Too many choices lead to consumer exhaustion or choice nihilism. There is a long consumer behavior literature on overchoice. *See, e.g.*, Sheena S. Iyengar & Mark R. Lepper, *When Choice is Demotivating: Can One Desire Too Much of a Good Thing*, 79 J. PERSONALITY & SOC. PSYCHOL. 995, 997–1004 (2000) (using field and laboratory experiments showing consumers are more likely to make purchases given smaller sets of choices); Benjamin Scheibehenne, Rainer Greifeneder & Peter M. Todd, *Can There Ever Be Too Many Options? A Meta-Analytic Review of Choice Overload*, 37 J. CONSUMER RES. 409 (2010) (reviewing the literature on overchoice); Barry Schwartz & Andrew Ward, *Doing Better but Feeling Worse: The Paradox of Choice*, *in* POSITIVE PSYCHOLOGY IN PRACTICE 86, 86–88 (P. Alex Linley & Stephen Joseph eds., 2004) (too much choice has negative consequences). For a discussion of how overchoice and other cognitive barriers prevent individuals from effectuating their real privacy preferences, see Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the "Privacy Paradox,"* 31 CURRENT ISSUES PSYCHOL. (forthcoming 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3456155.

243. This argument parallels a thesis in tort law known as the least, or cheapest, cost avoider, which posits that, as between two parties involved in an accident, the one more capable of efficiently addressing the risk involved should be responsible. *See* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS (1970); Guido Calabresi & Jon T. Hirschoff, *Toward a Test for*

Mark Zuckerberg talked about giving users more choices and more control fifty-three times during his 2018 testimony before the United States Senate.[244]

We live in a legal environment in which privacy rights mobilization is already difficult; managerial privacy compliance exacerbates the problem. Standing requirements[245] and other hurdles hamper privacy plaintiffs' use of tort law,[246] contract law,[247] and federal privacy statutes[248] to vindicate their privacy rights. Even the FTC's power to force a company to overhaul its approach to privacy and security is under scrutiny.[249] Current law's consent paradigm imposes minimal obligations on technology companies while giving them ample opportunity to manipulate consumers by design.[250] And most users are dissuaded from even learning about their privacy rights because so many corporate executives and self-styled experts say that privacy is dead.[251] But by focusing on compliance paper trails,

Strict Liability in Torts, 81 YALE L.J. 1055, 1060 (1972) (the party that could avoid an accident at lowest cost should be liable for the accident even if he took due care).

244. *See Facebook, Social Media Privacy, and the Use and Abuse of Data, Hearing Before the S. Comm. on the Judiciary and the S. Comm. on Commerce, Sci., & Transp.*, 115th Cong. (2018) (testimony of Mark Zuckerberg, Chairman and CEO, Facebook, Inc.).

245. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1541–42 (2016) (requiring data breach plaintiffs to demonstrate concrete and particularized harm for Article III standing); *see* Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 440 (2017) (noting that *Spokeo* "seems to be serving no purpose other than to constitutionalize a deregulatory agenda").

246. *See, e.g.*, Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995) (rejecting an intrusion upon seclusion claim against American Express for renting purchase histories because plaintiffs were "voluntarily, and necessarily, giving information to defendants"). *But see* Scott Skinner-Thompson, *Privacy's Double Standards*, 93 WASH. L. REV. 2051, 2051 (2018) (showing how plaintiffs of privilege fair better in privacy tort claims and arguing for a reinvigoration of privacy tort law to protect the privacy rights of marginalized populations).

247. *See, e.g.*, *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 316–18 (E.D.N.Y. 2005) (rejecting a contract claim against JetBlue for disclosing customer information to third parties in contravention of its privacy policy because plaintiffs failed to identify and plead any damages). *But see* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 755 (2018) (arguing that courts should consider intangible, but no less serious, harms when considering invasion of privacy claims and failing to do so runs afoul of the common law).

248. *See, e.g.*, *In re* Pharmatrak, Inc. Privacy Litig., 292 F. Supp. 2d 263 (D. Mass. 2003) (granting summary judgment to defendant Pharmatrak on claims that it violated the Electronic Communications Privacy Act because plaintiffs failed to demonstrate the requisite intent).

249. *See, e.g.*, LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018) (holding that an FTC consent order requiring a company to overhaul its security practices to meet a general standard of "reasonableness" is unenforceable for vagueness).

250. *See* HARTZOG, *supra* note 71, at 21–54 (describing how technologies are designed to manipulate users into giving their data to tech companies); *see id.* at 62–67 (showing how companies extract consent from users by relying on confusion and exhaustion); *see also* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1005–06 (2014) (discussing the manipulative work of "dark patterns" and noting that "[e]ven general knowledge of consumer psychology, coupled with clever design, can lead to abuse"); Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proc. ACM on Hum.- Computer Interaction. (Sept. 20, 2019), https://arxiv.org/pdf/1907.07032.pdf [per ma.cc/77D5-ENTJ].

251. *See, e.g.*, Thomas L. Friedman, *Four Words Going Bye-Bye*, N.Y. TIMES (May 20, 2014), https://www.nytimes.com/2014/05/21/opinion/friedman-four-words-going-bye-bye.html [https://perma

managerialization of privacy law makes vindicating privacy rights even harder. Eleven of thirteen privacy compliance professionals I interviewed agreed with the assessment from a risk and compliance executive in New York that "we document everything so we have a log when someone comes after us."[252] Many privacy technology vendors also see compliance records as a means of protecting the company against consumer lawsuits or government investigations, as demonstrated by how many market themselves as helping clients achieve GDPR compliance by preparing for audits.[253] Demonstrations of these products and their market positioning suggest that the products are almost entirely focused on "reducing the cost, time and effort required to prepare for audits."[254] Even the Information Commissioner's Office (ICO) of the United Kingdom fell into this line of thinking. In its *Guide to the General Data Protection Regulation (GDPR)*, the ICO counseled companies to document processing activities to "help [them] demonstrate [their] compliance with other aspects of the GDPR."[255]

When a company can claim that it should not be held responsible for data misuse because, despite privacy problems in a final product, they completed a privacy impact assessment and documented internal approaches to privacy issues, individuals and regulators are both immediately put on the defensive and may be dissuaded from mobilizing their rights and investigative powers in the first place.[256] Granted, the GDPR includes documentation requirements;[257] companies need reports to prove they took "reasonable and appropriate" steps to protect consumer privacy under FTC consent decrees.[258] But the way some market players conflate the structure of

.cc/43TD-JL3S] (declaring "privacy is over"); Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [https://perma.cc/V88U-AE89] (quoting Mark Zuckerberg as saying "that privacy was no longer a 'social norm'"); Polly Sprenger, *Sun on Privacy: "Get Over It,"* WIRED (Jan. 26, 1999, 12:00 PM), https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ [perma.cc/B23E-CJRC] (quoting Scott McNealy, former chairman of Sun Microsystems).

252. Interview with risk and compliance executive, in N.Y.C., N.Y. (Aug. 8, 2017) (notes on file with author).

253. Compliance Point, for example, guarantees that its OnePoint platform "enables organizations to implement a unified approach to complying with . . . HIPAA, . . . FISMA[(Federal Information Security Management Act)], . . . Cyber Security Framework, GDPR, and more." *See the Difference OnePoint Delivers*, COMPLIANCE POINT, https://www.compliancepoint.com/onepoint [https://perma.cc/9L9Y-Z65N].

254. *Id.*

255. INFO. COMMISSIONER'S OFFICE, GUIDE TO THE GENERAL DATA PROTECTION REGULATION (GDPR) 98 (Mar. 22, 2018), https://iapp.org/media/pdf/resource_center/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf [perma.cc/S5W3-WCAU].

256. *See* COHEN, *supra* note 17, at 145 (describing how managerialization can contribute to the erosion of procedures that traditionally protected individual rights).

257. *See* GDPR, *supra* note 9, art. 30, ¶ 1, at 50–51.

258. *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief at 10, Fed. Trade Comm'n v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf [perma.cc/X

compliance (the records) with actual compliance (following the GDPR) is striking.

