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 why.

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 in part because the responsibility for fulfilling legal obligations is being outsourced to engineers at third-party technology vendors who see privacy law through a corporate, rather than substantive, lens. This phenomenon is placing privacy law in the middle of a process of what scholars have called 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.

---

* Professor of Law and Director, Innovation Center for Law and Technology, New York Law School. PhD, Columbia University; J.D., Harvard Law School. This 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, Celine Castets-Renard, Danielle Keats Citron, Rebecca Crootoff, Lauren Edelman, Nikolas Guggenberger, Woodrow Hartzog, Joris van Hoboken, Chris J. Hoofnagle, Thomas Kadri, Mike Kwet, Karen Levy, Mason Marks, James A. Mourey, Frank Munger, Przemyslaw Palka, Ed Purcell, Joel Reidenberg, Neil Richards, Paul Schwartz, Eli Seims, Jake Sherkow, Richard Sherwin, Liron Shilo, Priscilla Smith, Kathy Strandburg, and Olivier Sylvain. 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. I do not outsource my responsibility for any errors.

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 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

---

[1] *See* John Constine, *Facebook Admits Cambridge Analytica Hijacked Data on Up to 87M Users*, TECHCRUNCH (Apr. 4, 2018), https://techcrunch.com/2018/04/04/cambridge-analytica-87-million/.

[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/.

[3] *See* Die-Cast 2-Slice Smart Toaster, https://www.breville.com/us/en/products/toasters/bta820.html (last visited Aug. 23, 2018).

[4] *See* Electric Toothbrushes with Bluetooth Connectivity, https://oralb.com/en-us/products/compare/bluetooth (last visited Aug. 23, 2018).

[5] *See* Cory Doctorow, *The Internet of Connected Sex Toys is Every Bit as Horrifyingly Insecure and Poorly Thought Out as You Imagine*, BOINGBOING.NET (Feb. 2, 2018 9:28 AM), https://boingboing.net/2018/02/02/sarah-jamie-lewis.html. *See also* The Internet of Dongs Project, https://internetofdon.gs/ (last visited Aug. 23, 2018).

[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.

[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; Taylor Hatmaker, *In 2006, Harvard Also Conducted a Facebook Study that Went Too Far*, THE DAILY DOT (July 12, 2014 6:55 AM), https://www.dailydot.com/debug/facebook-t3-study-tastes-ties-time/.

[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, 2018 O.J. L 119 [hereinafter, GDPR].

called "comprehensive"[10] and "one of the strictest privacy laws in the world."[11] California's Consumer Privacy Act (CCPA)[12] goes even further.[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 reclaimed the Fourth Amendment's historical commitment to curtail pervasive police surveillance by requiring warrants for cell-site location data.[15] And the E.U. 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 responsibility for fulfilling legal obligations is being outsourced to engineers who see privacy law through a corporate, rather than

---

[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/.

[12] *See* Cal. Civ. Code § 1798.100 (West 2018).

[13] *See* Lydia De la Torre, *GDPR Matchup: The California Consumer Privacy Act of 2018*, IAPP PRIVACY TRACKER (Jul 31, 2018), https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/ (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.

[14] *See* CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016) (describing the origins and multiple ways the FTC protects the privacy of US consumers); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (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. U.S., 138 S. Ct. 2206 (2018) (requiring government to obtain a warrant before acquiring cell-site location data). *See also* Riley v. California, 134 S. Ct. 2473 (2014) (declaring warrantless search of arrestee's cell phone unconstitutional); U.S. v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) ("longer term GPS monitoring … impinges on expectations of privacy").

[16] *See* Case C-362/14, Maximillian Schrems v. Data Protection Commissioner [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).

substantive, lens.[17] This Article provides the first picture of this growing privacy outsourcing market. Based on original primary source research into the ecosystem of privacy compliance, I argue that because compliance is being outsourced to third-party technology vendors that instantiate their own vision of the law into their services, privacy law is in the middle of 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 ambiguously worded legal requirements allow compliance professionals on the ground 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, mistaking mere symbols of compliance with adherence with 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—can 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

---

[17] Outsourcing can reduce economic welfare, *see, e.g.*, Jakob Roland Munch & Jan Rose Skaksen, *Specialization, Outsourcing, and Wage*, 145 REV. WORLD ECON. 57 (2009) (finding that foreign outsourcing harms domestic workers), while it reduces costs. But there is a qualitative difference between outsourcing services like cloud technologies and custodial or catering staff, on the one hand, and outsourcing legal interpretations, on the other. Indeed, such outsourcing reduces privacy law to what corporations want, not what consumers need, and constitutes a critical flaw in the edifice of privacy protection.

[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.

[21] *Id*. at 12-13.

diversity offices that compliance professionals created on the ground.[22] The problem is far more pervasive than even Edelman suggested.

In this Article, I present original research showing that privacy standards are being coopted 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. 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 inside technology companies[24] play in implementing privacy law. But they are not alone.[25] Among the many stakeholders involved are the nearly 200 technology vendors who instantiate their own interpretations of privacy law into the designs of automated tools, often marketing themselves as one-stop compliance shops. These vendors "managerialize" privacy law, shifting the site at which the law is interpreted and negotiated away from experts and toward engineers and technology salespersons. They become the locus of legal decision making, think about privacy in managerial terms, and often create symbolic structures of compliance—from toothless privacy offices 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.

If left unabated, this outsourcing of privacy law to vendors and consultants will have profound and troubling implications for privacy law,

---

[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 HOUSTON 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. *See* Trevor J. Pinch & Weibe E. Bijker, *The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit from Each Other*, in THE SOCIAL CONSTRUCTION OF TECHNOLOGICAL SYSTEMS (Wiebe Bijker et al. eds. 1987) (describing the author's social construction of technology, or SCOT, model).

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[26] or actually incorporating them into statutes, thereby undermining the capacity for law to achieve more robust privacy protections for users.[27] We already see this happening in the privacy space, as when the FTC includes auditing requirements in its consent decrees but fails to ensure their rigor or when the GDPR requires data collectors to hire privacy officers, but fails to ensure their empowerment. 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, judges, and lawyers, and toward engineers, the substantive and procedural protections of due process may dissipate.[28]

Outsourcing privacy law compliance to engineers can further erode traditional paradigms of expertise,[29] including those taught in law school, that ensure social and pro-consumer values at least have a seat at the table in practice. At a time when social values and respect for expertise is under attack, in general, narrow, compliance-oriented approaches to privacy offered by third-party consultants and vendors threaten to undermine another pillar of democratic society.[30] All of this may also have an

---

[26] *See* Ian Kerr & Carissima Mathen, *Chief Justice John Roberst is a Robot*, Paper Presentation, WeRobot 2014, University of Miami School of Law, *available at* http://robots.law.miami.edu/2014/wp-content/uploads/2013/06/Chief-Justice-John-Roberts-is-a-Robot-March-13-.pdf (discussing the difference between mere compliance and actual adherence to the law).

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

[28] *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 agency decision-making).

[29] *See* Gil Eyal, *For a Sociology of Expertise: The Social Origins of the Autism Epidemic*, 118 AM. J. SOC. 863 (2013) (developing the field of the sociology of expertise in contrast to the limited theoretical window of the sociology of professions).

[30] Today, the erosion of respect for expertise is most notably affecting the press and science. *See generally, e.g.*, TOM NICHOLS, THE DEATH OF EXPERTISE: THE CAMPAIGN AGAINST ESTABLISHED KNOWLEDGE AND WHY IT MATTERS (2017) ("Americans have reached a point where ignorance, especially of anything related to public policy, is an actual virtue. To reject the advice of experts is to assert autonomy, a way for Americans to insulate their increasingly fragile egos from ever being told they're wrong about anything."); *see also*

asymmetrical impact on the technology industry. Wealthy companies that can afford both in-house and outsourced privacy expertise will take advantage of their market power to frame the law in ways that benefit them, erect barriers in front of competitors and small firms, and ignore the needs and preferences of users.

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 technology vendors to play, but outsourced engineering talent deciding what the law requires of their clients is not one of them. Rather, vendors can help their clients by providing the kind of information companies need to follow the law, leaving the work of legal compliance to the experts. All levels of the consumer privacy ecosystem—from lawmakers to civil society to academics—can aid in this effort. Crafting a space for vendors that advances both corporate and consumer interests will require understanding how we got here, how consultants and technology vendors can do better, and how the social process of law can honestly translate privacy's laws on the books to real privacy protections on the ground. These are the goals of this Article.

Part I situates privacy technology vendors in the ecosystem of the social practice of privacy law, alongside lawyers, regulators, state attorneys-general, CPOs, and in-house engineers, and recognizes that privacy laws are neither written nor implemented in vacuums and are subject to influences from those responsible for compliance on the ground. Part II describes the narrative of legal endogeneity and argues that some privacy technology vendors are undermining 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. Notably, this part does not argue that technology vendors alone are responsible for legal endogeneity in privacy law. Indeed, that is a

---

Vidya Narayanan et al., *Polarization, Partisanship and Junk News Consumption over Social Media in the US*, COMPROP DATA MEMO (Feb. 6, 2018), *available at* http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/02/Polarization-Partisanship-JunkNews.pdf.

collective effort that requires explication beyond the scope of this Article.[31] Rather, I demonstrate for the first time how this relatively new and growing market of vendors is uniquely and forcefully contributing to the problem. Finally, Part III addresses the dangers of legal endogeneity head on, identifying ways in which technology vendors can actually support substantive, pro-consumer privacy law and recommending changes to law and the social practice of privacy law. 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 this third-party vendor market is so new and unexplored, 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 IAPP national conference, "Privacy. Security. Risk. 2017"; the 2018 International Privacy+Security Forum and 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.[32] 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 privacy space. I reviewed their marketing literature and products and services online. Along with a small team of research assistants, I used LinkedIn Premium services to identify employees by company. I distributed a survey to representatives from all identified vendors to elicit themes in their conceptualization of privacy and their responsibilities to their clients, and supplemented that survey with interviews with representatives from five companies. These five companies were not meant to represent a random sample. 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

---

[31] This is the subject of an untitled book project, accepted for publication by Cambridge University Press.

[32] The author was invited to speak at the IAPP conference, the ESMT Annual Forum, and CyberWeek 2018.

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, how they conceptualized their responsibilities and goals, and to minimize response biases from surveys,[33] I participated in webinars hosted by vendor 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.[34] 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.[35] Undoubtedly essential, this fertile research agenda is also incomplete. Insufficient attention has been paid to the social

---

[33] 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, or 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. PSYCH. 263 (1985) (collecting the literature).

[34] This series of interviews included those conducted for a related research project. *See* Waldman, *Designing Without Privacy*, *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*, 17 HUMAN ORG. 28, 28–29 (1958–1959) (discussing methodologies).

[35] For example, Orin Kerr has studied the Fourth Amendment in a long research agenda too voluminous to cite here. *See, e.g.*, Orin Kerr, *Cross-Enforcement of the Fourth Amendment*, 132 HARV. L. REV. __ (forthcoming 2019); Orin Kerr, *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 U.C.L.A. L. REV. 1149 (2005). So has Margot Kaminski. *See, e.g.*, Margot Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167 (2017); Margot Kaminski, *Siri-Ously 2.0: What Artificial Intelligence Reveals about the First Amendment*, 101 MINN. L. REV. 2481 (2017).

structures on the ground—the people, professional organizations, and corporations—that not only turn that 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.[36] It didn't 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.[37] 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.[38]

Danielle Citron has explored the agile privacy work of state attorneys-general (AGs), long active but overlooked privacy enforcers.[39] 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.[40] They were also less constrained by the politics that can paralyze federal agencies.[41] As a result, state AGs have become the "front

---

[36] *See* 15 U.S.C. § 45(a)(1) ("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). *See* 15 U.S.C. § 45(a)(2). *See also* Solove & Hartzog, *supra* note 14, at 599-600; HOOFNAGLE, *supra* note 14, at 119-23.

[37] Fed. Trade Comm'n, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress 1-3 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[38] *See* Solove & Hartzog, *supra* note 14, at 607.

[39] *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747 (2017) (showing how state attorneys general can be more effective than federal regulators at privacy enforcement, but also face certain hurdles and employ ineffective policies).

[40] *Id*. at 786-95.

[41] *Id*. at 750, 786.

line of privacy enforcement:"[42] in 2017, for example, state AGs, alone or in concert, reached settlements on data breach and privacy claims with Target,[43] Lenovo,[44] Hilton,[45] Vizio,[46] and a handful of other corporations, and initiated actions against Equifax.[47]

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.[48] And *Making Your Privacy Practices Public* takes the vague requirement in the California Online Privacy Protection Act (CalOPPA) that privacy policies should be "conspicuous"[49] and translates that into specific recommendations on readability and design.[50] The Texas AG's office took generalized language in the Children's Online Privacy

---

[42] *Id*. at 749.

[43] Assurance of Voluntary Compliance, In the Matter of Investigation by Eric T. Schneiderman, Attorney General of the State of New York, of Target Corporation, No. 17-094 (May 15, 2017), available at https://ag.ny.gov/sites/default/files/nyag_target_settlement.pdf.

[44] Press Release, Attorney General Becerra Announces $3.5M Settlement with Lenovo for Preinstalling Software that Compromised Security of its Computers (Sept. 5, 2017), *available at* https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-35m-settlement-lenovo-preinstalling-software.

[45] Press Release, A.G. Schneiderman Announces $700,000 Joint Settlement With Hilton After Data Breach Exposed Hundreds of Thousands of Credit Card Numbers (Oct. 31, 2017), *available at* https://ag.ny.gov/press-release/ag-schneiderman-announces-700000-joint-settlement-hilton-after-data-breach-exposed.

[46] Stipulated Order for Permanent Injunction and Monetary Judgment, *Federal Trade Commission, et al. v. Vizio, Inc*., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), *available at* http://nj.gov/oag/newsreleases17/Vizio-Order.pdf.

[47] 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., Consumer Data Security Breach Litigation* , MDL Dkt. No. 2800 (Judicial panel on Multi-district Litigation, Sept. 11, 2017), *available at*: http://www.almcms.com/contrib/content/uploads/sites/292/2017/09/Equifax-MDL-motion.pdf.

[48] 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; Citron, *supra* note 39, at 760.

[49] Cal. Bus. & Prof. Code § 22575(a).

[50] *See* 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

Protection Act and concluded that collecting location data from anyone under thirteen violated the law.[51] 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.[52] State AGs may not have written the privacy laws,[53] but as Citron showed, they infuse the law with pro-consumer values and play a critical role in their construction and practical implementation.