The focus on documentation as an end in itself elevates a merely symbolic structure to evidence of actual compliance with the law, obscuring the substance of consumer privacy law and discouraging both users and policymakers from taking more robust actions. Paul Butler made a similar argument about the effect of *Gideon v. Wainwright*[259] on the incarceration of poor persons of color.[260] By focusing on a process right—the right to counsel—*Gideon*, Butler argues, obscured the "real crisis of indigent defense" that prison is designed for poor people and not rich ones.[261] Ensuring some adequate representation "invests the criminal justice system with a veneer" of legitimacy, impartiality, and protection for ordinary persons, discouraging anyone from digging any deeper.[262] Butler concluded that "[o]n its face, the grant that *Gideon* provides poor people seems more than symbolic: it requires states to pay for poor people to have lawyers. But the implementation of *Gideon* suggests that the difference between symbolic and material rights might be more apparent than real."[263] The same thing is happening in privacy law. Privacy professionals' and third-party vendors' focus on records and documentation offers a convenient veneer of legitimacy to a process of technology design, data use, and information flow that remains unaltered and harmful to consumers.

Risk framing also tilts the scales against consumers. When compliance professionals focus on managing corporate risk under privacy laws, they focus on what is good for them, not what the law requires in substance. Like the management lawyers in Edelman's research, many of whom recommended creating symbolic structures to make employers appear like they were doing their best to improve workplace equality,[264] some privacy professionals see compliance as convenient ways to stave off investigations, audits, and legal challenges. Within a risk narrative, that positioning serves to discourage rights mobilization and regulatory inquiry.[265]

QH9-8HQE] (alleging that the hotel chain failed "to provide *reasonable* and *appropriate* security for the personal information [it] collected and maintained" (emphasis added)); *see also* Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators (Dec. 17, 1980), *reprinted in In re* Int'l Harvester Co., 104 F.T.C. 949, 1070–76 (1984), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [perma.cc/Q5RE-Y334] (explaining evolution of, and rationale for, FTC's consumer unfairness jurisdiction).

259. 327 U.S. 335 (1963).

260. *See* Paul D. Butler, *Poor People Lose:* Gideon *and the Critique of Rights*, 122 YALE L.J. 2176 (2013).

261. *Id.* at 2178.

262 *Id.* at 2178-79.

263. *Id.* at 2191–92 (emphasis omitted).

264. *See* EDELMAN, *supra* note 18, at 16–64 (discussing the ways in which management lawyers focus more on impression management than with actually fostering nondiscrimination").

265. *Id.* at 165–67; *see also* COHEN, *supra* note 17, at 145.

6. Deference to Symbols in Privacy Law

The legal endogeneity narrative reaches its climax when, after becoming part of our collective legal consciousness, merely symbolic structures are leveraged by lawyers, judges, and regulators as actual evidence of adherence to the law.[266] There are three steps in this process: "reference, relevance, and deference."[267] Reference occurs where judges merely refer to symbolic structures in their decisions. Relevance involves a judge noting or ruling that having a structure, like an internal dispute resolution process, is relevant to whether a company complied with a law like Title VII.[268] And deference, the final stage, occurs when judges see the mere presence of a compliance structure as dispositive.[269] In the employment discrimination context, Edelman found evidence of deference to merely symbolic structures littered throughout the law. Management attorneys listed them in their defense briefs, judges referred to them and pointed to them as evidence of compliance, and even plaintiffs' lawyers adopted them as goals for injunctive relief.[270] In the privacy space, it remains difficult to assess legal endogeneity just yet because a new privacy law landscape is still unfolding.[271] But the process is indeed ongoing.

---

266. *See* EDELMAN, *supra* note 18, at 168 (discussing the definition of legal endogeneity and the stage of legal deference to symbolic compliance).

267. *Id.* at 173.

268. Importantly, Title VII of the Civil Rights Act prohibits workplace discrimination on the grounds of race, color, religion, sex, and national origin. *See* Pub. L. No. 88-325, 78 Stat. 335 (codified as amended at 42 U.S.C. §§ 2000e to 2000e-17 (2012)). It does not require internal dispute resolution protocols. A company could comply with anti-discrimination law without them. The legal endogeneity problem at the deference stage is that legal systems confuse the mere presence of a structure with actual compliance with the law.

269. *See* EDELMAN, *supra* note 18, at 173.

270. *Id.* at 171–73.

271. The final text of the GDPR was announced in 2016 and its effective date was May 25, 2018. *See* GDPR, *supra* note 9; *see also The History of the General Data Protection Regulation*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [https://perma.cc/6AFH-Y2UP]. There are also several privacy bills under consideration in the United States Congress. Senator Ron Wyden (D-Oregon) has proposed the Consumer Data Protection Act, which calls for more transparency, empowers the FTC as a privacy regulator, includes a right to access and correct data, imposes fines, and proposes possible criminal penalties for executives. *See* Mind Your Own Business Act of 2019, S. __, 116th Cong. (1st Sess. 2019), https://www.wyden.senate.gov/imo/media/doc/Mind%20Your%20Own%20Business%20Act%20of%202019%20Bill%20Text.pdf [https://perma.cc/A9AD-56MC]. Senator Brian Schatz (D-Hawaii), along with fourteen Democratic co-sponsors, introduced the Data Care Act at the end of the last Congress. Data Care Act of 2018, S. 3744, 115th Cong. (2d Sess. 2018), https://www.schatz.senate.gov/imo/media/doc/Data%20Care%20Act%20of%202018.pdf [perma.cc/527V-VZ2Z]. The Data Care Act is based on principles of fiduciary law and imposes duties of care, loyalty, and confidentiality on data collectors. *See also* Keir Lamont, *Senate Commerce Committee Hears Consumer Perspectives on Privacy Legislation*, DISRUPTIVE COMPETITION PROJECT (May 3, 2019), http://www.project-disco.org/privacy/050319-senate-commerce-committee-hears-consumer-perspectives-on-privacy-legislation/#.XM1Ioi2ZOu4 [https://perma.cc/822A-MK4Q]. California's Consumer Privacy Act takes effect on January 1, 2020, and New York State is considering a new comprehensive privacy law, as well. *See* Issie Lapowsky,

Since the mid-1990s, the FTC has enforced a largely self-regulatory privacy regime,[272] which has allowed industry to set the terms of the debate. Almost all of what Daniel Solove and Woodrow Hartzog have called the "common law of privacy"—the decades of FTC consent decrees—are actually settlement agreements with regulated entities.[273] That means that the law regulating technology companies is, in part, dictated by the companies themselves. The FTC also defers to industry practices in the area of data security.[274] Companies will often promise that customer information is encrypted,[275] secured,[276] or adequately protected.[277] But when there is a data breach, the FTC relies on the customary practices of industry to set a baseline for what a company should have done in the first place. In *United States v. ValueClick*, for example, the FTC alleged that ValueClick "did not encrypt sensitive information consistent with industry standards."[278] And in *In re Eli Lilly & Co.*, the FTC alleged that the company failed to use the "industry standard secure socket layer encryption."[279] Industry custom has long been a yardstick by which the common law measured reasonable

New York's Privacy Bill Is Even Bolder than California's, WIRED (June 4, 2019, 7:00 AM), https://www.wired.com/story/new-york-privacy-act-bolder/ [https://perma.cc/FJR4-MBY6]. Although it is true that the EU Privacy Directive, which the GDPR replaced, created some significant privacy and security compliance requirements and that discussions about the GDPR began long before its text was released, the privacy compliance market is still relatively new.

272. *See* Haynes, *supra* note 196, at 593 (noting that "[o]nline privacy policies have appeared . . . as a voluntary measure by websites" (footnote omitted)); Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046–47 (2000) (discussing how the FTC's suggestion of more privacy regulation resulted in more sites offering privacy policies).

273. *See* Solove & Hartzog, *supra* note 14, at 606 ("In nearly all of the FTC's Section 5 cases and complaints alleging violations of COPPA, GLBA, and the Safe Harbor Agreement, the final disposition of the matter is a settlement, default judgment, or abandonment of the action by the FTC in the investigatory stage."); *see also* COHEN, *supra* note 17, at 188 (noting that consent decrees bring in private power to government decisions).

274. *See* Solove & Hartzog, *supra* note 14, at 636.

275. *See* Complaint for Permanent Injunction and Other Equitable Relief ¶ 43, Fed. Trade Comm'n v. Rennert, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000), http://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm [perma.cc/XNB5-E332].

276. *See* Complaint, *In re* Eli Lilly & Co., 133 F.T.C. 763 (2002) (No.C-4047).

277. *See, e.g.*, Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 12, 14, United States v. ValueClick, Inc., No. CV08-01711MMM(RZx) (C.D. Cal. Mar. 13, 2008), http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317complaint.pdf [https://perma.cc/B77C-K7AC].

278. *Id.* at 11.

279. *Eli Lilly*, 133 F.T.C. at 765.

care.[280] But even customs have to be reasonable,[281] suggesting a two-step reasonable care analysis. By starting with a heuristic set by industry, the analysis becomes endogenous, giving companies the opportunity to set a presumption that needs to be refuted, rather than the other way around. And even if we accept the relevance of industry custom in the FTC's privacy "common law," the prevalence of industry standards still speaks to the way regulated entities set the baseline on which they will be judged.

The FTC also defers to other industry structures of symbolic compliance. After the organization TRUSTe, now TrustArc, started issuing privacy "seals" certifying that a website's privacy policy met certain standards and norms, the FTC incorporated those seals as evidence of compliance.[282] In *FTC v. Toysmart.com*,[283] for example, the FTC noted that Toysmart had become "a licensee of . . . an organization that certifies the privacy policies of online businesses and allows such businesses to display a . . . trustmark or seal."[284] In so doing, the FTC was referring to a structure a third party had developed on its own, thus pushing TRUSTe's seals into the legal consciousness. As Solove and Hartzog note, this pushed more websites to create privacy policies.[285]

And despite their hype, the FTC's privacy assessments defer to corporate compliance structures all the time. Because assessments are based on attestations from corporate officers rather than independent investigation, Facebook was able to lie routinely to the FTC during its initial and biennial assessment reports required under the 2011 Consent Decree.[286] And the FTC's latest settlement with the company offers more of the same in this respect. Rather than empowering a strong independent auditor, the

280. *See, e.g.*, Trimarco v. Klein, 436 N.E.2d 502, 505 (N.Y. 1982) ("[W]hen proof of an accepted practice is accompanied by evidence that the defendant conformed to it, this may establish due care . . . ."); United States v. Carroll Towing Co., 159 F.2d 169, 179 (2d Cir. 1947) ("it may be that the custom" in New York Harbor was to not have bargees aboard their boats and if so, that "custom should control"); *see also* Clarence Morris, *Custom and Negligence*, 42 COLUM. L. REV. 1147 (1942) (evidence of custom is helpful because popular customs call into question plaintiff arguments about the feasibility of a different approach and highlight the place of the customary practice in society).

281. *See Trimarco*, 436 N.E.2d at 506 (noting that industry custom can only set the standard of due care if the industry custom is itself reasonable).

282. The FTC did sue TRUSTe for failing to "conduct annual recertifications for all companies holding TRUSTe Certified Privacy Seals" despite promises to the contrary. *See* Complaint at 4, *In re* True Ultimate Standards Everywhere, Inc, No. 1323219 (F.T.C. Nov. 17, 2014), https://www.ftc.gov/system/files/documents/cases/141117trustecmpt.pdf [perma.cc/P9N6-CJ5U].

283. First Amended Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. July 21, 2000), http://www.ftc.gov/sites/default/files/documents/cases/toysmartcomplaint.htm [perma.cc/32CZ-ELQK].

284. *Id.* ¶ 8.

285. *See* Solove & Hartzog, *supra* note 14, at 593.

286. *See* Complaint for Civil Penalties, Injunction, and Other Relief ¶¶ 12, 124, 181, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf [perma.cc/84LK-6Y35].

settlement permits assessments to be based entirely on documents Facebook provides to the assessor.[287] That means that Facebook will set the terms for its own evaluation, with assessors never looking under the hood.[288]

The GDPR also incorporates industry structures. Recognizing the importance of an internal advocate for privacy, the GDPR requires companies to hire a data protection officer and involve her "in all issues which relate to the protection of personal data."[289] Article 35 also requires companies to complete data protection impact assessments (DPIAs) before processing data.[290] Both of these elements are undoubtedly important. But a data protection office is a structure that could become merely symbolic if, as research has shown, the office is marginalized, unsupported, and disconnected from the process of technology design.[291] And DPIAs can become simple paper trails when seen as ends in themselves rather than as a substantive guide for helping a company determine if it should go ahead with or abort its planned data use. Companies can, therefore, take advantage of the delays and complexities in judicial decision-making to decide for themselves what the GDPR requires in practice.[292]

In the end, these seemingly small beachheads of symbolic structures in the law are nevertheless worrisome because they may have an anchoring effect on judges and regulators. Anchoring is a cognitive bias in which one relies too heavily on an initial piece of information when making decisions.[293] In this context, a symbolic structure like a seal or a CPO office could anchor an impression, later made official in a judicial decision or

287. *See* Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf [https://perma.cc/2QRJ-9KGF] [hereinafter Facebook Stipulated Order].

288. *See* COHEN, *supra* note 17, at 191 (noting that standards for what is and what is not acceptable tend to develop among auditors, particularly when their work is based on corporate-defined "best practices," leaving the details undiscovered).

289. *See* GDPR, *supra* note 9, art. 38, at 55–56.

290. *See id.* art. 35, at 53.

291. *See* Waldman, *supra* note 24 (showing that the pro-privacy ethos of privacy professionals inside corporations was not being fully realized because forces both exogenous and endogenous to the company created a disconnect between privacy professionals and engineers).

292. Europe has tried to stop companies from undermining the GDPR by having the Data Protection Board (DPB), formerly the Article 29 Working Party, and national data privacy authorities issue opinion and guidance documents that detail what does and does not comply with the GDPR. As Margot Kaminski has deftly studied, the DPB's interpretations are essential to properly construing the GDPR's requirements. *See* Kaminski, *supra* note 118. However, as noted earlier, the Board's guidance is still vague and there are still wide gaps in its coverage, thus allowing corporate actors to step in. *See supra* notes 121–122 and accompanying text.

293. *See, e.g.*, Timothy D. Wilson et al., *A New Look at Anchoring Effects: Basic Anchoring and Its Antecedents*, 125 J. EXPERIMENTAL PSYCHOL. 387, 387–88 (1996) (discussing the traditional anchoring effect and describing experiments verifying the impact of anchoring even on non-comparative judgments).

regulatory order, that a company is compliant with the law, even if the seal is meaningless or the CPO's office cannot influence design or data use.

C. The Sociopolitical Narrative of Symbolic Privacy Compliance

Undoubtedly, many of the privacy compliance structures developed at companies do constrain abusive data use practices. They serve as guardrails and set the tone for what data use practices are appropriate. But the trend toward compliance in name only, while not universal, is unmistakable. And we should be wary of these developments. Legal endogeneity threatens the rule of law by undermining the ability of social legislation to achieve its goals.[294] Faced with laws passed to give consumers more privacy protections, on the one hand, and a business model driven by the collection of consumer data, on the other, technology companies reorient regulatory legislation in ways that minimize disruption to profits regardless of what that does to privacy, shaping the contours and the meaning of the law as we know it. The merely symbolic structures companies create give them yet another chance—after intense lobbying[295] and actually drafting new legislation themselves[296]—to water down regulatory requirements they find onerous. Endogeneity, therefore, shifts the locus of power from policymakers to corporate actors, allowing companies to transform regulations aimed at curbing their excesses into pathways that actually serve their interests.

By shifting the locus at which privacy law is negotiated from policymakers to corporations, we also change the discourse of power. The language we use shapes our understanding and perceptions of legitimacy, reality, and legality.[297] As Foucault argued, "discourse transmits and produces power."[298] Critical race theorists have made similar arguments

294. *See* EDELMAN, *supra* note 18, at 216.