Kenneth Bamberger and Deirdre Mulligan then studied how chief privacy officers (CPOs) also fill gaps left open by privacy law.[54] Through a series of interviews with privacy professionals recognized as leaders in their fields,[55] Bamberger and Mulligan concluded that CPOs saw their companies' responsibilities as more than just compliance; rather, legal rules provided a floor.[56] Several American CPOs talked about their jobs in fiduciary terms: they were "steward[s]" of data and "responsibl[e]" to consumers.[57] In short, some CPOs saw their primary objective as creating and maintaining "the company's trusted relationship" with customers, employees, and society.[58] 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 10 years.[59] Today, 47,164 people on LinkedIn list "chief privacy officer," "deputy chief privacy officer," or other upper- or middle-management level privacy position as their current employment.[60]

---

[51] Citron, *supra* note 39, at 780.

[52] *Id*. at 759 n. 60, 774.

[53] 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. *See id*. at 758-59. *See also* Colin Provost, *State Attorneys General, Entrepreneurship, and Consumer Protection in the New Federalism*, 33 PUBLIUS: J. FEDERALISM 37, 39 (2003) (discussing the legislative role of attorneys general).

[54] *See* BAMBERGER & MULLIGAN, *supra* note 23; Bamberger & Mulligan, *supra* note 23.

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

[56] *Id*. at 60, 64.

[57] *Id*. at 66.

[58] *Id*. at 67.

[59] *See id*. at 261.

[60] Based on a LinkedIn Premium Advanced Search filtered by "job titles" using the search terms "chief privacy officer" [hereinafter, LinkedIn Survey]. 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.

B. Shifting Privacy Responsibilities

All of these social groups – FTC commissioners, state AGs, and CPOs—share one essential quality: they are steeped in the law.[61] Lawyers are at least trained in the rule of law. Lawyers learn to interpret statutes in line with legislative objectives and to translate legislative or regulatory actions into practice. Lawyers generally understand the importance of due process, transparency, and explanation.[62] Of course, lawyers do not always operate with fidelity to justice,[63] but they offer institutional competencies in legal interpretation and compliance that other professions do not.

But, in reality, many legal decisions are made by nonlawyers. Kate Klonick has shown that armies of online content moderators negotiate free speech law.[64] Online platforms do the same for fair use determinations in copyright law.[65] We outsource constitutional responsibilities to police officers, who make practical interpretations of search and seizure law in the moment.[66] Catherine Crump argues that surveillance policy is made by

---

[61] 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, https://www.ftc.gov/about-ftc/biographies/former-commissioners (last visited Sept. 26, 2018). And although CPOs do not always have to have J.D. degrees, the IAPP recently found that 6 in 10 privacy professionals at large firms have law degrees. *See* IAPP, FULL REPORT: BENCHMARKING PRIVACY MANAGEMENT AND INVESTMENTS OF THE FORTUNE 1000 [hereinafter, IAPP BENCHMARKING SURVEY], at 10, https://iapp.org/media/pdf/resource_center/2014_Benchmarking_Report.pdf.

[62] *See* Citron, *supra* note 28, at 1254-1255 (noting that human deliberation in federal agency decision-making adds respect for process and transparency).

[63] *See, e.g.*, Jonathan K. Van Patten, *Lawyer Advertising, Professional Ethics, and the* Constitution, 40 S.D. L. REV. 212, 212 (1995) ("Lawyers are said to be greedy, dishonest, disruptive, manipulative, arrogant, abusive, obnoxious, obstructive, uncaring, unscrupulous, … . In short, they act without principle."). *See also* MONROE H. FREEDMAN, UNDERSTANDING LAWYERS' ETHICS 109-10, 119 (1990) (criticizing the unscrupulous lawyer Roy Cohn); Brett Samuels, *Michael Cohen Pleads Guilty to 8 Counts*, THE HILL (Aug. 21, 2018 4:54 PM), https://thehill.com/regulation/administration/402906-cohen-pleads-guilty-to-federal-charges.

[64] *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).

[65] *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).

[66] *See* GREGORY H. 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) ("[P]olice interpretation of the law helps operationalize its legal authority, and to that

vendors hired by the government.[67] And we are increasingly outsourcing judicial decision-making to mediators and arbitrators who hear evidence, consider legal arguments, and issue binding orders.[68]

Nor are privacy decisions on the ground always made by lawyers. Elsewhere, I explored how engineers employed by technology companies instantiate a particular vision of privacy law in the products they create.[69] Because of the networks they sit in and their proximity to the design process,[70] engineers have outsized 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.[71] Where privacy professionals created company-wide protocols and trainings to help integrate privacy into design, many engineers make privacy decisions ad hoc and often prioritize efficiency,

---

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… .").

[67] *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).

[68] *See, e.g.*, CHARLES GARDNER GEYH, COURTING PERIL: THE POLITICAL TRANSFORMATION OF THE AMERICAN JUDICIARY 16-43 (2015); 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).

[69] *See* Waldman, *Designing Without Privacy*, *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).

[70] This argument reflects actor-network theory (ANT), developed by the science and technology studies scholars Michel Callon and Bruno Latour. 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: Toward an Actor-Network Theory of Design*, 1 DESIGN & CULTURE 273 (2009). *But see* Susan Leigh Star, *Power, Technology and the Phenomenon of Conventions*, *in* TECHNOSCIENCE: THE POLITICS OF INTERVENTIONS 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).

[71] *See* Waldman, *Designing Without Privacy*, *supra* note 24, at 681-85.

speed, and other engineering values over privacy.[72] 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.[73] This means that in some cases, privacy law, generally, privacy by design, in particular,[74] and the visions of earnest and hardworking privacy professionals are not being fully realized; the engineers whose job it was to translate internal privacy rules into design had 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 lawyers to engineers. As Citron has argued, automating the law through technological filters can undermine substantive and procedural safeguards, replace transparent procedures with opaque algorithms, and short circuit deliberative decision-making with quick computer-generated answers.[75] There is even a greater risk, one which this Article explores: the automation of privacy law compliance to engineers at third-party vendors is threatening to replace real pro-consumer progress with mere symbols of compliance, undermining the promise of pro-privacy laws.

II. Undermining Privacy Law

---

[72] *Id*. at 685-89, 711-16.

[73] *Id*. at 716-25.

[74] 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 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, at Recital 46. *See also* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE SEVEN FOUNDATIONAL PRINCIPLES (2009), http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf. It has more recently received more systematic scholarly attention. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018).; HELEN NISSENBAUM & MARY FLANAGAN, VALUES AT PLAY IN DIGITAL GAMES (2014); Katie Shilton, *Technology Development with an Agenda: Interventions to Emphasize Values in Design*, in Proceedings of the Annual Meeting of the Am. Soc. for Info. Sci. & Tech. (2010); BATYA FRIEDMAN, HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY (1997) (challenging the idea that efficiency and functionality are the central foci of design and showing how values are integrated into new products).

[75] *See* Citron, *supra* note 28, at 1254-1255.

FTC commissioners, AG offices, corporate CPOs, and the engineers on the ground have an impact on the framing of privacy law. But the center of gravity is shifting even more. Privacy law is being defined, negotiated, and practiced by an army of third-party vendors. Many of them are coding their version of privacy law into the designs of tools they claim will help data collectors comply with privacy law's many mandates. And, crucially, some outsourced providers 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.[76]

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 third-party vendors undermines that commitment. Second, many consultants and technology create symbolic structures of compliance that often—though certainly not always—ossify into compliance in name only. Third, this emerging legal endogeneity has the effect of entrenching the power of large corporations, frustrating the integration of privacy into design, undermining the capacity of privacy law to achieve its substantive goals, and damaging the rule of law, in general. 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.

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 on 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 protected categories persist[ed]."[77] 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

---

[76] *See* EDELMAN, *supra* note 18, at 12, 14.

[77] *Id*. at 6-10 (providing statistical evidence for ongoing racial and gender inequality in the workplace).

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.[78]

Sometimes, these structures have important expressive effects:[79] a policy of nondiscrimination is a first step toward embedding nondiscrimination in the ethos of a company.[80] 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.[81] 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.[82]

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] *Id*. at 11, 153-96.

[79] *See, e.g.*, Danielle Keats Citron, *Law's Expressive Value in Combatting Cyber Gender Harassment*, 108 MICH. L. REV. 373 (2009) (discussing how the law is necessary for persuading individuals, platforms, and the law to take seriously that cyberharassment 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).

[80] 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. Then, routines are "performed" by workers on the ground: real people doing real work translating the mission into action, products, and widgets. *See* Martha S. Feldman & Brian T. Pentland, *Reconceptualizing Organizational Routines as a Source of Flexibility and Change*, 48 ADMIN. SCI. Q. 94, 95– 96 (2003). *See also* Bruno Latour, *The Powers of Association*, 32 SOC. REV. 264, 266–68, 271–73 (1984).

[81] *See* EDELMAN, *supra* note 18, at 14.

[82] *See id*. at 168-73.

legal profession, to name just a few.[83] 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.[84] 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.[85] 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. The process starts when a legislature passes a law with ambiguous or vague requirements.[86] 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."[87] 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,[88] but regardless of their origin, they leave the door open to wildly different interpretations from those responsible for compliance on the ground.[89]

---

[83] *Id*. at 21.

[84] *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/ (providing examples of industry players moving into policymaking roles).

[85] *See* EDELMAN, *supra* note 18, at 170-71.

[86] 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).

[87] 42 U.S.C. § 2000e et. seq. (as amended).

[88] *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 (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).

[89] *See* EDELMAN, *supra* note 18, at 42-55 (discussing ambiguity in Title VII and related laws).

Legislative ambiguity gives corporate professionals—lawyers, consultants, and compliance experts, for example—the chance to define what the law means. 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.[90] And they use the leeway they were given by ambiguous law to conclude that their goal is to minimize the risk of litigation for their employer, not actually eliminate bias, discrimination, and inequality.[91]

These professionals then develop compliance-oriented solutions in response to legal requirements as they see 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.[92] To comply with Title VII, for example, companies draft policies, create new offices and positions, develop dispute resolution mechanisms and reporting structures, and hire consultants to craft new approaches, to name just a few steps. And these systems spread rapidly through industry as professionals share their innovations with colleagues.[93]

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. When an employee has a discrimination claim, she doesn't immediately go to a judge. She tells her diversity officer, 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. And yet, 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 or were steeped in the structures in the first place.[94]

These structures are then mobilized by corporations to push back when employees try to vindicate their rights. In the Title VII context,

---

[90] *Id*. at 30-31.

[91] *Id*. at 31.

[92] *Id*. at 31-33.

[93] *Id*. at 32.

[94] *Id*. at 33-39. *See also* Klonick, *supra* note 64, at 1618-22, 1630-31 (arguing that platforms like Google and Facebook developed content moderation policies and processes that resemble "heuristics and structures familiar in legal decision-making in part because those who developed the structures were steeped in First Amendment law).

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.[95] 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,[96] allowed compliance structures to enter into the legal consciousness as evidence of real progress,[97] and transformed the few workplace discrimination proceedings into debates over structures rather than civil rights.

The final stage of legal endogeneity is deference to symbolic structures by the courts, 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 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.[98] 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,[99] the increasingly common tendency for lawyers on both sides of discrimination cases to refer

---

[95] *See* EDELMAN, *supra* note 18, at 158-67.

[96] *Id*. at 37. *See also* KRISTEN 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).

[97] *See* EDELMAN, *supra* note 18, at 37-8. By "legal consciousness," Edelman was referring to society's general conception of what the law means, something affected by the media, popular culture, political leaders, individual backgrounds, and cultural experiences with the law, to name just a few. *See id*. at 154.

[98] *See id*. at 173.

[99] *See, e.g.*, Burlington Indus., Inc. v. Ellerth, 524 U.S. 742 (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 Savings Bank v. Vinson, 477 U.S. 57, 72-73 (1986) (holding that although the mere presence of a grievance procedure and nondiscrimination 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).

to these structures in their briefs,[100] and judicial politics,[101] 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.[102] 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.

B. Legal Endogeneity in Privacy Law

A similar narrative is playing out in privacy law today, and the outsourcing of privacy law compliance to engineers is a chief catalyst. Ambiguous privacy rules, from the GDPR to FTC decrees, open the door for vendors to frame the law in ways that serve corporate, rather than consumer, interests. They become the locus of the social practice of privacy law because they, not legislators or even CPOs, embed their legal vision into technology design. And their proliferation throughout the privacy compliance market impacts the legal consciousness: judges, 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 indelible as Edelman fears it is for Title VII and workplace equality.[103] This Part establishes the narrative of legal endogeneity in privacy law and maps the ways in which third-party technology vendors are contributing to the erosion of substantive privacy protection.

1. Ambiguity in Privacy Law

---

[100] *See* EDELMAN, *supra* note 18, at 170-72.

[101] *Id*. at 190.

[102] Edelman calls this the "legal consciousness," or "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. *See* 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 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).

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

Privacy law's flexible definitions[104] and standards,[105] sometimes challenging even in the hands of lawyers, are particularly vulnerable to being weakened and undermined by technology design and symbolic

---

[104] There is a rich tradition of scholars exploring the meaning of privacy. Almost all of them recognize its malleability. *See, e.g.*, Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 234 (1977) (noting that privacy has a "protean "a protean capacity to be all things to all lawyers."); 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."); 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 hasn't stopped scholars from trying. Privacy has been defined as a right to be let 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* Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); DANIEL J. SOLOVE, THE DIGITAL PERSON 90, 94, 102-04 (2004); JULIE INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); Steve Matthews, *Anonymity and the Social Self*, 47 AM. PHIL. Q. 351, 351 (2010); Jean L. Cohen, *The Necessity of Privacy*, 68 SOC. RES. 318, 319 (2001); 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); Charles Fried, *Privacy*, 77 YALE L. J. 475, 484 (1968); JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2000); Howard B. White, *The Right to Privacy*, 18 SOC. RES. 171, 180-81 (1951); Robert S. Gerstein, *Intimacy and Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 265 (Ferdinand Shoeman, ed., 1984); NEIL M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, PRIVACY, AND THE INTEGRITY OF SOCIAL LIFE (2009); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L. J. __ (forthcoming 2019); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016). *See also* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012); ANITA ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988).

[105] 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 POSNER, THE PROBLEM 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 J. Schlag, *Rules and Standards*, 33 U.C.L.A. L. REV. 379, 383-420 (1985) (examining the form and rhetoric of the rules versus standards debate).

structures. When law takes the form of flexible standards, decision makers on the ground are empowered to adapt, consider changes in context, and assess what is best under the circumstances,[106] especially before a court of law has a chance to have its say. But vague standards can also be problematic. The "staggeringly complex" and "ambiguous"[107] GDPR lays out several of these broad standards that need to be given "specific substance over time."[108] 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."[109] 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.[110] Even guidance documents from the Article 29 Working Party, an advisory group of data protection authorities from across Europe,[111] 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."[112] And scholars have suggested a variety of definitions, ranging from vague

---

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

[107] 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.

[108] *See* Margot Kaminski, *The Right to Explanation, Explained*, at *9 (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3196985.

[109] *See* GDPR, *supra* note 9, art. 25, at 48.

[110] *See* Ari Ezra Waldman, *Privacy's Law of Design*, 9 U.C. IRVINE L. REV. __ (forthcoming 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 processes instantiated in hardware and software." HARTZOG, *supra* note 74, at 11.

[111] 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, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (last visited May 3, 2018).

[112] Art. 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things 3, *available at* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. 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.

privacy principles[113] and privacy-enhancing technologies[114] to sets of values[115] or "boundaries and goals" for design[116] to norms based on products liability for design defects.[117] This ambiguity will persist until European courts set out clear rules.

The GDPR's consent requirements are also unclear. If companies want to collect ordinary, non-sensitive data, user consent must be "unambiguous."[118] If the data is sensitive, including physical and mental health information, race, ethnicity, or sexual orientation, for example, consent must be "explicit."[119] The two concepts are not the same,[120] but neither the GDPR itself nor any interpretive document clarify what steps make consent explicit rather than just unambiguous. For example, although the Article 29 Working Party 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

---

[113] Ann Cavoukian, the former Information & Privacy Commissioner of Ontario, Canada, has argued that privacy by design is "the philosophy and approach of embedding privacy into the design specifications of various technologies." ANN CAVOUKIAN, PRIVACY BY DESIGN 1 (2009), *available at* http://www.ipc.on.ca/images/Resources/privacybydesign.pdf. *See also* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE SEVEN FOUNDATIONAL PRINCIPLES (2009), http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.

[114] *See, e.g.*, Ira Rubinstein & Nathaniel Good, *Privacy By Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L. J. 1333, 1341-1342 (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).

[115] *See, e.g.*, NISSENBAUM & FLANAGAN, *supra* note 74 (discussing the way in which game designers integrate values into their products).

[116] HARTZOG, *supra* note 74, at 7.

[117] *See* Waldman, *Privacy's Law of Design*, *supra* note 110 (applying several analogies from the law of products liability for design defects to specify what privacy by design should mean in practice).

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

[119] *Id*., art. 9, para. 2(a), at 38.

[120] *See* 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) [first reading], at 3 (Dec. 15, 2015) ("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.").

in itself constitute unambiguous consent," it never makes clear what kind of positive action is required.[121]

Alongside the GDPR, privacy professionals in the United States must incorporate FTC consent decrees into the legal context in which their companies operate.[122] But despite a growing agenda as the de facto federal privacy regulator,[123] 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.

This is particularly true for the FTC's assessment requirements. The FTC requires companies operating under consent decrees to submit assessments roughly every two years for the life of the order.[124] 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.[125] That seems specific enough, without much opportunity for error. But *assessments* aren't audits, and 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.[126] Assessments are based on

---

[121] Art. 29 Data Protection 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.

[122] 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).

[123] 15 U.S.C. § 45(a)(1) (2016) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

[124] *See, e.g.*, Decision and Order at 5, In the Matter of Google, Inc., FTC File No. 102 3136, No. C-4336 (Oct. 13, 2011) [hereinafter, Google Order], https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf; Decision and Order at 4, FTC File No. 092 3093, No. C-4316 (Mar. 2, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf.

[125] *See* Google Order, *supra* note 124, at 5.

[126] *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 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-

assertions from management rather than wholly independent analyses from auditors, and are usually framed by goals set by management.[127] 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.

Another ambiguous standard is the FTC's requirement that companies provide "adequate" notice to consumers. In *FTC v. Frostwire, LLC*,[128] 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.[129] In *FTC v. Echometrix*,[130] the FTC found that broad statements in its privacy policy were too vague and "failed to disclose *adequately*" the company's data collection regime.[131] And in *In re Sears Holdings Management Corp.*,[132] the FTC concluded that Sears' long, legalese licensing agreement "failed to disclose *adequately* that the software application, when installed" would monitor a long list of consumer behavior.[133] 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 isn't left open to interpretation on the ground is the FTC's baseline rule: don't lie.[134]

Ambiguous laws and flexible standards are nothing new. The limitations of language and the legislative drafting process often result in

---

55 (1997) (describing the responsibilities of independent auditors under Section 10A of the Securities Exchange Act).

[127] *See* Megan Gray, *Understanding and Improving Privacy "Audits" Under FTC Orders*, at 6, STAN. L. SCH. CENTER FOR INTERNET & SOC. (Apr. 18, 2018 1:10 PM), https://cyberlaw.stanford.edu/files/blogs/white%20paper%204.18.18.pdf.

[128] Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Frostwire, LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 12, 2011), http:// www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf.

[129] *Id*. at 16 (emphasis added).

[130] Complaint for Permanent Injunction and Other Equitable Relief, FTC 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.

[131] *Id*. at 4, 5 (emphasis added).

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

[133] *Id*. at 5.

[134] *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).

statutes and rules that leave their meaning and details to those interpreting them.[135] And the debate over standards and rules is as old as the common law.[136] Margot Kaminski argues that seemingly vague terms in the GDPR become clear when we combine the GDPR with interpretive tools, including reports from the Article 29 Working Party. That is, she argues, how it's supposed to work.[137] 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.[138]

But interpretations of the GDPR and FTC actions neither emerge in a vacuum nor necessarily take on the color the Working Party or the FTC intend. Rather, interpretations are made by real people affected by biases, social influences, and institutional pressures.[139] And by the FTC's own count, the agency averages only 10 privacy-related cases per year, limiting the sources lawyers have from which to glean lessons and find clarity.[140] Even if clarity is to come, the FTC and data protection authorities will only have the opportunity to issue official judgments after protracted investigations and litigations. Until then, corporate actors on the ground

---

[135] See e.g., Kenneth Bamberger, *Normative Canons in the Review of Administrative Policymaking*, 118 YALE L. J. 64, 75-76 (2008); 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 (2002). *See also* REED DICKERSON, THE INTERPRETATION AND APPLICATION OF STATUTES 43-53 (1975) (discussing how the inherent limitations of language create ambiguity in statutes).

[136] *Compare, e.g.*, Baltimore & Ohio Railroad 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 Railway 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.*, FREDERICK SCHAUER, PLAYING BY THE RULES 149-55 (1991); MARK KELMAN, A GUIDE TO CRITICAL LEGAL STUDIES 15-63 (1987); Duncan Kennedy, *Form and Substance in Private Law Adjudication,* 89 HARV. L. REV. 1685, 1689-90 (1976).

[137] *See* Margot Kaminski, *The Right to Explanation, Explained*, at *9 (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3196985.

[138] *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).

[139] 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).

[140] *See* Solove & Hartzog, *supra* note 14, at 600.

can use their first-mover advantage to entrench their interpretations of the law before any court has its say,[141] interpreting vague terms in light of corporate, rather than consumer, values. And as the responsibilities for legal interpretations increasingly shift from lawyers to engineers at technology vendors, the GDPR's and the FTC's intent becomes more distant.

2. Framing Corporate Obligations Narrowly in Terms of Risk Avoidance

Recognizing the ambiguity 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.[142] As Edelman describes, these professionals "make certain laws or norms visible or invisible to employers and frame those laws' relevance to organizational life."[143] In so doing, they shape the "aesthetic of the law," determining not just what laws make it through the filter, but what those legal obligations look like.[144] Human resources professionals and lawyers figure prominently in Edelman's work on the implementation (or lack thereof) of civil rights laws.[145] In the privacy space, lawyers, CPOs, and their staffs should assume the 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 and to protect consumers from predatory data collection practices.[146]

---

[141] The first-mover advantage refers to the benefits that accrue to a company that is first in the market. *See, e.g.*, William T. Robinson & Sungwook Min, *Is the First to Market the First to Fail? Empirical Evidence for Industrial Goods Businesses*, 39 J. MARKETING RES. 120, 126 (2002); 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). 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.

[142] Bamberger & Mulligan, *supra* note 23, at 271, 292.

[143] EDELMAN, *supra* note 18, at 82.

[144] *Id*.

[145] *See id*. at 78-80.

[146] The GDPR's first stated goal is "protection of natural persons with regard to the processing of personal data." *See* GDPR, *supra* note 9, art. 1, at 32. *See also* Assembly Bill 375, Sec. 2 (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.").

But this is more of an ideal type than anything else. On the ground, third-party technology vendors have become increasingly active in framing the requirements of privacy law. They are, of course, not alone; in-house and firm lawyers,[147] management consultants,[148] and even marketing professionals[149] play important, and sometimes frustrating roles, as well. But the role of privacy technology vendors is both powerful and underexplored. Based on primary source research, including interviews, marketing literature, industry journal articles, blogs, and white papers, these vendors more commonly frame privacy duties narrowly, either as focused on corporate risk avoidance or on small pieces of broader privacy obligations, ignoring privacy's flexible standards in favor of easy-to-code, yet underinclusive rules.[150] This happens even where CPOs try to bring a strong, pro-consumer, trust-based vision of privacy to their work[151] because that commitment to privacy can be undermined by third-party vendors.

---

[147] 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 In House 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.

[148] 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 GDPR compliance" and helps companies with "[r]egulation interpretation; … Compliance solutions—people, process and technology execution for an effective cybersecurity and privacy program; [and] Compliance management—monitoring and maintaining controls going forward." *See* Protiviti, GDPR Is Here—Now What?, https://www.protiviti.com/US-en/technology-consulting/general-data-protection-regulation (last visited Sept. 6, 2018). Galexia helps companies "understand their legal, regulatory and best practice requirements," and "develop[s] compliance tools, manage stakeholder consultation and architect solutions." *See* Services, http://www.galexia.com/public/services/ (last visited Sept. 6, 2018).

[149] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp (describing in part the role of marketing professionals in encouraging statisticians to develop privacy invasive algorithms).

[150] *See* Citron, *supra* note 28, at 1255 & n. 31 (noting that expert agency deliberation may falter in an era of automated decision making because of an increasingly tendency to "adopt policies involving simple questions and answers that are easy to translate into code, even when strong substantive reasons favor a more nuanced approach.").

[151] *See* BAMBERGER & MULLIGAN, *supra* note 23, at 66-68 (noting that many CPOs interviewed believed that corporate privacy strategy was about maintaining user trust and being stewards of data and responsible to consumers).

In the last three years, more than 170 companies have emerged to meet the informational and technological needs of organizations trying to comply with the GDPR and new FTC consent decrees.[152] My research suggests that technology vendors say their expertise is in implementation; they sell themselves as doers. But in "doing" privacy law, in creating systems, developing compliance software, and filling corporate needs, these vendors are designing tools that reflect normative decisions about what compliance should look like. And their vision is narrowly defined, managerially focused, and compliance-oriented rather than robust or consumer-friendly.

Although it is beyond the scope of this Article to profile every vendor on the market, research into vendors' products, marketing strategies, and personnel, as well as interviews with vendor executives and the privacy professionals that work with them, reveal that some of these firms are selling themselves as experts and marketing their tools as easy-to-use silver bullets for complying with specific legal mandates. Some of them are underinclusive and unverified: they focus on the codable parts of privacy law and often do so based on an engineer's interpretation of legal requirements.

JLINC Labs, for example, an Oakland-based company with 13 employees, exactly none of whom are lawyers, claims its consent management technology can "makes it easy to comply with any data-related legislation."[153] Nymity's privacy compliance software claims that it is "GDPR Ready" and helps "organizations attain, maintain and demonstrate ongoing compliance."[154] FairWarning, which markets privacy and security solutions to health care providers, claims its program "fully addresses 5 of the Phase 2 HIPAA Audit protocol elements and partially

---

[152] The IAPP's *2017 Privacy Tech Vendor Report* included 51 vendors. The 2018 version includes 165, showing significant expansion of the market. Both sources are relevant. *See* IAPP, 2017 PRIVACY TECH VENDOR REPORT (2017), *available at* https://iapp.org/media/pdf/resource_center/Tech-Vendor-Directory-1.4.1-electronic.pdf; IAPP, 2018 PRIVACY TECH VENDOR REPORT (2018), *available at* https://iapp.org/media/pdf/resource_center/2018-Privacy-Tech-Vendor-Report.pdf [hereinafter, VENDOR REPORT]; *see also* Privacy Ecosystem Map, https://download.trustarc.com/dload.php/?f=3URZXT1A-545 (last visited Sept. 4, 2018).

[153] *See* JLINC, What is JLINC?, https://www.jlinc.com/ (under, "Legislative Compliance = $") (last visited Sept. 9, 2018).

[154] *See* Nymity, Privacy Compliance Software, at 3, *available at* https://info.nymity.com/hubfs/Nymity%20Story/Nymity%20Story.pdf?pdf=Nymity-Story; *see also generally* GDPR COMPLIANCE: HOW NYMITY SOLUTIONS HELP 2018 4-17 (on file with author) (noting how Nymity programs can achieve GDPR compliance for any company).

addresses 26 more."[155] ZLTech also offers "GDPR-Ready Solutions," and explicitly claims that its tools to identity, minimize, and govern personal data uses will make clients compliant with multiple parts of the GDPR.[156] In entering this market for legal compliance technologies, these companies are instantiating into their designs particular visions of what the law requires.[157]

Privacy compliance technologies fall into five categories.[158] Most reflect a particular interpretation of a vague law. The largest category, with 99 companies in the market,[159] includes vendors that help companies understand what data they have, how the data is gathered, and who has access to it. These companies offer data discovery and data mapping tools,

---

[155] *See* Fair Warning, Overview: Protecting PHI and Enabling Compliance (on file with author) (referring to the Department of Health and Human Services audit rules and protocols released on March 21, 2016); *see also OCR Launches Phase 2 of HIPAA Audit Program*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html?language=es (last visited Dec. 17, 2018) (noting that Phase 2 audits ensure that entities covered by HIPAA comply with Privacy, Security, and Breach Notification Rules).