295. *See Lobbying: Top Spenders*, CTR. FOR RESPONSIVE POL., https://www.opensecrets.org/lobby/top.php?indexType=s [https://perma.cc/AYL4-R3KS].

296. *See, e.g.*, Abbe R. Gluck & Lisa Schultz Bressman, *Statutory Interpretation from the Inside—An Empirical Study of Congressional Drafting, Delegation, and the Canons: Part I*, 65 STAN. L. REV. 901, 906 (2013); *see also* Nourse & Schacter, *supra* note 90, at 575.

297. *See, e.g.*, Richard K. Sherwin, *Dialects and Dominance: A Study of Rhetorical Fields in the Law of Confessions*, 136 U. PA. L. REV. 729 (1988) (noting a change in how we talk about confessions and arguing that power has shifted alongside).

298. 1 MICHEL FOUCAULT, THE HISTORY OF SEXUALITY 101 (Robert Hurley trans., 1978) (arguing that the medical and psychiatric disciplines' use of the rhetoric of "normal" and "abnormal" sexual desire to distinguish opposite-sex from same-sex attraction gave power and legitimacy to heteronormative thinking, institutions, and constituencies); *see also* Gerald Turkel, *Michel Foucault: Law, Power, and Knowledge*, 17 J.L. & SOC'Y 170, 172 (1990) (describing Foucault's argument on "discourses of domination").

about the power of speech.[299] As have feminist scholars.[300] Our social understanding of privacy is written and discussed in a variety of ways, sometimes conflicting, overlapping, and cacophonous.[301] But through the noise, the discourse is accessible to consumers: it's "creepy" when Alexa listens to everything we say,[302] "anonymity" protects people from the effects of revelation,[303] we want more "control" over our information,[304] and we "trust" our friends to keep our secrets.[305] In a world where compliance professionals determine what the law requires and create symbolic compliance tools, the discourse of law becomes the discourse of compliance, paper trails, and checklists. This disempowers consumers, who have no access to this privacy discourse, and again serves to undermine the promise of privacy law as consumer protection.

More troubling is why this is happening. If, as I have endeavored to show, legal endogeneity is a problem for privacy law, it is not a surprising one. It is, I argue, the natural byproduct of our neoliberal managerial system, one that prizes and valorizes efficiency and deregulated markets over consumer welfare.

Neoliberalism represents resistance to a political system oriented around social values, solidarity, and welfare and replaces it with one dedicated to individualism as a paramount social value. Its proponents argue that individual human well-being is best "advanced by the maximization of entrepreneurial freedoms within an institutional framework characterized by[, among other things,] private property rights, individual liberty, [and]

299. *See, e.g.*, Charles R. Lawrence III, *If He Hollers Let Him Go: Regulating Racist Speech on Campus*, 1990 DUKE L.J. 431, 444 ("[R]acist speech constructs the social reality that constrains the liberty of non-whites because of their race."); *see also* PATRICIA J. WILLIAMS, THE ALCHEMY OF RACE AND RIGHTS 61 (1991) (we live with the legacy of slavery in part through "powerful and invisibly reinforcing structures of thought, language, and law").

300. *See, e.g.*, MARGARET THORNTON, DISSONANCE AND DISTRUST: WOMEN IN THE LEGAL PROFESSION (1996) (using real world examples of female lawyers to argue that Foucault's discourse of power is fundamentally a gendered dynamic).

301. *See* SOLOVE, *supra* note 114, at 14–36 (reviewing some of the many different definitions of privacy); *see* WALDMAN, *supra* note 114, at 13–45 (grouping seemingly conflicting visions of privacy into negative and positive conceptions).

302. Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 61–71 (2013) (describing situations where technologies functioned in ways users found "creepy").

303. This is particularly helpful for members of marginalized and stigmatized communities. *See, e.g.*, Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159 (2015) (arguing that privacy should be understood as preventing intimate information from serving as the basis of discrimination).

304. *See* INNESS, *supra* note 114, at 56 (privacy is "control over a realm of intimacy"); WESTIN, *supra* note 114, at 7 (defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"); Matthews, *supra* note 114, at 351 (privacy is making the choice to "control" and "manage" the boundary between ourselves and others).

305. *See* WALDMAN, *supra* note 114, at 51–52 (noting that trust allows us to share because it creates expectations of confidentiality and adherence to norms).

unencumbered markets."[306] Julie Cohen argues that law has facilitated remaking of society around neoliberal political economy.[307] For example, law defines property rights, limits oversight, grants legal immunity to corporations, creates self-regulatory regimes, and so forth. For privacy, this manifests itself when regulators rely on industry to make policy, as when corporate "best practices" are accepted without interrogation or assessments are taken at face value without independent investigation.[308] Often, this orientation results in what Jodi Short has called the "paranoid style" of governance,[309] or an overly modest approach based on exaggerated worries about state power and insufficient sensitivity to private power.

This is precisely what we see happening in privacy law. The FTC's humble regulatory posture, including its settlement practice, its inability to impose administrative fines, and its deferential stance on corporate assessments, just to name a few, stem from a neoliberal ethos that prioritizes deregulated markets and corporate innovation over human welfare. Even if the FTC wanted to perform more robust oversight, it has been hemmed in by Congressionally-imposed limitations on its authority, limitations that also stem from a neoliberal bent toward public regulation.[310] Europe has tried a different approach, with more active regulators and a more involved government. But no matter how aggressive European data protection authorities become, the relatively permissive approach in the United States, the primary home of the largest technology companies, will continue to hinder the European goal of protecting the fundamental right to data privacy.

In addition to formal legal institutions, law is institutionalizing neoliberalism through the ground-up "self-interested efforts of information-economy participants and the lawyers and lobbyists they employ."[311] Those efforts, examples of which are described throughout this Article, are geared toward protecting corporate power, minimizing the disruptive effects of regulation, reducing the risk of litigation, and increasing the efficiency and independence of the means of production. Julie Cohen describes those efforts as managerial. Managerial institutions are those that translate neoliberal ideology into an organizational system focused on deploying informational, structural, and technological tools to make themselves more

306. *See* COHEN, *supra* note 17, at 7 (quoting David Harvey, *Neoliberalism as Creative Destruction*, 610 ANNALS AM. POL. & SOC. SCI. 22, 22 (2007)).

307. *See id.* at 8–9.

308. *See supra* Part II.B.6; *see* also Gray, *supra* note 215.

309. Jodi L. Short, *The Paranoid Style in Regulatory Reform*, 63 HASTINGS L.J. 633, 635 (2012), *quoted in* COHEN, *supra* note 17, at 187.

310. *See* HOOFNAGLE, *supra* note 14, at 65, 166.

311. *See* COHEN, *supra* note 17, at 9.

efficient.[312] A managerial approach uses legal structures and discourse to privilege corporate efficiency and independence from government.[313] As a result, it undermines regulatory legislation from within, facilitating the creation of merely symbolic compliance structures. In the privacy space, the managerial ethos encourages in-house attorneys and privacy professionals to interpret legal obligations in line with corporate, rather than consumer, goals: the managerial question is "*how can we prove compliance with the least disruption and risk to production?*" instead of "*how can we proceed while creating fewer privacy risks for our consumers?*"[314] Companies also leverage paper trails to document their technical compliance with the law rather than using them to enhance substantive privacy protection for consumers through privacy-enhancing design.[315] Companies are even starting to outsource their privacy compliance functions to technology vendors.[316] This shifts a significant cost center, but it narrows privacy to what can be coded into software, thus impeding consumer privacy rights and frustrating the goals of privacy legislation. And yet, as discussed above, these procedures can serve as evidence of compliance even if they are substantively impotent.