[156] *See, e.g.*, Nymity, Reporting on GDPR Compliance, https://info.nymity.com/reporting-on-gdpr-compliance-whitepaper (last visited Sept. 9, 2018) (implying use of toolkit with comply with Article 30 reporting requirements); *see also* Nymity, Nymity's GDPR Compliance Toolkit, https://info.nymity.com/gdpr-compliance-toolkit (last visited Sept. 9, 2018) (Articles 15 (right of access), 17 (right to erasure, or "right to be forgotten"), 18 (right to restriction on processing), 25 (right to privacy by design and by default), 30 (reporting), and 32 (security of personal data) of the GDPR).

[157] When scholars like Joel Reidenberg and Lawrence Lessig argued that computer code is a regulating force of online behavior, they were referring to how the design or code of built online environments can constrain or enable behavior online. *See* Joel R. Reidenberg, *Les Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554-555 (1997) ("The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations."); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (2006) (similar). That is a related, but distinct point. My argument is that technology vendors are instantiating into technology designs their interpretations of what the law requires, thereby mixing law and code to constrain behavior.

[158] This is slightly different than the IAPP's taxonomy, which lists 10 categories. Some of those categories have been combined because the companies often offer overlapping tools. The categories here are also honed through additional research beyond the Vendor Report.

[159] *See* VENDOR REPORT, *supra* note 152, at 9-14.

like those created by Advanced Metadata[160] and CipherCloud,[161] which help companies determine what kind of personal data they have and how they flow throughout a company. This category also includes website scanners, which identify embedded cookies and trackers,[162] and activity monitors, which determine who accesses customer information. This can help companies comply with several legal requirements, including users' right to access, correct, and receive copies of personal data being collected and processed;[163] the GDPR's documentation, security, and data transfer

[160] *See* Advanced Metadata, http://www.advancedmetadata.com/ (last visited Sept. 8, 2018) ("We leverage subject matter expertise to generate best-in-class content and apply our data management and data science expertise to automate regulatory regime governance. Our RegTech Solution helps companies comply with several regulatory regimes via a series of modules. Our GDPR module and algorithms are an excellent resource for organisations where data is central to their success. Our methodology involves performing Data Validation against a selected data sample based on characteristics highlighted as being a priority by the company assessment tool.");

[161] *See* Get Ready for the GDPR, https://www.ciphercloud.com/gdpr-compliance (last visited Sept. 8, 2018) ("CipherCloud Helps GDPR Compliance With: Strong encryption and tokenization for cloud data, meeting GDPR standards for data protection[;] Encryption keys controlled exclusively by customers, meeting "pseudonymization" requirements[;] Exemption from breach notification requirements by effectively anonymizing data[;] Technology specifically called for to meet Privacy by Design and Default principals[;] Dramatic reduction in audit scope by removing data exposure to cloud providers.").

[162] A "cookie" is a data files that records information about a user to personalize her browsing experience and allow websites to remember her when she returns. *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1227-29 (1998) (describing cookie function).

[163] *See* GDPR, *supra* note 9, art. 55, at 43. *See also* Cal. Civ. Code § 1798.100(d).

rules,[164] the ePrivacy Directive,[165] European human rights law,[166] U.S. federal privacy statutes,[167] and the FTC's privacy jurisprudence.[168]

Information gathering tools do not always touch on legal rules so overtly. Services like those provided by BigID,[169] for example, only provide companies with data maps and analytics. But to gather data necessary for privacy law compliance, the designs of many these technologies have to reflect the vendors' interpretations of the legal definitions of "personal information," the category of data to which state, national, and international privacy rules apply. Many vendors, however, focus only on helping clients manage "personally identifiable information" or PII.[170] But

---

[164] *See id*. at art. 30, para. 1, at 50-51 (documentation rules), art. 32, at 52 (security), art. 20, at 45 (data transfer).

[165] *See* Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. L. 136 [hereinafter, ePrivacy Directive].

[166] Indeed, the fact that a hospital lacked activity monitoring was determinative in the European Court of Human Rights (ECHR) in the case, *I v. Finland*, Appl. No. 20511/03 (July 17, 2008), where the ECHR held that a medical records platform that had no access logs and no mechanism for recording and retaining the records of who might have patient data violated Article 8 of the European Convention for the Protection of Human Rights, guaranteeing citizens a right to privacy. *See* European Convention for the Protection of Human Rights and Fundamental Freedoms, Art. VIII, https://www.echr.coe.int/Documents/Convention_ENG.pdf (last visited Sept. 8, 2018). In other words, the state had a legal obligation to ensure that the medical records platform its hospitals used were designed with activity monitoring tools.

[167] *See* 15 U.S.C. §§ 6801-6809 (giving the FTC the authority to "establish appropriate standards for the financial institutions subject to their jurisdiction" in order to "insure the security and confidentiality of customer records and information" and "protect against unauthorized access.").

[168] *See, e.g.*, In re HTC Am. Inc., FTC File No. 122 3049, No. C-4406, at 3 (F.T.C. July 2, 2013) (consent order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf (requiring a "comprehensive security program" with "administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered device functionality or covered information.").

[169] *See* Advanced PI/PII Discovery, https://bigid.com/ ("Inventory PII by data subject & residency for GDPR" and "Document GDPR Article 30 with "living" data flow diagrams).

[170] *See, e.g.,* Cognigo, Achieve GDPR Compliance in Days, Not Months, https://www.cognigo.com/gdpr-3/#demo (last visited Dec. 6, 2018) (referring to "AI-powered PII recognition" and a "proprietary PII Recognition" that is "able to detect data subjects by understanding context").

current laws regulate "personal data"[171] and "personal information,"[172] which go beyond than PII to embrace the way seemingly nonsensitive data can be analyzed to create intimate information.[173] Despite guarantees of compliance, some vendors may be exposing their clients to risk because of their incorrect interpretations of what the law requires.

Second, assessment management software, offered by 65 technology vendors according to the IAPP,[174] can automate the day-to-day work of privacy programs, including operationalizing Privacy Impact Assessments (PIAs),[175] training employees, and completing and submitting compliance documents to regulators. PIAs are expressly required by the GDPR[176] and the FTC requires regulated entities to engage in ongoing monitoring and reporting for up to 20 years after signing a consent decree.[177] PIAs outsourced to vendor software, however, reflect legal requirements as interpreted by the designers of that software. According to the IAPP, although most companies use their in-house legal team to

---

[171] *See* GDPR, *supra* note 9, art. 4(1), at 33 (including "name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" as "personal data").

[172] *See* Cal. Civ. Code § 1798.140(o)(1) (including identifiers, protected characteristics, commercial information, biometric data, browsing history, geolocation data, employment information, education data, and any related inferences under "personal information").

[173] *See, e.g.*, Michael Kosinski, David Stillwell, & Thore Graepel, *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, Proceedings of the Nat'l Acad. of Sci. Apr. 9, 2013, *available at* https://www.pnas.org/content/110/15/5802.

[174] *See* VENDOR REPORT, *supra* note 152, at 9-14.

[175] A Privacy Impact Assessment (PIA), first deployed in the government context, is a formal "analysis of how personally identifiable information is collected, retained, used, [and] shared." The 2002 E-Government Act requires all federal agencies to conduct and issue PIAs "for all new or substantially changed technology that collects, maintains or disseminates personally identifiable information." Fed. Trade Comm'n, Privacy Impact Assessments, https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments. PIAs are not without their challenges. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *PIA Requirements and Privacy Decision-Making in U.S. Government Agencies, in* PRIVACY IMPACT ASSESSMENTS 225, 225-74 (David Wright & Paul De Hert eds., 2012).

[176] *See* GDPR, *supra* note 9, art. 35, at 53-54.

[177] *See, e.g.*, Press Release, FTC Says Hello to 1996 by Waving Goodbye to Thousands of Administrative Orders that Are at Least 20 Years Old, FTC (Dec. 20, 1995), available at http://www.ftc.gov/news-events/press-releases/1995/12/ftc-says-hello-1996-waving-goodbye-thousands-administrative (noting both existing and future consent orders would last twenty years); see also, e.g., Decision and Order at 2, Sony BMG Music Entm't, F.T.C. File No. 062 3019, No. C-4195, at 10 (June 29, 2007), https://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019do070629.pdf (noting 20 year time frame).

conduct PIAs, 15% use a vendor-designed template that may be different than ones created by lawyers or made available by government agencies.[178] CyberSaint Security, for example, markets its own template and guarantees that clients who use its platform can "instantly see [their] compliance status for … GDPR, … FIPS"[179] or "any framework or standard."[180] A demonstration of the product reflects this point: the platform allows companies to maintain and update compliance questionnaires, all of which are created by CyberStrong itself.[181]

Third, 48 companies offer consent management software that can track and record user affirmative consent.[182] To effectively assist with compliance, however, these tools have to be coded to recognize, distinguish, and obtain the different kinds of legal consents – explicit,[183] unambiguous,[184] verifiable,[185] written and informed,[186] and so forth—all of which have (different) legal definitions. Despite those hurdles, vendors often sell themselves as comprehensive consent solutions. 3PHealth, for example, developed a mobile platform that allows individuals to have "complete control" over sharing their personal information and calls the platform a "simple, consistent, comprehensive data privacy and individualization navigation framework."[187] A product demonstration reveals little in-app distinction between the types of consent needed among

---

[178] IAPP & TRUSTARC, MEASURING PRIVACY OPERATIONS 12 (Dec. 5, 2018), *available at* https://iapp.org/media/pdf/resource_center/IAPP-Measuring-Privacy-Operations-FINAL.pdf [hereinafter, MEASURING PRIVACY].

[179] CyberSaint Security, The CyberStrong Platform 2 (2018) (available for download at https://content.cybersaint.io/learn-more-the-cyberstrong-platform?hsCtaTracking=2472ecde-ea53-4206-882b-8b9fd42cbff3%7C542110f0-14ae-4431-b87c-8ca808d368a9) (on file with author).

[180] *See* CyberSaint Security, Product Overview, https://www.cybersaint.io/product-overview (last visited Dec. 6, 2018).

[181] Telephone interview/product demonstration with Eamonn Burke, CyberSaint Security (Dec. 7, 2018) (notes on file with author).

[182] *See* VENDOR REPORT, *supra* note 152, at 9-14.

[183] *See, e.g.*, Cal. Fin. Code § 4052.5 (requiring explicit consent before financial companies can share customer information).

[184] *See, e.g.*, GDPR, *supra* note 9art. 4, at 34 (consent must be unambiguous); *id.*, art. 9, para, 2(a), at 38.

[185] *See* Children's Online Privacy Protection Act (COPPA) of 1998, Pub. L. No. 105-277, 112 Stat. 2681-2728, 15 U.S.C. §§ 6502(b)(I)(a)(ii) (requiring verifiable parental consent).

[186] *See, e.g.*, Alaska Stat. § 18.13.010(c) ("A general authorization for the release of medical records or medical information may not be construed as the informed and written consent required by this [law].").

[187] *See* 3PHealth, Choice Story, at 2, https://www.3phealth.com/wp-content/uploads/2018/09/Choice%C2%AE-Story-181102.pdf (last visited Dec. 5, 2018).

different privacy laws, preferring a standardized opt-in approach to all.[188] That type of affirmative consent may suffice in many circumstances, but even so, it reflects a coded interpretation of privacy's law of consent.

Fourth, de-identification tools designed by 26 different companies[189] allow organizations to process personal data safely in compliance with various state,[190] national,[191] and international statutes[192] that require data anonymity or pseudonymity. But these laws leave room for interpretation: engineers at these vendors decide both the kind of anonymization used and the subset of data to which it applies. Arcad Software, for example, says that its "DOT Anonymizer" is "[d]esigned to meet the strictest requirements of the GDPR" by "hiding or anonymizing the personal elements of data."[193] But that requires coding for what a law defines as "personal elements," a process the company does not explain.

Finally, 29 vendors offer incident response platforms that help companies respond to data breaches swiftly and with proper notice, as required by the GDPR[194] and statutes in every state in the United States.[195] There are two types of vendors in this space. Companies like Proofpoint

---

[188] Telephone interview and product demonstration with Peter Cranstone, CEO, 3PHealth, Dec. 11, 2018 (notes on file with author).

[189] *See* VENDOR REPORT, *supra* note 152, at 9-14.

[190] *See, e.g.*, Cal. Civ. Code § 1798.140(o)(1) (defining "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.").

[191] *See* Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.); *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 U.C.L.A. L. REV. 1701, 1736-38 (2010) (discussing how HIPAA's Privacy Rule was promulgated alongside a strong faith in the power of anonymization to protect personal information).

[192] The GDPR applies to "personal data," which is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR, *supra* note 9, art. 4, para. 1, at 33; *see also* GDPR, *supra* note 9, recital 25, at 5.

[193] Protection of Personal Data, DOT-Anonymizer White Paper, at 10 (available for download, on file with author).

[194] *See* GDPR, *supra* note 9, art. 33, at 52 (requiring notification to national data protection authorities within 72 hours of a data breach).

[195] *See* Security Breach Notification Laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Jan. 2, 2019).

position themselves as technological resources to stay ahead of and respond to digital threats. They don't make promises about regulatory compliance. Other vendors make legal conclusions about their tools and guarantee legal compliance as part of technical incident response. Resilient, for example, states that its Privacy Module guides clients "through the *correct* response to data loss incidents, helping to meet regulatory deadlines" and other GDPR requirements. It tells clients which authorities to notify, "how they should be notified, and what information is required," and provides their own proprietary templates for those purposes.[196] To do that, though, Resilient has to code interpretations of the law into those guidelines, recommendations, and templates.

Many of these vendors also frame their platforms as easy ways to avoid noncompliance risks. ZLTech markets its "GDPR-Ready Solutions" as ways to avoid "the risk of unprecedented sanctions."[197] And Clarip, a software-as-service provider, bills itself as "the next generation … data privacy platform that helps brands minimize privacy risks."[198] Other companies approach risk differently. Spearline, for example, provides a compliance management platform that, among other things, allows companies to identify and patch risks to data security.[199] Undoubtedly, not all third-party vendors see their role as mitigating corporate risks of noncompliance, but many follow that model.

This risk focus is also reflected in the industry literature. In the Journal of Data Protection and Privacy, an industry journal offering analysis of international privacy developments,[200] 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

---

[196] *See* Monica Dubeau, *Resilient Platform Adds GDPR Regulations, Helping Organizations Address 72-Hour Notification Requirement*, IBM RESILIENT BLOG (May 24, 2018), https://www.resilientsystems.com/cyber-resilience-knowledge-center/incident-response-blog/resilient-platform-adds-gdpr-regulations-helping-organizations-address-72-hour-notification-requirement/ (emphasis added).