Without evidence, industry also deploys the neoliberal discourse of deregulation and innovation to push back against what it sees as burdensome regulation.[317] For example, during a June 2019 hearing on New York State's proposed privacy bill, four representatives from industry—Ted Potrikus, the President and CEO of the Retail Council of New York State; Christina Fisher, Executive Director for Massachusetts and the Northeast of TechNet; Zachary Hecht, Policy Director for TechNYC; and John Olsen, Director of the Northeast Region of the Internet Association—referred to dangers of privacy laws stifling innovation twenty-seven times in one hour.[318] Google, Facebook, Amazon, and the American Chamber of

312. *Id.* at 143–45.
313. *Id.* at 156–57.
314. *See supra* Part II.B.2.
315. *See supra* Part II.B.2–II.B.5.
316. *See* Ari Ezra Waldman, *Outsourcing Privacy* (under submission) (manuscript on file with author). The IAPP's 2017 Privacy Tech Vendor Report included fifty-one vendors. The 2018 version includes 192, showing significant expansion of the market. *See* IAPP, 2017 PRIVACY TECH VENDOR REPORT (2017), https://iapp.org/media/pdf/resource_center/Tech-Vendor-Directory-1.4.1-electronic.pdf [perma.cc/QKN6-7VRV]; IAPP, 2018 PRIVACY TECH VENDOR REPORT 16 (2018), https://iapp.org/media/pdf/resource_center/2018-Privacy-Tech-Vendor-Report.pdf [perma.cc/EEY4-7CKY] [hereinafter VENDOR REPORT].
317. *See* COHEN, *supra* note 17, at 12–13.
318. *See Joint Public Hearing: To Conduct Discussion on Online Privacy and What Role the State Legislature Should Play in Overseeing It: Joint Public Hearing Before the S. Standing Comm. on Consumer Prot. and Standing Comm. on Internet and Tech.* (N.Y. 2019), https://www.nysenate.gov/calendar/public-hearings/june-04-2019/joint-public-hearing-conduct-discussion-online-privacy-and [https://perma.cc/KJZ6-R88M].

Commerce lobbied the European Union to weaken the GDPR in the name of innovation.[319] The Technology Policy Institute, a think tank almost entirely funded by large technology corporations, concluded that "there is no evidence . . . that use of big data for commercial and other non-surveillance purposes has caused privacy harms" and warned against innovation-stifling regulation.[320] And the discourse has made its way into official government documents. In 2010, the Department of Commerce published a paper that presumed privacy and innovation were in tension, using variations of the word "innovation" seventy-six times in seventy-eight pages.[321] Concerns about how privacy could disrupt innovation also figured prominently in the FTC's 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change*,[322] and in two reports from the Obama Administration in 2012[323] and 2014.[324]

Neoliberal managerialism and discourse, therefore, contribute to the endogeneity of privacy law by simultaneously weakening government's oversight posture and strengthening industry's ability to frame legal requirements in ways that serve their data-hungry business models. Together they create a political environment that prioritizes efficiency and demonizes regulation while imbuing the legal consciousness of corporate actors with the notion that leveraging merely symbolic structures is morally, politically, and even legally acceptable.

That might suggest that the legal endogeneity narrative described in this Article is more a systemic problem with today's political economy and compliance culture rather than a problem unique to privacy. That is both

---

319. *See* 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.

320. THOMAS M. LENARD & PAUL H. RUBIN, TECH. POLICY INST., THE BIG DATA REVOLUTION: PRIVACY CONSIDERATIONS 3, 26 (Dec. 2013), https://techpolicyinstitute.org/wp-content/uploads/2013/12/the-big-data-revolution-privac-2007594.pdf [perma.cc/DC3T-LD4V].

321. *See* DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK, at i (Dec. 16, 2010), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf [perma.cc/ZH82-TCDZ] ("Addressing [privacy] issues in way that protects the tremendous economic and social value of the Internet without stifling innovation . . . .").

322. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [perma.cc/V4Z9-2767] (referencing the notion that privacy regulation could harm innovation nineteen times, not including footnotes).

323. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 23, 2012), https://www.hsdl.org/?abstract&did=700959 [https://perma.cc/B692-EN7H].

324. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 20 (May 2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [perma.cc/LRL3-JRVJ] (referencing innovation concerns thirty times in seventy-nine pages, not including footnotes).

right and wrong. Though focusing on employment discrimination and the merely symbolic structures erected to comply with Title VII, Edelman suggested that some of the blame lay with "compliance professionals" who, in part because of "their professional training and roles,"[325] will frame the law in managerial ways. She also noted that because of "the growing compliance industry that markets its services, the risk framing [contributing to legal endogeneity] continues well after employers come to see the legal environment as a threat."[326] These problems are inherent to the compliance industry as a whole, not just in the privacy compliance space.

That said, seeing legal endogeneity as simply a general compliance problem misses the point. It is indeed a compliance problem, but one that is both new to privacy and uniquely detrimental to realizing the promises of law in information domains like privacy. Legal endogeneity has thrived in an era in which both industry and government have been informationalized. Where traditional legal regimes have either been slow to catch up or remain structurally incompatible with information-based systems, companies have rushed in to fill the void with internal structures that have the veneer of legality but serve their own interests. And judges are attracted to them as convenient, heuristic ways to (inadequately) apply familiar concepts to new problems.[327] And privacy, unlike employment discrimination, is steeped in technology, some of which is far beyond the casual expertise of judges, lawyers, and juries. When confusion abounds and regulated entities are assumed to be experts,[328] the exogenous legal system sees itself less competent to intercede and decide difficult questions for itself.[329] It becomes even more humble, even more "paranoid," and leaves corporate actors to act with even more impunity. Given the terabytes of data these companies collect and the manipulations possible from analyzing that data, that kind of unregulated freedom is uniquely dangerous.

---

325. EDELMAN, *supra* note 18, at 31.

326. *Id.* at 82.

327. *See* Cohen, *supra* note 17, at 143–69 (showing how managerialization of regulatory functions has become a feature of the information age).

328. There is a long literature describing the trust we sometimes blindly place in technology and the faith we put in its designers. *See, e.g.*, Kevin Anthony Hoff & Masooda Bashir, *Trust in Automation: Integrating Empirical Evidence on Factors that Influence Trust*, 57 HUM. FACTORS 407, 409–28 (2015) (collecting the literature on trust in automation and technology).

329. This phenomenon exists in other areas of the law, not just in privacy. *See, e.g.*, NEIL K. KOMESAR, LAW'S LIMITS: THE RULE OF LAW AND THE SUPPLY AND DEMAND OF RIGHTS 22 (2001) ("[T]he political process . . . functions worse as numbers and complexity increase and as the distribution of stakes becomes more complex and more dispersed."); Jay P. Kesan, *An Autopsy of Scientific Evidence in a Post*-Daubert *World*, 84 GEO. L.J. 1985, 2040 (1996) (noting that judges are reluctant "gatekeepers" of scientific evidence, instead delegating their duty to assess reliability of evidence). This is qualitatively different than *Chevron* deference, where it is appropriate and expected for judges to defer to agency experts. *See* Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 865 (1984) (regulatory schemes may be "technical and complex" and "[j]udges are not experts in the field").

III. RECLAIMING PRIVACY LAW'S PROMISE

So far, in constructing a legal endogeneity narrative in privacy law, I have argued that ambiguity and paper trail-based safe harbors in data protection law have given those on the ground the opportunity to frame legal requirements in ways that advance corporate, rather than consumer, interests.[330] This can have the effect of elevating form over substance, catalyzing the development of compliance structures that, on their face, seem to comply with the law, but, as mere symbols of compliance, actually frustrate the legislative goal of protecting the privacy of data subjects.[331] The last part of the legal endogeneity cycle occurs when mere symbols of compliance are given the official imprimatur by the law, or when symbolic structures fill the void left by the ambiguous laws that gave rise to them in the first place.[332] Evidence of judicial and regulatory deference to symbolic structures is already spreading throughout privacy law.[333] And that is putting privacy protection and the rule of law at risk.[334] Taking action now may still allow us to reverse course.

There is probably no single quick fix, no single way of writing a comprehensive privacy law that would always prevent managerialization and legal endogeneity, especially since neoliberalism fosters an environment that contributes to legal endogeneity. But that does not mean we have no recourse. We can try to stop the worst of legal endogeneity during its six-stage process.[335] Elsewhere, I have discussed some legal and structural changes necessary to encourage engineers to respect robust conceptions of privacy and to integrate privacy into every corner of a corporation's ethos, practice, and routine.[336] Similarly, changes in the exogenous legal context in which technology companies operate may be able to rewrite the inchoate legal endogeneity narrative I have so far described.

A. Law Reform

330. *See supra* Part II.B.1.

331. *See supra* Parts II.B.3–II.B.5.

332. *See* EDELMAN, *supra* note 18, at 168–215 (demonstrating the deference to symbolic structures in employment antidiscrimination law by courts and the Equal Employment Opportunity Commission).

333. *See supra* Part II.B.6.

334. *See supra* Part II.C.

335 *See supra* Figure 1 accompanying note 87.

336. *See* Waldman, *supra* note 24, at 701–25 (relying on a framework of supra, macro, meso, and micro factors developed by Ruth Aguilera to understand why businesses may engage in corporate social responsibility programs that are not profit-oriented).

The law contributes to the spread of merely symbolic structures by leaving it up to compliance professionals to interpret the meaning of vague statutes. It also incorporates discourse and processes that lend themselves to check-box compliance, managerialization, and the erosion of consumer values in favor of corporate ones. In both systematic and specific ways, the law can do better.

We need to move away from process-oriented, check-box visions of privacy law that are susceptible to symbolic structures. Fortunately, we have other options. Woodrow Hartzog has called for leveraging contract, tort, and consumer protection law to regulate the design of new technologies.[337] Elsewhere, I argued for leveraging lessons from the law of products liability for design defects to create an accountability regime for companies that design technologies with insufficient designed-in privacy protections.[338] A products liability regime is less susceptible to legal endogeneity than compliance-based approaches because of the powerful role litigation and courts can play in influencing design across an entire industry.

In addition, Jonathan Zittrain, Jack Balkin, Daniel Solove, Danielle Citron, and I have argued that data collectors should be treated as fiduciaries of our information and, therefore, subject to similar duties of care, loyalty, and confidentiality that characterize our relationships to doctors, lawyers, and trustees.[339] Duties of care would require companies that collect and process our information to take reasonable steps to secure personal data from unauthorized access. With "reasonable" defined according to traditional common law principles,[340] companies would have to do more

337. HARTZOG, *supra* note 71, at 120–56.

338. *See* Waldman, *supra* note 120.

339. *See, e.g.*, SOLOVE, *supra* note 114, at 102 (positing that businesses that are collecting personal information from us should "stand in a fiduciary relationship" with us); WALDMAN, *supra* note 114, at 79-92; Danielle Citron, *Big Data Brokers as Fiduciaries*, CONCURRING OPINIONS (June 19, 2012), http://www.concurringopinions.com/a rchives/2012/06/big-data-brokers-as-fiduciaries.html [https://perma.cc/82VQ-NX92] (a fiduciary relationship between data brokers and users would help fight the massive power imbalance that exists in today's unregulated environment); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), http://www.theatlantic.com/technology/archiv e/2016/10/information-fiduciary/502346/ [https://perma.cc/FK4B-XG5E]; Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016) ("[M]any online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries toward their customers and end-users.").

340. *See, e.g.*, Bethel v. N.Y.C Transit Auth., 703 N.E.2d 1214, 1216–17 (N.Y. 1998) (discussing the reasonable person standard). The literature on the reasonableness standard in tort law is voluminous. For some examples, please see Martha Chamallas, *Gaining Some Perspective in Tort Law: A New Take on Third-Party Criminal Attack Cases*, 14 LEWIS & CLARK L. REV. 1351, 1356–61 (2010) (discussing the prominence of the objective "reasonable person" standard in tort law); Joseph H. King, Jr., *Reconciling the Exercise of Judgment and the Objective Standard of Care in Medical Malpractice*, 52 OKLA. L. REV. 49, 49–56 (1999); *see also* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL & EMOTIONAL HARM §§ 9–11 (AM. LAW INST. 2010). The literature critiquing the reasonable person

than copy the symbolic structures created throughout their industry. They would have to ensure that those structures provide sufficient security to meet the legal standard of reasonableness.[341] Duties of loyalty mean that a company cannot use our data in ways that would foreseeably cause harm or would be highly offensive to a reasonable user. Playing with our emotions,[342] manipulating elections,[343] and listening in on our personal conversations,[344] for example, would be off limits. And duties of confidentiality would ensure that a company does not share any of our data with a third party unless those third parties agree to fulfill the same duties of care, loyalty, and confidentiality. A bill proposed at the end of the 115th Congress by Senator Brian Schatz of Hawaii reflected some of these ideas.[345] This is not to say that these proposals, if adopted, could never be undermined by merely symbolic structures. A first step, though, is to orient privacy law toward well-worn standards that have the clarity of centuries of common law behind them yet cannot easily be reduced to simple and underinclusive code.

B. Rule-Making and Guidance

European governments are trying to protect the integrity of the GDPR by cutting off the opportunity for corporations to determine for themselves what the GDPR requires. The European Data Protection Board, along with the privacy authorities of member states, are issuing guidance documents to spell out GDPR mandates in more detail. The UK ICO, for example, has issued guidance documents that give specific examples of the types of designs that meet GDPR legal standards.[346] And to meet the consent

standard is itself extensive. *See, e.g.*, Margo Schlanger, *Injured Women Before Common Law Courts, 1860-1930*, 21 HARV. WOMEN'S L.J. 79 (1998).

341. *See, e.g.*, Trimarco v. Klein, 436 N.E.2d 502, 505–07 (N.Y. 1982) (holding that evidence of industry custom is relevant for negligence but not dispositive because the custom must also be determined to be reasonable).

342. *See* Robinson Meyer, *Everything We Know About Facebook's Secret Mood Manipulation Experiment*, ATLANTIC (June 28, 2014), https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/ [https://perma.cc/33WW-CKER].

343. *See, e.g.*, Adam Pasick, *Facebook Says It Can Sway Elections After All—For a Price*, QUARTZ (Mar. 1, 2017), https://qz.com/922436/facebook-says-it-can-sway-elections-after-all-for-a-price/ [https://perma.cc/M5WR-5U63].

344. *See, e.g.*, Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You This Whole Time*, WASH. POST (May 6, 2019), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/ [https://perma.cc/8UL9-NUTM].

345. Data Care Act of 2018, S. 3744, 115th Cong. (2d Sess. 2018), https://www.schatz.senate.gov/imo/media/doc/Data%20Care%20Act%20of%202018.pdf [perma.cc/527V-VZ2Z].

346. At this writing, the United Kingdom is still planning on leaving the European Union by January 2020. Even if the UK does leave the Union, the UK ICO report is an example of a trend among European DPA.

requirements of Article 7, the agency advises that "affirmative opt-in methods might include signing a consent statement, oral confirmation, a binary choice presented with equal prominence, or switching technical settings away from the default."[347]

The United States lacks a similar resource for specificity.[348] This is why the FTC, or a new agency tasked specifically with privacy enforcement, needs the ability to write rules to clarify its authority. The purpose of agency rulemaking is to specify vague statutory requirements, offering clear notice as to what the law requires, an opportunity to participate in public governance, and a comprehensive resolution of questions facing large numbers of persons and businesses.[349] However, the FTC is limited by the "procedurally burdensome" process of Magnuson-Moss rulemaking,[350] which requires the FTC to conduct industry-wide investigations, prepare reports, propose rules, engage in a series of public hearings, and consider other alternatives.[351] The process is so difficult that the FTC has not engaged in it in decades.[352] This lack of rulemaking authority ensures that, without more, privacy regulation from the FTC will remain vague and technology companies will remain the primary movers in determining what a given legal standard requires. As it is, the only way to discern what the FTC means by a specific term or phrase is to turn to its previous consent decrees, which

347. *See What Is Valid Consent?*, UK ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ [https://perma.cc/2SEG-CA93].