[197] *See, e.g.*, Kon Leong, *The GDPR Puzzle*, INSIDE BIG DATA (Sept. 7, 2017), http://www.zlti.com/wp-content/uploads/2017/09/The-GDPR-Puzzle-insideBIGDATA.pdf. *See also* ZLTech, GDPR-Ready Solutions 3 (pamphlet on file with author).

[198] *See* Clarip, https://www.clarip.com/business (last visited Sept. 14, 2018).

[199] *See* Spearline Data Protection, https://www.spearline.com/riskandcompliance/data-protection (last visited Sept. 14, 2018).

[200] *See* Journal of Data Protection and Privacy, https://www.henrystewartpublications.com/jdpp (last visited Sept. 14, 2018) ("Essential reading for Presidents, CEOs, CTOs, CFOs, COOs and CIOs in private and public sectors, Government Departments and membership/trade bodies").

example, the authors recognize the GDPR's requirement that privacy protection mechanisms be proportional to the risk data processing pose to users. But the lion's share of the article focuses on how PIAs can be used to mitigate corporate exposure to GDPR penalties.[201] Two practical guidebooks do the same.[202] 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,"[203] 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.

This risk framing pervades the privacy compliance landscape. The IAPP and TrustArc published a study focusing on prioritizing different parts of GDPR based on the risks of noncompliance to the company.[204] And the organization has also framed data minimization as a way of reducing corporate risk[205] 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.[206] This focus ultimately encourages many companies to house their privacy officers within their risk management departments,[207] but it also puts a decidedly corporate spin on privacy law itself. 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.[208]

---

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

[202] *See, e.g.*, Alan Calder, Richard Campo, & Adrian Ross, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide 142-58 (2018) (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).

[203] Bamberger & Mulligan, *supra* note 175, at 228.

[204] IAPP & TrustArc, Getting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation (2018).

[205] Webinar, Reducing Risk Through Data Minimization, Sept. 6, 2016, *available at* https://iapp.org/store/webconferences/a0l1a000002hDCIAA2/.

[206] *See, e.g.*, Webinar, the Role of Risk Management in Data Protection, Jan. 23, 2015, *available at* https://iapp.org/store/webconferences/a0l1a000000SKCzAAO/.

[207] 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).

[208] *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 to physical, material or non-material damage …"). *See also*

Framed narrowly, then, data minimization means doing the least possible to shield themselves from liability. Framed broadly, it is part of a broader data use approach that respects user wishes.

Framing the data privacy law 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,[209] especially since some executives still see privacy as inconsistent with corporate profit goals. The risk of a fine of 4% of global revenue goes a long way to making privacy compliance a central corporate mission.[210] 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.[211] And third-party vendors follow suit because it allows them to increase their market share and emphasize the importance of their services.[212] Companies respond to this framing: the IAPP found that organizations regulated by the GDPR are most likely to spend money on third-party vendors to address complex technical requirements of the law.[213]

But risk framing is problematic if our 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,[214] their need for trust,[215] and their consistent distaste for transfers of data to third

---

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").

[209] *See* EDELMAN, *supra* note 18, at 98.

[210] *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).

[211] *See* EDELMAN, *supra* note 18, at 97.

[212] *Id*. at 98.

[213] *See* IAPP & TRUSTARC, *supra* note 204, at 3, 5.

[214] *See* Frederic Stutzman & Woodrow Hartzog, *The Case for Online Obscurity*, 101 CAL. L. REV. 1 (2013); HARTZOG, *supra* note 110, at 110-11.

[215] *See* HARTZOG, *supra* note 74, at 97-107 (discussing various aspects of trust in privacy law); WALDMAN, *supra* note 104, at 1-10, 47-76 (arguing that privacy is based on relationships of trust between individuals and thus can protect the value of trust); Richards

parties.[216] 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,[217] especially if companies innovate and market around making privacy as essential aspect of their business model.

3. Symbols of Compliance

Having instantiated interpretations of privacy law into compliance technologies and framed corporate privacy obligations in terms of risk rather than substantive privacy protections for users, third-party vendors create structures and services to comply with their version of the law.[218] 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"[219] and because the GDPR requires the designation of a data protection officer (DPO),[220] many companies have to hire a DPO. Similarly, because the GDPR gives consumers a right to access their information and a right to erase

---

& Hartzog, *supra* note 104, at 451–57 (protecting privacy can build trust between online platforms and consumers); Kirsten Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online*, 18 FIRST MONDAY http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802 (2013); Katherine Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B. C. L. REV. 741 (2008); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1308–10 (2000) (noting that we entrust our data to web platforms).

[216] *See, e.g.*, Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J. LAW & TECH. 112, 131-34 (2017) (noting consistent consumer rejection of corporate practices that involve data collection through data brokers).

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

[218] 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.

[219] *See, e.g.*, Agreement Containing Consent Order, at 4, In the Matter of Google, Inc., Docket No. C-4336, No. 102 3136 (F.T.C. Oct. 24, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf [hereinafter, Google Consent Decree] (requiring a "comprehensive privacy program").

[220] *See* GDPR, *supra* note 9, arts. 37-39, at 55-56.

irrelevant, incorrect, and outdated information,[221] data collectors have to develop systems to find and categorize user data. And laws like CalOPPA require privacy notices that describe data use practices.[222] 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.[223] As is the process of online content moderation, where rules reflect neoliberal First Amendment principles[224] and questions are adjudicated with quasi-judicial proceedings.[225] Notably, symbolic structures are, on their own, not necessarily ineffective. An equal 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. 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.[226] In many companies, these structures are taken seriously and employees at all levels work with privacy offices to

---

[221] *Id*. at arts. 15, 17, at 43-44.

[222] Cal. Bus. & Prof. Code § 22575.

[223] *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.

[224] *See* Klonick, *supra* note 64, at 1618-22, 1658-62 (2018) (arguing that content moderation policies have a baseline in free speech norms).

[225] *See id*. at 1638-47 (showing how the process of content moderation bears some resemblance to judicial process); *see also* Kate Klonick & Thomas Kadri, *How to Make Facebook's 'Supreme Court' Work*, N.Y. TIMES (Nov. 17, 2018), https://www.nytimes.com/2018/11/17/opinion/facebook-supreme-court-speech.html (discussing Facebook's plan to create an independent body to make content moderation decisions).

[226] *See* BAMBERGER & MULLIGAN, *supra* note 23, at 83-6.

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,[227] they are now required by many state and federal mandates.[228] 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.[229] No one reads them[230] because they are long[231] and difficult to understand.[232] And they are designed and presented to us in ways that make them manipulative of our behavior.[233] 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.

Third-party vendors contribute to the development of merely symbolic structures in privacy law in several ways. They may reduce privacy programs to flow charts, check lists, and templates. For example, Nymity offers "software solutions for templating" to create an automated "privacy program … made up of policies, procedures, and other

---

[227] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 593 (2007) ("Online privacy policies have appeared…as voluntary measures by websites"); *see also* Solove & Hartzog, *supra* note 14, at 593-94; 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).

[228] *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).

[229] Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L. J. 39, 40, 87-88 (2015) ("[A]mbiguous wording in typical privacy policies undermines the ability of privacy policies to effectively convey notice of data practices to the general public.").

[230] *See, e.g.*, George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15, 15 (2004).

[231] 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 visited. *See* Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOM. & HIGH TECH. L. 273, 274 (2012). This translates to about 54 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. 540, 563 (2008).

[232] *See* 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).

[233] *See* Waldman, *supra* note 228, at 107-17.

accountability mechanisms."[234] Nymity also offers privacy management software that boils down to automated questionnaires for intracompany communications about privacy issues and data visualizations.[235] It can make approvals efficient "where multiple individuals," i.e., a separate privacy team, "are involved in the approval process."[236] 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. One engineer I interviewed noted that the protocols rarely had any substantive impact on design. As one former engineer put it, "we would need to run our design by privacy, legal, and marketing."[237] But the process was "compliance-style. I remember being told by my manager that 'privacy checked the boxes, so we can go ahead.'"[238] 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.[239] "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."[240] This narrow, compliance focus reduced internal compliance rules into a merely symbolic structure.

Another example of how third party vendors deploy merely symbolic structures that interfere with the substantive implementation of privacy law is how companies in the U.S. respond to FTC audit or "assessment" requirements. Assessments, like those required of Google[241] and Facebook,[242] are often the only real weapons in the FTC's arsenal[243]

---

[234] NYMITY, 2018 PRIVACY COMPLIANCE SOFTWARE BUYER'S GUIDE 9 (2018) (on file with author) (suggesting that its templating software will allow clients to create their privacy programs).

[235] *See id*. at 15 ("Section 3: Automated Privacy Management Software").

[236] *See id*. at 17.

[237] Telephone interview with former engineer at Google and Microsoft (Oct. 4, 2016) (notes on file with Author).

[238] Telephone interview with former Google employee (Apr. 18, 2016) (notes on file with Author).

[239] Google and Microsoft engineer interview, *supra* note 237.

[240] Google employee interview, *supra* note 238.

[241] *See* Google Consent Decree, *supra* note 219, at 5-6

[242] *See* Agreement Containing Consent Order, at 6-7, In re Facebook, Inc., Docket No. C-4365, No. 092 3184, at 5 (F.T.C. Nov. 29, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf

[243] 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*

because they ostensibly require a qualified, independent third party to verify corporate compliance. And they have been heralded as game changers.[244]

In reality, they have failed to achieve that goal because vendors have helped transform these assessments into mere symbols of compliance. The FTC wanted an assessment to ensure that Google, for example, had a privacy team, an ongoing and flexible privacy assessment process, relationships with vendors capable of protecting data, and a few other related requirements.[245] 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. As evidence for this conclusory statement, the report refers the reader to Google's responses to the auditor's questions, not any actual evidence.[246] 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."[247] 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 audits can become mere symbols of compliance.

Technology vendors contribute to the erosion of audits as effective oversight tools by offering nearly completed, and sometimes fully filled audit-ready reports to assert compliance. CyberSaint markets "audit-ready

---

Press Release, Commission Approves Federal Register Notice Adjusting Civil Penalty Amounts, FTC (Dec. 23, 2008), http://www.ftc.gov/opa/2008/12/civilpenalty.shtm.

[244] 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/ (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), 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/.

[245] *See* Google Consent Decree, *supra* note 219, at 5-6.

[246] Initial Assessment Report on Google's Privacy Program for the Period Oct. 29, 2011 – Apr. 25, 2012, at 9, *available at* https://epic.org/privacy/ftc/googlebuzz/FTC-Initial-Assessment-09-26-12.pdf.

[247] *Id*. at 14.

reports … that require no human effort to produce."[248] Nymity offers templates that are "60 percent complete, flexible to the needs" and business focus of the company, making regulatory "compliance easy."[249] These products are attractive to overworked privacy professionals seeking to reduce costs and work hours spent on audits and documentation. But at the same time, they foster the perception of compliance without any deep dive into substance.

4. Managerialization of Privacy Law

Despite elevating mere form over substance, these structures have diffused through the privacy ecosystem. The IAPP found that investment in third-party technology vendors was the second most popular strategy for privacy compliance in 2017.[250] The only barrier to using technology vendors was money: "if they've got the budget, they're in the market."[251] And privacy blogs and conferences are turning their attention to outsourcing privacy compliance with new and frequent analyses.[252]

This spotlight has catalyzed the spread of merely symbolic structures through networks of privacy professionals.[253] The same vendors work with many different companies. Vendors and consulting firms sponsor conferences of privacy professionals.[254] The IAPP's annual report on technology vendors gives members easy access to a curated list of

---

[248] *See* CyberSaint Security, All-In-One Integrated Risk Management, https://www.cybersaint.io/ (last visited Dec. 11, 2018).

[249] Interview with Paul Lewis, FIP, CIPM, CIPT, CIPP/C, CISSP, Senior Privacy Office Solutions Advisor, Nymity, Washington, D.C. (Feb. 27, 2018) (notes on file with author).

[250] *See* VENDOR REPORT, *supra* note 152, at 16; *see also* IAPP & EY, IAPP-EY Annual Privacy Governance Report iv-v (2017), *available at* https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf.

[251] IAPP & TrustArc, How Privacy Tech is Bought and Deployed 2 (2018), available at https://iapp.org/media/pdf/resource_center/iapp-trustarc-how-privacy-is-bought-used-final.pdf

[252] *See, e.g.*, Jeff Northrop, *50 Shades of the Privacy Profession*, PRIVACY TECH (Feb. 8, 2015), https://iapp.org/news/a/50-shades-of-the-privacy-profession/.

[253] See Mark 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).

[254] Sponsors of the 2018 Privacy+Security Forum, for example, included law firms, PwC, Radar, ZLTech, BigID, FairWarning, Nymity, TrustArc, Norton Rose Fulbright, Anonyme Labs, and others. *See* Privacy+Security Forum, 2018 Sponsors, https://privacyandsecurityforum.com/sponsors/ (last visited Dec. 8, 2018).

potential partners.[255] And professionals share their consultant and vendor experiences and recommendations with each other through serendipitous interactions at workshops and conferences.[256] Technology companies, then, outsource privacy compliance to the same set of vendors. This contributes 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.[257]

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.[258] What's happening in privacy law is similar. Even where in-house privacy professionals are doing their best, their tendency to outsource compliance to consultants and technology vendors is shifting privacy law to vendor engineers.

When CyberSaint, for example, feeds a new privacy or cybersecurity law through its natural language processing algorithm to create compliance questionnaires for clients to complete, assess their level of risk, and report to regulators,[259] CyberSaint and its engineers become the

---

[255] *See* VENDOR REPORT, *supra* note 152.

[256] *See* EDELMAN, *supra* note 18, at 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* IAPP Conferences, https://iapp.org/conferences/ (last visited Sept. 1, 2018). 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 Forum, https://privacyandsecurityforum.com/ (last visited Sept. 1, 2018). 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/ (last visited Sept. 1, 2018); Computers, Privacy, and Data Protection (CPDP), https://www.cpdpconferences.org/ (last visited Sept. 1, 2018); American and European privacy leads have found these meetings essential to "exchange knowledge[,] … discuss issues and … standards and understandings" and "create[] a network of diverse expertise." BAMBERGER & MULLIGAN, *supra* note 23, at 99 (quoting a data protection officer from Germany).

[257] See Paul J. DiMaggio & Walter F. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, AM. SOC. REV. 147, 147-49, 153 (1983).

[258] *See* EDELMAN, *supra* note 18, at 124-50.

[259] Telephone interview with Aemonn Burke, CyberSaint, Dec. 7, 2018 (notes on file with author).

filter for privacy law. They, or more accurately, the algorithm they design, determine what the law requires and what steps companies must take to comply. Nymity provides lists to clients to show them how to integrate privacy into design and into the corporate structure. Its automated compliance tools come "60% complete … and the business user fills out the rest" of the template to complete compliance documents.[260] Those tools may make Nymity's clients more efficient, but the decisions about how those tools work and what constitutes compliance were made long ago by Nymity engineers. When Radar, which provides data breach incident response management, states that it "generates an incident specific response plan and notification guidelines according to federal, state, and international laws" and "provides all the required documentation to support the organization's burden of proof obligation under the breach laws,"[261] Radar is the point at which the law is being negotiated. Radar engineers have embedded what they understood to be legal reporting and paper trail requirements. And AuraPortal's "GDPR Accelerator" calls itself an "All in 1" complete compliance management tool with templates, logs, and systems "with predesigned processes to comply with regulations."[262] Many other technology vendors make similar guarantees.[263] In all of these cases, the law is being interpreted and analyzed by engineers far from regulators' and CPOs' offices.

Vendors also 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

---

[260] Interview with Paul Lewis, FIP, CIPM, CIPT, CIPP/C, CISSP, Senior Privacy Office Solutions Advisor, Nymity, Washington, D.C. (Feb. 27, 2018) (notes on file with author).

[261] Radar, Product Data Sheet, Incident Response Management: Simplify Compliance with Automated Multi-Factor Risk Assessment (on file with author); *see also* Radar, Simplify Compliance with GDPR Breach Notification Obligations, https://www.radarfirst.com/gdpr (last visited Dec. 7, 2018).

[262] *See* AuraPortal, GDPR: Accelerate Compliance in Record Time, https://www.auraportal.com/product/gdpr/ (last visited Dec. 8, 2018).

[263] *See, e.g.*, Mentis, GDPR: Are You Prepared, http://www.mentisoftware.com/GDPR.html (last visited Sept. 9, 2018) (marketing its various platforms as compliant with several GDPR provisions); Tag Auditor with Trackermap, https://www.crownpeak.com/products/monitoring-solutions/tag-auditor-with-trackermap (last visited Sept. 9, 2018) (Evidon (now Crownpeak), a vendor that works with a diverse array of companies from Subaru to the Associated Press, offers website tracking and consent solutions they say "ensure" compliance with the GDPR, CalOPPA, and other statutes, among other tools).

diversity, generally,[264] and offered managerial (i.e., profit), rather than social, justifications for increased diversity.[265] 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.[266] Some vendors are doing the same thing to privacy. They market their privacy tools as enhancing efficiency, speed, and productivity,[267] 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.[268] The IAPP has hosted web conferences and published blogs focused on the efficiency and productivity benefits of privacy technology vendors.[269] And although consumers can benefit when companies start thinking about privacy as good for business,[270] the value proposition is

---

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

[265] *See id*. at 142-46 (showing how executives argued for greater diversity because it was increase profits and would be good for business).

[266] *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, 1609-1621 (2001). *See also id*. at 1621 ("diversity 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.

[267] 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." *See* AuraPortal, *supra* note 262.

[268] *See, e.g.*, Timothy Morey, Theodore "Theo" Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

[269] *See, e.g.*, Operationalizing Privacy Tech—A Privacy Pro's Perspective, Web Conference, Apr. 13, 2017, *available at* https://iapp.org/store/webconferences/a0l1a000003gUuyAAE/;

[270] *See* Ann M. Cavoukian, Info. and Privacy Comm'r Report, Privacy by Design 4 (2009), *available at* https://www.ipc.on.ca/wp-content/uploads/Resources/PbDREport.pdf; *see also* Joel Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 772 (1999) ("Privacy is a critical issue for the growth of electronic commerce. ..... The fair treatment of personal information and citizen confidence in such treatment are necessary conditions for electronic commerce over the next decade.").

nevertheless shifted from what helps consumers to what helps corporations.

When that happens, vendors advance managerial, rather than substantive, privacy goals.[271] Corporate goals like 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.[272] Even though, as Julie Cohen and others have noted,[273] 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;[274] however, merely symbolic structures are often being used to advance management goals to the detriment of consumers.

5. Managerialization and the Perception of Compliance

---

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

[272] *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. 13 (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 choose 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) (noting the comments from industry that privacy regulation would increase costs and decrease profits).

[273] *See, e.g.*, 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).

[274] 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/; Chris, Pahl, *Getting Your Board on Board, Part III*, IAPP (Sept. 2, 2012), https://iapp.org/news/a/getting-your-board-on-board-part-iii/.

This happens because the use of managerial rhetoric around privacy and the proliferation of compliance structures influence 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—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[275] that, over time, no one bothers to look under the hood and see the house of cards holding it all up.[276] The effect is the frustration of consumer privacy rights because users assume the law can't help them.

This is already happening in privacy law. As Joe Turow has shown, we assume that websites with privacy policies actually protect our privacy,[277] even though a privacy policy is merely a statement of data use practices rather than a promise of confidentiality.[278] And, as Woodrow Hartzog has argued, 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.[279] 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."[280]

---

[275] *See* EDELMAN, *supra* note 18, at 154-55 (arguing that in employment discrimination context, the managerialization of civil rights law encouraged many social groups – from employees to judges—to perceive the mere presence of an anti-discrimination policy, for example, as proof that the company was following Title VII).

[276] John Meyer and Brian Rowan called this the "rationalized myth" of formal structures. *See* John W. Meyer & Brian Rowan, *Institutional Organizations: Formal Structure as Myth and Ceremony*, 83 AM. J. SOC. 340, 342 (1977).

[277] *See* Joseph Turow, Michael Hennessy, & Nora Draper, *Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003-2015*, 62 J. BROADCASTING & ELEC. MEDIA 461, 461 (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, at 3, Pew Res. Center (Nov. 25, 2014), http://www.pewresearch.org/wp-content/uploads/sites/9/2014/11/PI_Web-IQ_112514_PDF.pdf (making similar findings across age and educational groups).

[278] *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).

[279] *See* HARTZOG, *supra* note 74, at 62-63.

[280] *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.*, 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:*

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.[281] No wonder Facebook CEO Mark Zuckerberg talked about giving users more choices and more control 53 times during his 2018 testimony before the United States Senate.[282]

Admittedly, privacy technology vendors operate in an anti-consumer legal environment where rights mobilization is already difficult. Standing requirements[283] and other hurdles hamper privacy plaintiffs' use of tort law,[284] contract law,[285] and federal privacy statutes[286] to vindicate

---

The Paradox of Choice, *in* POSITIVE PSYCHOLOGY IN PRACTICE 86-88 (2004) (too much choice has negative consequences); Sheena S. Iyengar & Mark R. Lepper, *When Choice is Demotivating: Can One Desire Too Much of a Good Thing*, 79 J. PERSONALITY & SOC. PSYCH. 995 (2000) (using field and laboratory experiments showing consumers are more likely to make purchases given smaller sets of choices).

[281] 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 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).

[282] *See* Facebook, Social Media Privacy, and the Use and Abuse of Data, Hearing Before the Committee on the Judiciary and the Commerce, Science, and Transportation Committee (2018) (testimony of Mark Zuckerberg, CRO, Facebook, Inc.).

[283] *See* Spokeo v. Robins, 136 S. Ct. 1540 (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.").

[284] *See, e.g.*, Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. Ct. App. 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. __ (forthcoming 2019) (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).

[285] *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 (2016) (arguing that courts should consider intangible, but no less serious, harms when considering invasion of privacy claims and failing to do runs afoul of the common law).

[286] *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

their privacy rights. Even the FTC's power to force a company to overhaul its approach to privacy and security is under scrutiny.[287] Current law's consent paradigm imposes minimal obligations on technology companies while giving them ample opportunity to manipulate consumers by design.[288] 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.[289]

But privacy technology vendors exacerbate this problem, particularly through their focus on compliance paper trails. ComplianceLog offers support for crafting internal privacy rules, website privacy policies, and markets itself as helping companies "document what data you are in contact with" so companies can provide reports if investigated by the data protection authority.[290] And PossibleNow collects express consent, cookie consent, and other preferences and provides a "paper trail" to "ensure regulatory compliance" with the GDPR, CCPA, Do Not Call, and other privacy laws.[291] Granted, the GDPR includes documentation requirements;[292] companies need reports to prove they took "reasonable and appropriate" steps to protect consumer privacy under FTC consent decrees.[293] But the way some of these vendors conflate the

---

Electronic Communications Privacy Act because plaintiffs failed to demonstrate the requisite intent).

[287] *See, e.g.*, LabMD, Inc. v. Fed. Trade Comm'n, No. 16-16270 (6th Cir. June 6, 2018), slip op. at 30-31 (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).

[288] *See* HARTZOG, *supra* note 74, 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).

[289] *See, e.g.*, Thomas Friedman, *Four Words Going Bye-Bye*, N.Y. TIMES (May 21, 2014), https://www.nytimes.com/2014/05/21/opinion/friedman-four-words-going-bye-bye.html (declaring "privacy is over"); Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan 20, 2010), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy (quoting Mark Zuckerberg as saying the "age of privacy is over."); 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/ (quoting Scott McNealy, former chairman of Sun Microsystems).

[290] *See* ComplianceLog, 3 Month License to Compliancelog, https://www.compliancelog.dk/ (translated from German) (last visited Dec. 11, 2018).

[291] *See* Privacy Compliance, https://www.possiblenow.com/privacy-compliance.php (last visited Sept. 9, 2018).

[292] *See* GDPR, *supra* note 9, at art. 30, para. 1, at 50-51.

[293] *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief, at 10, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PGR (D. Ariz. filed Aug. 9, 2012), *available at* http://

structure of compliance (the records) with actual compliance (following the GDPR) is striking. The purpose of the GDPR's records requirement is to be able to demonstrate legal adherence to all of the GDPR's requirements; Article 30 is a means, not an end in itself.[294] Many vendors, however, see compliance records as the end goal, as demonstrated by how many market themselves as helping clients achieve GDPR compliance by preparing for audits. 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."[295] A demonstration of the product and its market positioning are almost entirely focused on "reducing the cost, time and effort required to prepare for audits."[296]

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*[297] on the incarceration of poor persons of color.[298] By focusing on a process right—the right the counsel—*Gideon*, Butler argues, obscured the "real crisis of indigent defense" that prison is designed for poor people and not rich ones.[299] 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. Butler concluded that "[o]n its face, the grant that *Gideon* provides poor people

---

www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (alleging that the hotel chain failed "to provide *reasonable* and *appropriate* security for the personal information [it] collected and maintained"). *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), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm (emphasis added) (explaining evolution of, and rationale for, FTC's consumer unfairness jurisdiction).

[294] Recital 82 of the GDPR, which expands on Article 30, states that the purpose of Article 30's records requirement is to "demonstrate compliance with this Regulation." *See* GDPR, *supra* note 9, at recital 82, at 16.

[295] *See* Compliance Point, See the Difference OnPoint Delivers, https://www.compliancepoint.com/onepoint (last visited Dec. 11, 2018).

[296] *Id*.

[297] 327 U.S. 335 (1963).

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

[299] *Id*. at 2178.

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."[300] 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 technology vendors focus on providing tools that help companies manage corporate risk under privacy laws, they focus on what is good for their client, not what the law requires in substance. Like the management lawyers Edelman research, many of whom recommended creating symbolic structures to make employers appear like they were doing their best to improve workplace equality,[301] some privacy technology vendors are selling their products 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.[302]

6. Deference to Symbols in Privacy Law

The legal endogeneity narrative comes full circle when, after becoming part of our collective consciousness about the law, merely symbolic structures are leveraged by lawyers, judges, and regulators as actual evidence of legal adherence.[303] There are three steps in this process: "reference, relevance, and deference."[304] Reference occurs where judges merely refer to symbolic structures in their decisions. The relevance stage occurs when judges find the presence of those structures relevant for answering a legal or factual question, like when a judge rules that having an internal dispute resolution process is relevant to whether a company complied with Title VII.[305] And deference, the final stage, occurs when

---

[300] *Id*. at 2191-92.

[301] *See* EDELMAN, *supra* note 18, at 163-64 (discussing the ways in which management lawyers "appear to be more concerned with impression management than with eliminating discrimination.").

[302] *Id*. at 165-67.

[303] *Id*. at 168 (discussing the definition of legal endogeneity and the stage of legal deference to symbolic compliance).

[304] *Id*. at 173.

[305] Importantly, Title VII of the Civil Rights Act prohibits workplace discrimination on 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 (2011)). It does not require internal dispute

judges see the mere presence of a compliance structure as dispositive.[306] 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.[307] It is, however, difficult to assess vendors' role in cementing legal endogeneity just yet because the need for third-party technology vendors to help companies comply with laws like the GDPR is so new.[308] And although many vendors market themselves as offering paper trails and required documentation that meet compliance standards, courts and regulators have not yet deferred to those products in any official or systematic way. But the process has begun.

Since the mid-1990s, the FTC has enforced a largely self-regulatory privacy regime,[309] which has allowed industry to set the terms of the debate. As a result, the FTC has deferred to industry practices when assessing whether individual companies have complied with the law. This is particularly true in the area of data security.[310] Companies will often promise that customer information is encrypted,[311] secured,[312] or adequately

---

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.

[306] *See* EDELMAN, *supra* note 18, at 173.

[307] *Id*. at 171-73.

[308] 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, European Data Protection Supervisor, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Dec. 12, 2018). 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.

[309] *See* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 593 (2007) (noting that "online privacy policies have appeared … as a voluntary measure by websites"); 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).

[310] *See* Solove & Hartzog, *supra* note 14, at 636.

[311] *See* Complaint for Permanent Injunction and Other Equitable Relief ¶ 43, FTC v. Rennert, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm.

[312] *See* In re Eli Lilly & Co., 133 F.T.C. 763 (2002) (complaint).

protected.[313] 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 State v. ValueClick*, for example, the FTC alleged that ValueClick "did not encrypt sensitive information consistent with industry standards."[314] And in *In re Eli Lilly & Company*, the FTC alleged that the company failed to use the "industry standard secure socket layer encryption."[315] Granted, industry custom has long been a yardstick by which the common law measured reasonable care.[316] But even customs have to be reasonable,[317] 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," it still speaks to the way in which regulated entities set the baseline on which they will be judged.

The FTC has also deferred 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.[318] In *FTC v. Toysmart.com*,[319] for example, the FTC noted that

---

[313] *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. filed Mar. 13, 2008) [hereinafter, ValueClick Complaint], *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317complaint.pdf

[314] *Id*. at 11.