348. Granted, the California Attorney General's Office has issued interpretive guidance with respect to state law, but that has limited reach. *See, e.g.*, HARRIS, *supra* note 46.

349. *See* William S. Jordan, III, *Ossification Revisited: Does Arbitrary and Capricious Review Significantly Interfere with Agency Ability to Achieve Regulatory Goals Through Informal Rulemaking?*, 94 NW. U. L. REV. 393, 394 (2000).

350. Solove & Hartzog, *supra* note 14, at 620. In his comprehensive analysis of the history and development of the FTC, Chris Hoofnagle notes that after several years of rulemaking authority, the Federal Trade Commission Improvement Act of 1980 placed additional procedural hurdles in the FTC's rule-making powers. *See* HOOFNAGLE, *supra* note 14, at 65. For example, the Act introduced direct Congressional oversight. *Id.* And the law explicitly prohibited the FTC from using funds for three years "for the purpose of initiating any new rulemaking proceeding . . . which prohibits or otherwise regulates any commercial advertising." *Id.* (citing Pub. L. No. 96-252, 94 Stat. 474 (1980)). The Act did much "political and psychological damage to the Agency." *Id.* at 65. Notably, the FTC does have general rulemaking authority under the Children's Online Privacy Protection Act and the Gramm-Leach-Bliley Act. *See A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority* at app. C, FED. TRADE COMM'N (July 2008), http://www.ftc.gov/about-ftc/what-we-do/enfor cement-authority [perma.cc/9724-ZWF2] ("Special Statutes that mandate or authorize Commission rulemakings either antitrust and/or consumer protection related . . . include the Gramm-Leach-Bliley Act . . . [and] COPPA . . . .").

351. FED. TRADE COMM'N, RULEMAKING: OPERATING MANUAL, CHAPTER SEVEN, http://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf [perma.cc/GGM7-6LWP] (describing rulemaking procedures).

352. *See* Solove & Hartzog, *supra* note 14, at 620 n.176.

is what many practitioners do.[353] But that common law analysis cannot achieve the level of clarity rulemaking can. If applied to Section 5 of the FTC Act, which only prohibits "unfair and deceptive" practices, and any other privacy statute, rulemaking could cut legal endogeneity off at the knees, limiting the ability of people on the ground to managerialize vague statutory terms.

C. Changes at the FTC

The FTC should not accept the mere presence of symbolic structures as evidence of compliance with the law.[354] Deference to toothless internal structures is based on a neoliberal legal consciousness; regulators are primed to associate compliance structures with actual adherence to the substantive requirements of the law. As Edelman noted in the workplace discrimination context, the mere presence of these structures "creates an illusion of fairness" where none actually exists.[355] The remedy for that is simple: Stop being fooled by the illusion. This Article has diagnosed the problem, so we can hope that regulators, with the political will and when given sufficient financial resources,[356] will be more attuned to the ways in which corporations erect structures that comply with the law in name only.

On a more granular level, FTC assessments must be more effective; they must be intensive, independent third-party audits. Securities regulation may provide a starting point. Among many other changes, the Sarbanes-Oxley Act of 2002, as clarified by rules promulgated by the Securities and Exchange Commission, requires publicly traded companies to have a completely independent audit committee.[357] The committee serves as a check on nefarious financial reporting and is charged with the "appointment, compensation, and oversight" of the company's independent

353. *Id.* at 585 ("Those involved with helping businesses comply with privacy law—from chief privacy officers to inside counsel to outside counsel—parse and analyze the FTC's settlement agreements, reports, and activities as if they were pronouncements by the Chairman of the Federal Reserve.").

354. For the purposes of this Article, I am assuming that the FTC will remain the U.S. privacy regulator. That said, the FTC is structurally unfit to adequately protect our privacy. *See* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 887–88 (2003) (arguing that the FTC is not well situated to protect privacy because of its market-oriented mission).

355. *See* EDELMAN, *supra* note 18, at 219.

356. *See* McGeveran, *supra* note 10, at 1017–18 (discussing the lack of resources U.S. regulators bring to the privacy space now).

357. *See* Sarbanes-Oxley Act of 2002 § 301, 15 U.S.C. § 78j-1 (Supp. III 2003), Pub. L. 107-204, 116 Stat. 745, 776 (2002); SEC Listing Standards Relating to Audit Committees, 17 C.F.R. § 240.10A-3 (2005); SEC Standards Relating to Listed Company Audit Committees, 68 Fed. Reg. 18788 (Apr. 16, 2003) (to be codified at 17 C.F.R. pts. 228-29, 240, 249, 274). "Independent" means not being affiliated with the company other than as a director or receiving any compensation other than for serving as a director. *See* Sarbanes-Oxley Act § 301.

auditor.[358] The committee must include at least one financial expert and have a mechanism for anonymously reporting questionable accounting.[359] Sarbanes-Oxley made internal auditing teams cornerstones of business models: long seen as simple cost centers, audit teams are now essential to corporate governance and legal compliance.[360] Sarbanes-Oxley also requires executives to sign financial statements, ensuring greater involvement and establishing a sense of personal responsibility for honesty.[361]

A similar approach could both invigorate FTC-mandated audits and empower a company's internal privacy team, many of which are seen as cost centers, as well.[362] As discussed earlier, many companies subject to FTC consent decrees fulfill their audit requirements with assessments or attestations, without any deep, independent investigation. Sarbanes-Oxley-style rules governing both audit committees and independent audits themselves would both ensure greater adherence to the law and prevent the managerialization of privacy audits. Requiring executives to sign off on privacy audits and internal privacy programs, and subjecting them to civil and criminal penalties should they mislead regulators, could also have a sufficient motivating effect to take privacy seriously. The FTC's 2019 settlement with Facebook adopts this last suggestion.[363]

That said, it is not clear that an internal auditing system will be sufficient. Auditing-based models like the one in Sarbanes-Oxley are part of the privatization of regulation criticized above.[364] And, as Julie Cohen has argued, they "sit on the periphery of the regulatory state," having the look and feel of administrative oversight, but with too unhealthy a dose of private control.[365]

D. Empowering Individuals

Even an invigorated, aggressive FTC cannot do this alone. At most, the FTC averages ten privacy-related settlements per year.[366] The Commission's portfolio extends beyond privacy issues, covering many

358. *See* Sarbanes-Oxley Act § 301.
359. *Id.* §§ 301, 407.
360. *See* Craig Clay, *Sarbanes-Oxley: 15 Years of Successes and Challenges*, ACCT. TODAY (Sept. 15, 2017, 4:31 PM), https://www.accountingtoday.com/opinion/sarbanes-oxley-marks-15-years-of-successes-and-challenges [https://perma.cc/3MCJ-F7LE].
361. *See* Sarbanes-Oxley Act § 302; 17 C.F.R. § 228.
362. *See* IAPP & TRUSTARC, MEASURING PRIVACY OPERATIONS 10 (2018), https://iapp.org/media/pdf/resource_center/IAPP-Measuring-Privacy-Operations-FINAL.pdf [https://perma.cc/QL29-U66J] (noting many privacy departments are seen as cost centers).
363. *See* Facebook Stipulated Order, *supra* note 287.
364. *See supra* Part B.3-B.5.
365. *See* COHEN, *supra* note 17, at 192–93.
366. *See* Solove & Hartzog, *supra* note 14, at 600.

"unfair and deceptive" practices in commerce.[367] And FTC settlements offer corporations an entry point for institutionalizing and validating their merely symbolic compliance structures.

Therefore, any new privacy law must include a private right of action. Although judicial proceedings are not immune to the endogeneity cycle—indeed, reference, relevance, and deference are judicial contributions to the problem—giving individuals the opportunity to realize their rights in court has worked in the past. Civil litigation made dangerous machines safer;[368] private lawsuits gave us seatbelts,[369] stronger automobile frames,[370] safer doors,[371] side impact protection,[372] and many other car safety features.[373] Little if any of that would have happened if car safety was the exclusive responsibility of a small, underfunded regulatory agency that has acceded to a self-governing privacy regime.