[315] Eli Lilly, 133 F.T.C. at 765.

[316] *See, e.g.*, Trimarco v. Klein, 436 N.E.2d 502, 510 (N.Y. 1982) ("when 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 (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).

[317] *See* Trimarco, 436 N.E.2d at 511 (noting that industry custom can only set the standard of due care if the industry custom is itself reasonable).

[318] 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, In the Matter of True Ultimate Standards Everywhere, Inc, No. 1323219, at 4 [hereinafter, TRUSTe Complaint], *available at* https://www.ftc.gov/system/files/documents/cases/141117trustecmpt.pdf.

[319] First Amended Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. July 21, 2000) [hereinafter

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."[320] 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.[321]

The GDPR has incorporated industry structures, as well. Over the last two decades, an entire class of privacy professionals has emerged, first in the financial and health sectors, and later expending to other industries.[322] Today, 47,164 people on LinkedIn list "chief privacy officer," "deputy chief privacy officer," or other upper- or middle-management level privacy position as their current employment.[323] 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."[324] That is 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.[325]

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.[326] In this context, a symbolic structure like a seal or a CPO office could anchor an impression, later made official in a judicial

---

Toysmart.com Complaint], *available at* http://www.ftc.gov/sites/default/files/documents/cases/toysmartcomplaint.htm.

[320] *Id*. at ¶ 8.

[321] *See* Solove & Hartzog, *supra* note 14, at 593.

[322] *See* Bamberger & Mulligan, *supra* note 23, at 261.

[323] Based on a LinkedIn Premium Advanced Search filtered by "job titles" using the search terms "chief privacy officer" conducted on December 13, 2018. 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.

[324] *See* GDPR, *supra* note 9, at 55-56.

[325] *See* Waldman, *Designing Without Privacy*, *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).

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

decision or 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. Although products from technology vendors have yet to make their way into law either by reference or deference, the same anchoring effect could occur in the future.

C. The Risks of Outsourcing

For the most part, the IAPP sees the growth of privacy technology vendors as a positive development: privacy professionals "can now shop among dozens of vendors to find solutions to challenges created" by the GDPR and other laws.[327] But that speaks to the advantage of having many market participants, not the value and effectiveness of an industry where engineers make legal conclusions. Indeed, conceptualizing third-party technologies as solutions to legal compliance problems carries significant risks, some practical and some systemic.[328]

1. Practical Concerns

Privacy compliance technologies are often marketed to privacy professionals in need through persuasive, though not necessarily honest, advertising narratives. After reviewing every company and product in the IAPP's 2018 Privacy Tech Vendor Report, the disconnect between advertising and reality is clear: Almost 72% of vendors will, at some point, position their products and services as achieving GDPR compliance, generally,[329] and yet most are designed to meet only two or three of the GDPR's many requirements, if that. Indeed, not a single company even offers products that fit in each of the five categories of services described above.[330] Given uncertainty about the meaning of some GDPR requirements,[331] and the associated anxiety about the financial catastrophe

---

[327] *See* VENDOR REPORT, *supra* note 152, at 16.

[328] This list excludes some obvious risks associated with new technologies, including post-release bugs and failures, that may expose the company to even greater risk.

[329] Based on a review of websites of companies listed in the Tech Vendor Report. VENDOR REPORT, *supra* note 152, at 9-14.

[330] *See supra* Part II.B.2.b.

[331] *See, e.g.*, Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 17, 44 (2017) (arguing that it is not clear whether the GDPR includes a right to algorithmic explanation). *See also* 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.

of noncompliance,[332] privacy professionals, or the executives they support, may be uniquely susceptible to promises that vendors can make their troubles disappear. This makes leveraging the vendor market particularly risky for privacy professionals, especially where vendors are functionally reducing privacy law to its code-able pieces. Such underinclusive compliance technologies may then have the effect of increasing corporate exposure to administrative fines if in-house constituencies confuse purchasing a compliance technology that does a few things with actually solving a problem.

Clearly, though, not all in-house constituencies are the same. Outsourcing privacy compliance to third party technology vendors will also have an asymmetrical effect on industry. Outsourcing is often cheaper than building something internally, the latter of which requires in-house technical expertise, large salaries and benefits for new hires, and institutional time and capacity.[333] Companies like Microsoft can handle much of its compliance responsibilities in-house; in January 2019, the company started offering compliance support to customers.[334] Indeed, as the IAPP and TrustArc recently found, budgetary constraints likely explain why many companies have neither conducted nor hired anyone to help with data mapping, data inventories, or privacy impact assessments, despite GDPR requirements.[335]

Even for those companies in the technology vendor market, size and budget matter. Hiring vendors requires legwork: a clear set of goals, ongoing relationship maintenance, employee training, technology assessment, and integrating the technology into the company practice and routine.[336] Denise Farnsworth, Jazz Pharmaceuticals CPO, recommends first "go[ing] through the regulations and statutes that are relevant to your company, then you determine the thing you need to comply with" before

---

[332] *See* Paul Nemitz, *Fines Under the GDPR*, CPDP 2017 Conference Book, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3270535; *see also* PONEMON INST. & MCDERMOTT WILL & EMERY, THE RACE TO GDPR: A STUDY OF COMPANIES IN THE UNITED STATES AND EUROPE (Apr. 2018), https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf (reporting on a survey showing both significant lack of readiness for the GDPR and anxiety about fines).

[333] *See* VENDOR REPORT, *supra* note 152, at 18.

[334] *See* Liam Tung, *Struggling to Comply with GDPR? Microsoft 365 Rolls Out New Privacy Dashboards*, ZDNET (Jan. 30, 2019 7:37 AM), https://www.zdnet.com/article/struggling-to-comply-with-gdpr-microsoft-365-rolls-out-new-privacy-dashboards/.

[335] *See* MEASURING PRIVACY, *supra* note 178, at 7-8, 11 (reporting on results of survey of 496 privacy professionals).

[336] *See* VENDOR REPORT, *supra* note 152, at 16.

hiring a vendor.[337] Anick Fortin-Cousens, CPO of IBM Canada, notes that vendor management is "a big job for the vendor and for the purchasing company. Implementation involves a lot of back and forth. It's a real partnership and requires assigned resources on the part of the vendor and customer. We had daily and weekly interactions … ."[338] And once the vendor's product is up and running, there's more work to be done, including training and integrating the use of the product into the corporate culture.[339] All of that takes time and money, two things that small companies and start-ups don't have.

Larger companies can leverage internal expertise to conduct extensive due diligence, beta testing, and background research on potential vendors. They can leverage superior bargaining power to adapt vendor products to their interests. They can even buy the best products, leaving the rest of the market with inferior choices or just more expensive ones. And given that these technologies embody legal interpretations, the advantages of size and scale will allow large companies to build structures that frame the law in ways that benefit them, not their competitors and consumers.

2. Systemic Dangers

These concerns alone should give privacy professionals pause. But even more systemic dangers are looming. Outsourcing legal decisions to engineers is a threat to the role of expertise in society. Many technology vendors are coding their interpretations of legal requirements into their products, offering them as solutions to legal problems. That work often happens without lawyers.[340] Advanced Metadata, for example, makes much of its "20 years of experience in data science and information management," but all of its 3 employees are data analysts.[341] CipherCloud, which provides cloud-based data mapping, hosted a webinar in which its senior vice president of strategy and alliances and its vice president of marketing, neither of whom are privacy professionals nor privacy lawyers, claimed that the company's cloud-based tools can help "reach GDPR

---

[337] *Id*. at 19.

[338] *Id*. at 22.

[339] *Id*. at 25.

[340] *See* Waldman, *Designing Without Privacy*, *supra* note 24, at 694-96 (noting that lawyers are not involved in the design process at high technology companies).

[341] *See* Team, http://www.advancedmetadata.com/ (last visited Sept. 8, 2018).

compliance with four key capabilities."[342] That is a legal conclusion made by salespersons. Making legal conclusions without legal expertise, and burying those conclusions into code, not only risks making bad products. It also constitutes a threat to the legal and privacy professions by implicitly characterizing the skills of legal interpretation and implementation as routinizable, irrational, imperfect, or just too human.[343] As Frank Pasquale has argued, the notion that any engineer, entrepreneur, or businessperson can neatly code privacy law, and the human judgments and negotiations it demands, into a machine loses the "qualitative evaluation and … humble willingness to recalibrate and risk-adjust quantitative data" that come with human experts.[344]

It also only covers code-able parts of privacy law. Some privacy compliance technologies, therefore, embody an epistemic error: they assume that privacy law is reducible to factors that AI can identify. It isn't.[345] Privacy is about relationships,[346] obscurity,[347] affordances,[348] and

---

[342] *See* Navigate the GDPR with Four Key Capabilities, https://pages.ciphercloud.com/sap-successfactors-gpdr-emea-webinar-lp.html?utm_medium=ws&utm_source=direct&utm_campaign=sap-gdpr-webinar-ws-direct&utm_term=sap&utm_content=sap-gdpr-webinar (last visited Aug. 12, 2018).

[343] *See* ADAM GREENFIELD, RADICAL TECHNOLOGIES: THE DESIGN OF EVERYDAY LIFE 190-207 (2018); Frank Pasquale, *A Rule of Persons, Not Machines: The Limits of Legal Automation*, 87 GEO. WASH. L. REV. __, *20-23 (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135549 (challenging the view that contracts and legal provisions can be coded).

[344] *See* Frank Pasqaule, *Professional Judgment in an Era of Artificial Intelligence and Machine Learning*, at *2 (forthcoming 2019), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067711.

[345] Scholars recognize that not everything can be coded, especially when it comes to persons and data. *See, e.g.*, Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 19 THEORETICAL INQUIRIES L. __ (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081776 (recognizing that there are elements of the human self not computable); *see also* BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 29-34 (2018) (arguing that AI solutions to social problems transforms humans into mere "cogs" in the wheel); EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM (2014) (coining the frame "technological solutionism" to describe the approach, common in Silicon Valley, that everything has an engineering solution); JARON LANIER, YOU ARE NOT A GADGET (2011) (discussing the dehumanizing effects of solely technical solutions).

[346] *See* WALDMAN, *supra* note 104 (arguing that privacy is the expectations derived from social relationships based on trust).

[347] *See* Stutzman & Hartzog, *supra* note 214 (arguing that privacy exists even when personal information is technically available for others because the costs of gathering and analyzing that information keeps people obscure).

[348] Affordances are the capabilities and limitations that impact our ability to perceive our environment. For example, we perceive a mountain cliff as dangerous; a bird

contextual expectations,[349] not just paper trails and data maps. Even the best technology products cannot capture all of that.

By shifting the locus at which privacy law is negotiated from those trained in the law to those trained in technology, privacy technology vendors also change the discourse of power. The language we use shapes our understanding and perceptions of legitimacy, reality, and legality.[350] As Foucault argued, "discourse transmits and produces power."[351] Critical race theorists have made similar arguments about the power of speech.[352] As have feminist scholars.[353] Our social understanding of privacy is written and discussed in a variety of ways, sometimes conflicting, overlapping, and cacophonous.[354] But through the noise, the discourse is accessible to

---

perceives it as either irrelevant or a jumping off point. *See* Ryan Calo, *Privacy, Vulnerability, and Affordance*, 66 DEPAUL L. REV. 591, 602-3 (2017) ("As with other features of an environment, what privacy affordances exist varies by personal capacity. A cupboard may afford physical concealment to a child but not an adult. A famous person cannot rely on the anonymity of the crowd. … People of color may draw greater scrutiny by the surveillance state and hence have both a greater need for and lesser chance to privacy's affordances.").

[349] *See* NISSENBAUM, *supra* note 104 (arguing that perceptions of privacy are really about context-specific expectations about the proper flow of information).

[350] *See* THOMAS WARTENBERG, THE FORMS OF POWER 135 (1990) ("Power, in the form of discursive influence, can take place at the most basic level of the constitution of a human being's understanding of the world, it need not be limited to the restructuring of options already given to an agent."). *See also* 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).

[351] 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 attractive gave power and legitimacy to heteronormative thinking, institutions, and constituencies). *See also* Gerald Turkel, *Michel Foucault: Law, Power, and Knowledge*, 17 L. & SOC'Y REV. 170, 172 (1990) (describing Foucault's argument on "discourses of domination").

[352] *See, e.g.*, Charles R. Lawrence, *If He Hollers Let Him Go: Regulating Racist Speech on Campus*, 1990 DUKE L. J. 431, 444 (1990) ("racist 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").

[353] *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).

[354] *See* Solove, *supra* note 104, 14-36 (reviewing some of the many different definitions of privacy); *see* WALDMAN, *supra* note 104, 13-46 (grouping seemingly conflicting visions of privacy into negative and positive conceptions).

consumers: it's "creepy" when Alexa listens to everything we say,[355] "anonymity" protects people from the effects of revelation,[356] we want more "control" over our information,[357] and we "trust" our friends to keep our secrets.[358] Shifting that discourse into the language of technology—binary code, source code, "black box" algorithms[359] protected by trade secrecy,[360] emergent and intelligent machines[361]—empowers technologists as the new governors of society and the dictators of social control. In a world where technology vendors determine what the law requires and design those requirements into compliance tools, the discourse of law becomes the discourse of engineering. This disempowers consumers, who have no access to a technology-driven privacy discourse, and again serves to undermine the promise of privacy law as consumer protection.

---

[355] Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J. L. & TECH. 59, 61-70 (2013-2014) (describing situations where technologies functioned in ways users found "creepy").

[356] 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).

[357] *See* INNESS, *supra* note 104, at 56 (privacy is "control over a realm of intimacy"); WESTIN, *supra* note 104, 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 104, at 351 (privacy is making the choice to "control" and "manage" the boundary between ourselves and others).

[358] *See* WALDMAN, *supra* note 104, at 51-52 (noting that trust allows us to share because it creates expectations of confidentiality and adherence to norms).

[359] *See* FRANK PASQUALE, BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

[360] There is a growing literature on the role of trade secrecy in keeping algorithms hidden from users. *See, e.g.*, Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2017) (arguing that trade secrecy should not be privileged in criminal proceedings, especially where automated systems are being used to take away liberty); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 5 (2017) (algorithms are "shrouded in secrecy"). The arguments are being made in court. *See, e.g.*, State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

[361] Some scholars note that the discourse of AI is inherently hidden from us. *See, e.g.*, Maayan Perel & Niva Elkin-Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, 69 FLORIDA L. REV. 181, 186-90 (2017) (explaining why transparency would not help ordinary users understand automated decision making algorithms); *see also* Julie Brill, Former Comm'r, Fed. Trade Comm'n, Keynote Address Before Coalition for Networked Information 8-9 (Dec. 15, 2015), https://www.ftc.gov/system/files/documents/public_statements/895843/151216cnikeynote.pdf (former FTC Commissioner, Julie Brill, noting difficulties in making algorithms transparent, calling on companies to address fairness themselves).