Private rights of action can protect privacy laws against the cycle of legal endogeneity by forcing organizations to take privacy more seriously than they do now. As we have seen, some corporations frame privacy law compliance around minimizing the risk of litigation.[374] Because they do so in a legal environment where federal standing requirements[375] and narrowly drafted laws[376] have made it difficult to bring claims except in a few circumstances, the risk of a lawsuit is low. Low risk means investing in privacy from the ground up brings little in return, thus contributing to crumbling privacy infrastructures. And although privacy professionals and privacy lawyers are rightly wary of European regulators empowered by the GDPR, European data protection regulators cannot effectively monitor the global landscape of data collection.[377]

Admittedly, private rights of action are not panacean levers of reform. Opening the door to impact civil litigation could mean very little without

367. 15 U.S.C. § 45(a)(4)(B) (West 2019).

368. *See, e.g.*, Grimshaw v. Ford Motor Co., 174 Cal. Rptr. 348, 376–80 (Cal. Ct. App. 1981) (Ford Pinto case).

369. *See, e.g.*, AlliedSignal, Inc. v. Moran, 231 S.W.3d 16, 28 (Tex. App. 2007).

370. *See, e.g.*, Dyson v. Gen. Motors Corp., 298 F. Supp. 1064, 1074 (E.D. Pa. 1969).

371. *See, e.g.*, Seliner v. Ford Motor Co., No. 2002-30454, 2004 WL 5014479 (Tex. Dist. Ct. Aug. 9, 2004).

372. *See, e.g.*, Dawson v. Chrysler Corp., 630 F.2d 950, 958 (3d Cir. 1980).

373. *See* AM. ASS'N FOR JUSTICE, DRIVEN TO SAFETY: HOW LITIGATION SPURRED AUTO SAFETY INNOVATIONS 4–11 (2010).

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

375. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (holding that a violation of the Fair Credit Reporting Act, "divorced from any concrete harm," does not satisfy Article III standing requirements).

376. Most privacy laws do not include private rights of action. Fifteen state data breach notification statutes do, however. Stephen Embry, *State Data Breach Notification Laws Just Got Crazier*, A.B.A. (Apr. 19, 2016), https://www.americanbar.org/publications/youraba/2016/may-2016/state-data-breach-notification-laws-just-got-crazier.html.

377. *See* McGeveran, *supra* note 10.

concomitant liberality from judges in recognizing privacy harms, especially where judges demand a laser precise causal chain between privacy breach and some concrete pecuniary injury.[378] Despite some progress in this area, judicial reliance on concreteness and financial loss is sticky in part because it fits both judges' perceptions of their own institutional competence and a narrative that industry has been pushing for years.[379] After all, litigation can favorably tilt toward wealthy, entrenched interests that have the power, money, and time to litigate not just for individual wins—in which case, settlements may make rational sense—but for structural advantage in precedent, governing law, and legal consciousness.[380] That said, a private right of action is one of several weapons needed to change the status quo. It can "catalyz[e] a societal shift toward a thicker notion of industrial responsibility," as it did with mass environmental torts and products liability.[381] And in a world where our regulatory agencies have taken a step back from the kind of robust, industry-wide rules necessary to keep individuals safe, the courts can nudge the kind of structural change we sorely need.

E. Compliance Professionals

Privacy lawyers and compliance professionals are a diverse group of committed leaders, many of whom chose their professions because they believe in consumer privacy, not because they wanted to undermine it in the name of corporate profits. Many of these professionals, however, are torn between their privacy advocacy and the need to influence policy with a seat at the table or the ear of the executive.[382] Standing in the way of corporate profits by saying "no" too often or rejecting profitable products for privacy reasons can erode trust with executives, damage their ability to get things done, or get them fired and replaced by someone more pliant.[383] Many privacy professionals I interviewed echoed these concerns. For example, a

378. *See* Solove & Citron, *supra* note 247, at 755.

379. *See* Julie E. Cohen, *Information Privacy Litigation as a Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 555 (2017) ("[S]trictness toward information privacy claims align with the interests of powerful information businesses that are repeat players in the litigation system. But debates about injury-in-fact in the information economy do not simply reflect a banal story of interest group capture. Rather, they hint at a more complex process involving both deep capture and institutional path-dependence. Deep capture—or capture at the level of ideology—proceeds as well-resourced repeat players work to craft compelling narratives about the contours of legal entitlements and the structure of legal institutions.").

380. *See* Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 LAW & SOC'Y REV. 95 (1974).

381. Cohen, *supra* note 379, at 574.

382. *See* Nelson & Nielsen, *supra* note 157, at 447.

383. *Id.* at 446–48.

former chief privacy officer based in Chicago found the problem of symbolic structures "intriguing" but wondered:

> What else are we supposed to do. We really serve two masters: the regulators and our bosses. If I go too far with the chief executive, he could just as easily ignore me and sideline my office from important decisions. Earning their trust is important, and you can't do that if you don't have the company's interests in mind.[384]

I am sensitive to these practical concerns, which make the social practice of privacy law far more complicated than writing laws in state capitols or in Congress. That said, the privacy professionals and lawyers I interviewed thought certain changes made sense. Several privacy leads thought "clearer guidance from the FTC or from Congress" with "specific statements on what is required" would be welcome because, as one current CPO noted, "then I can go to the executive team and say, 'look, we *have* to do this.' That makes it so much easier for me to do real privacy advocacy inside the company."[385] Others also said that more resources, moving privacy out of the compliance portfolio, and elevating the CPO to a board-level position would help get the message across.

Scholars have argued that the best way to ensure privacy becomes part of the ethos of a company is to have distributed privacy responsibilities through different business units.[386] That is an important first step, but it does not address the problem of merely symbolic privacy structures. Business unit leaders should not just have local responsibility for integrating privacy into their work; they should also be held responsible for substantive results. That is, it is one thing to task a business-line executive with developing specific privacy practices or completing a privacy impact assessment. As this Article has shown, executives can take that responsibility and supervise the creation of a house of cards of privacy structures. A more powerful approach would be to evaluate subordinates for their substantive privacy progress—namely, whether a new product collects the least amount of data necessary, limits data collection for a single purpose, includes designs that make it easy for users to exercise their rights, eliminates dark patterns, protects the unique privacy needs of marginalized populations, and so forth. Achieving some of these goals may have been the purpose of deploying a PIA in the first place, but shifting the metric of evaluation of a privacy

384. Interview with former chief privacy officer, in San Diego, Cal. (Oct. 17, 2017) (notes on file with author).

385. Interview with chief privacy officer, in Washington, D.C. (Oct. 4, 2018) (notes on file with Author).

386. *See* BAMBERGER & MULLIGAN, *supra* note 23, at 83–86.

program from a structure to substance would stop legal endogeneity in its tracks.

CONCLUSION

Privacy law is at risk. As this Article has attempted to show, it is undergoing a process of what Lauren Edelman called legal endogeneity, whereby systems that have the veneer of legality—paper trails, assessments and audits, internal and external policies, to name just a few—take the place of actual adherence to the law. And when these merely symbolic structures proliferate, they undermine the substantive power of the law and shift the discourse of power, all to the detriment of consumer privacy.

It is important to note what this Article is not arguing. It does not argue that all compliance professionals are part of the problem. Nor does it argue that they alone are responsible for undermining the promise of privacy law. Rather, the impact of corporate compliance structures is both significant and underexplored. This Article has endeavored to fill a gap in the legal, sociological, and interdisciplinary privacy literatures by describing a narrative that has gone mostly unnoticed in the practice and study of privacy law.

But more work needs to be done. Future research will explore the role of privacy technology vendors within an ecosystem of social forces influencing the implementation of privacy law on the ground. Another project will explore the engineerization of automated decision-making. And additional research is necessary on responses to the problem of legal endogeneity, including ongoing work on privacy education for engineers and licensing requirements for those designing software tools. More broadly, the growing impact of symbolic compliance reminds scholars that the social practice of law, the way real people tasked with implementing the law filter legal requirements for society, requires significantly more scholarly attention. Identifying the erosion of privacy law is a first step. Even harder work comes next.