Translating law through code also undermines due process. Privacy technologies embody particular visions of what privacy laws require. But the design process where that instantiation occurs is almost entirely hidden to us. Law, however, is traditionally interpreted out in the open, with explanations: legislative hearings are public records, legislative histories are integral to legal understanding, judicial opinions have explanations designed in, and every state and the federal government have open records laws that make the practice of policy open to the public. Moreover, law is normally characterized by procedural and substantive due process that safeguard its legitimacy.[362] As Danielle Citron has argued, the tendency to shift legal decisions to automated technologies erases these safeguards, leaving consumers unprotected.[363] The more we ask "black box" algorithms to implement the law, the more we undermine the project of public governance.[364]

III. Reclaiming Privacy Law's Promise

So far, in constructing a legal endogeneity narrative in privacy law, I have argued that ambiguity in data protection law has given those on the ground the opportunity to frame legal requirements in ways that advance corporate, rather than consumer, interests.[365] In particular, I have argued that engineers at third-party vendors are instantiating their own visions of what the law requires into technology products that offer data collectors compliance solutions, shifting the locus at which privacy law is negotiated

---

[362] The connection between due process and the legitimacy of law is a well-worn topic in the legal, political science, and philosophical literatures. *See, e.g.*, JOHN RAWLS, A THEORY OF JUSTICE 239 (1971) ("The 'rule of law' requires some form of due process"); *see also* R. George Wright, *The Fourteen Faces of Narrowness: How Courts Legitimize What They Do*, 31 LOY. L.A. L. REV. 167, 169-70 (1994) (due process is just the beginning of a process of legitimation of law); Goldberg v. Kelly, 397 U.S. 254, 270 (1970) ("Certain principles have remained relatively immutable in our jurisprudence. One of these is that where governmental action seriously injures an individual, and the reasonableness of the action depends on fact findings, the evidence used to prove the Government's case must be disclosed to the individual so that he has an opportunity to show that it is untrue.") (internal citations omitted).

[363] *See* Citron, *supra* note 28.

[364] *See, e.g.*, Houston Fed. of Teachers v. Houston Ind. Sch. Dist., 251 F. Supp. 3d 1168, 1180 (2017) (use of a proprietary algorithm to determine teacher hiring, contract renewal, and promotion gave teachers "no meaningful way to ensure correct calculation of their … scores, and as a result [we]re unfairly subject to mistaken deprivation of constitutionally protected property interests in their jobs.").

[365] *See supra* Part II.B.1.

far from legislative chambers and even CPOs offices.[366] 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.[367] 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.[368] Evidence of judicial and regulatory deference to symbolic structures is already spreading throughout privacy law.[369] And that is putting privacy protection and the rule of law at risk.[370] Taking action now may still allow us to reverse course.

Of course, privacy professionals should do their due diligence when hiring and working with vendors.[371] That goes without saying. And 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.[372] Similarly, changes in the exogenous legal context in which vendors operate and new approaches to the way they do their work and market themselves to privacy professionals may be able to rewrite the inchoate legal endogeneity narrative I have so far described.

A. Law Reform

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

---

[366] *See supra* Part II.B.2.b.

[367] *See supra* Parts II.B.3-II.B.5.

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

[369] *See supra* Part II.B.6.

[370] *See supra* Part II.C.

[371] *See* VENDOR REPORT, *supra* note 152, at 20-21 (discussing how privacy professionals should vet vendors).

[372] *See* Waldman, *Designing Without Privacy*, *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).

values in favor of corporate ones. In both systematic and specific ways, the law can do better.

We need to move away from transactional visions of privacy law that are susceptible to symbolic structures. Currently, almost all approaches to consumer data protection are based on a pared down version of the Fair Information Practices (FIPs), a set of privacy principles developed in 1973 by the Department of Housing, Education, and Welfare (HEW).[373] Although the HEW Report and a similar set of guidelines from the Organization for Economic Cooperation and Development (OECD) recommended that users be informed of data use practices, have the opportunity to correct their data, receive purpose and scope limitations on data collection, and consent to any secondary users of their information,[374] among other things, two of the recommendations—notice and consent—have become the backbone of international privacy law.[375] Even the GDPR, which has been called the most comprehensive data protection law in the world, is, at its core, a consent-based regime.[376]

But both notice, usually in the form of a privacy policy, and consent, often manifest in the boxes we click to accept terms of service or cookies, are flawed, and we ask too much of both.[377] We can neither

---

[373] U.S. DEP'T OF HEALTH, EDUCATION, AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973), http://www.epic.org/privacy/hew1973report/ [hereinafter "HEW REPORT"]. The Report was "the first portrait of information gathering and its impact on personal privacy ever provided by the U.S. government." ROBERT ELLIS SMITH, BEN FRANKLIN'S WEBSITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 327 (2000).

[374] *See* HEW REPORT, *supra* note 373, at 41-2; ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD), OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA at Part II (2001), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[375] *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 969-70 (2017) ("User interfaces can be designed to extract our 'consent' or to encourage us to disclose in ways that we do not even notice. ... Data that is collected with our consent can be leveraged against us.").

[376] *See* GDPR, *supra* note 9, art. 4, at 33 (consent must be freely given, specific, informed, unambiguous, clear, and affirmative); *see also id*. at art. 7, at 37 (laying out the conditions for consent). With user consent, many of the GDPR's restrictions on data collection and processing do not apply.

[377] *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Consent*, 96 WASH. U. L. REV. __ (forthcoming 2019). A long line of scholars has discussed the limited efficacy of a privacy regime based on consent and user control. To capture the best of those arguments, please see Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J. L. & POL'Y FOR INFO. SOC'Y 485, 490-96 (2015) (discussing the drawbacks

adequately process the information in a privacy policy[378] nor reasonably handle every button, click, box, and setting that is designed for us to relay our consents to data collection.[379] Moreover, their purely transactional nature, limited to posting documents and clicking buttons, make them uniquely susceptible to the tools of symbolic compliance by technology: it's easy to code in a button or toggle (even with haptics) to let users manifest consent. A legal regime based on notice and consent, therefore, falls into the morass of technological solutionism where opportunistic privacy compliance vendors are waiting.

Fortunately, we have other options. Woodrow Hartzog has called for leveraging contract, tort, and consumer protection law to regulate the design of new technologies.[380] Jonathan Zittrain, Jack Balkin, Dan 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.[381] A bill proposed at the end of the 115th Congress by Senator Brian Schatz of Hawaii reflected some of these

---

to notice and choice); *see also* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGY, AND PRACTICES 363–64 (Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, & Sabrina di Vimercati eds., 2008) (discussing how individuals make contextual choices rather than purely rational ones in information vacuums).

[378] *See* Reidenberg et al., *supra* note 229, at 40, 87-88.

[379] *See* Woodrow Hartzog, *The Case Against Idealizing Control*, 4 EUR. DATA PROTECTION L. REV. 423, 428-29 (2018) ("The problem with thinking of privacy as control is that if we are given our wish for more privacy, it means we are given so much control that we choke on it.").

[380] HARTZOG, *supra* note 74, at 120-56.

[381] *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 102–03 (2004) (positing that businesses that are collecting personal information from us should "stand in a fiduciary relationship with us"); 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."); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016, 9:48 AM), http://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/; Danielle Citron, *Big Data Brokers as Fiduciaries*, CONCURRING OPS. (June 19, 2012, 5:08 PM), http://www.concurringopinions.com/archives/2012/06/big-data-brokers-as-fiduciaries.html (a fiduciary relationship between data brokers and users would help fight the massive power imbalance that exists in today's unregulated environment).

ideas.[382] This is not to say that these proposals, if adopted, could not 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.

Greater specificity in other aspects of the law would help combat the legal endogeneity narrative, as well. The United Kingdom's Information Commissioner's Office (UKICO) has issued guidance documents that give specific examples of the types of designs that meet GDPR legal standards. For example, to meet the consent requirements of Article 7, the UKICO 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."[383] The United States lacks a similar resource for specificity.[384] is why the FTC 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.[385] However, the FTC is limited by the "procedurally burdensome" process of Magnuson-Moss rulemaking,[386] which requires the FTC to conduct

---

[382] S. __, 115th Cong., 2d sess., A Bill to Establish Duties for Online Service Providers with Respect to End User Data That Such Providers Collect and Use, *available at* https://www.schatz.senate.gov/imo/media/doc/Data%20Care%20Act%20of%202018.pdf.

[383] *See* What Is Valid Consent, UKICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ (last visited Dec. 20, 2018).

[384] Granted, the California Attorney-General's office has issued interpretive guidance with respect to state law, but that has limited reach. *See, e.g.*, 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.

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

[386] *See* 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. For example, the Act introduced direct Congressional oversight. And the law explicitly prohibited the FTC from using funds for 3 years "for the purpose of initiating any new rulemaking proceeding … which prohibits or otherwise regulates any commercial advertising." HOOFNAGLE, *supra* note 14, at 65 (*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-

industry-wide investigations, prepare reports, propose rules, engage in a series of public hearings, and consider other alternatives.[387] The process is so difficult that the FTC has not engaged in it in 37 years.[388] This lack of rulemaking authority ensures that, without more, privacy regulation from the FTC will remain vague. And, as Citron has noted, the FTC is also reluctant to issue specific closing letters on their investigations.[389] The only other way to discern what the FTC means by a specific term or phrase is to turn to its previous consent decrees, which is what many practitioners do.[390] 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.

On a more granular level, the FTC must be more active vendor regulators. Its first investigation into the vendor market, a suit alleging that TRUSTe failed, despite its promises, to annually recertify companies that earned one of the vendor's sought-after privacy seals, shows how vendors can manipulate consumers.[391] But like so many of the FTC's investigations, the action against TRUSTe was just another chapter in the Commission's limited broken promises jurisprudence.[392] Privacy technology vendors are not breaking promises to users; rather, some are subverting user expectations of data protection by undermining privacy law.[393] To the

---

Leach-Bliley Act. *See* A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, at app. C, FTC (July 2008), http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority ("Special Statutes that mandate or authorize Commission rulemakings either antitrust and/or consumer protection related … include the Graham-Leach-Bliley Act … [and] COPPA ….").

[387] FTC, Rulemaking: Operating Manual, Chapter Seven, http://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf (last visited Dec. 21, 2018) (describing rulemaking procedures).

[388] *See* Solove & Hartzog, *supra* note 14, at 620 n. 176.

[389] *See* Citron, *supra* note 39, at 760.

[390] *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.").

[391] *See* TRUSTe Complaint, *supra* note 318.

[392] *See* Solove & Hartzog, *supra* note 14, at 629-30 (describing how much of the FTC's privacy investigations have been related to companies lying on their privacy policies).

[393] *Id*. at 590 (recommending the FTC focus on protecting consumer expectations rather than merely regulating lying).

extent that vendors mislead their clients about their compliance capabilities and ultimately deceive end users about how their privacy is protected, the FTC has statutory authority to rein in the industry.[394]

FTC audits must also be more effective. Securities regulation may provide a helpful model. 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.[395] The committee serves as a check on nefarious financial reporting and is charged with the "appointment, compensation, and oversight" of the company's independent auditor.[396] The committee must include at least one financial expert and have a mechanism for anonymously reporting questionable accounting.[397] 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.[398] Sarbanes-Oxley also requires executives to sign financial statements, ensuring greater involvement and establishing a sense of personal responsibility for honesty.[399] 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.[400] As discussed earlier, many companies subject to FTC consent decrees fulfil their audit requirements with assessments or attestations, without any deep, independent investigation.[401] Sarbanes-Oxley style rules governing both audit committees and independent audits

---

[394] *Id*. at 667-76 (suggesting a broader focus on user expectations through various tools).

[395] *See* Sarbanes-Oxley Act of 2002 § 301, 15 U.S.C. §78j-1 (Supp. III 2003), Pub. L. 107-204, 116 Stat. 745 (2002); SEC Listing Standards Relating to Audit Committees, 17 C.F.R. §240.10A-3 (2005); SEC Standards Relating to Listed Company Auditing Requirements, 68 Fed. Reg. 18,788 (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.

[396] *See* Sarbanes-Oxley Act, § 301.

[397] *Id*. at §§ 301, 407.

[398] *See* Craig Clay & Daniel Kim, *Sarbanes-Oxley: 16 Years of Successes and Challenges*, ACCOUNTING TODAY (Sept. 15, 2017 4:31 PM), https://www.accountingtoday.com/opinion/sarbanes-oxley-marks-15-years-of-successes-and-challenges.

[399] *See* Sarbanes-Oxley Act, § 302; 17 C.F.R. §§ 228.

[400] *See* MEASURING PRIVACY, *supra* note 178, at 10 (noting many privacy departments are seen as cost centers).

[401] *See supra* notes 124-127 and 241-249 and accompanying text.

themselves would both ensure greater adherence to the law and prevent the managerialization of privacy audits. Requiring executives to sign off on privacy audits could also have a sufficient motivating effect to take privacy seriously.

B. New Approaches for Privacy Technology Vendors

Outsourced technologies can still play important roles in the privacy law ecosystem by providing companies with the information they need to comply with the law. Information resource companies do not make legal conclusions, and when they do provide information about the law, they do so with experts in privacy law. Privacy professionals report great demand for these kinds of products, noting that compliance is impossible without knowing what data they have and without knowing what the law requires.[402]

This market includes TeachPrivacy,[403] a training service for privacy professionals run by privacy law scholar Daniel Solove, that helps those on the ground do their jobs by providing accounts of relevant laws and describing industry best practices. TeachPrivacy offers 123 courses—some as short as 2-5 minute—on a range of topics, including a "Privacy Awareness Complete Training Program," "The Lifecycle of Personal Data," and series of courses on the Health Information Privacy and Accountability Act (HIPAA).[404] Solove is also an active blogger, writing explanatory pieces as an influencer on LinkedIn, and a well-regarded scholar.

DataGuidance markets itself as a privacy information provider, as well.[405] Its platform summarizes new privacy regulations and creates comparison charts that allow clients to see privacy laws across the world, learn what they need to do to comply, and print out the relevant documents.[406] In-house privacy analysts work with "over 400 privacy

---

[402] VENDOR REPORT, *supra* note 152, at 9-14.

[403] TeachPrivacy was founded by a leading privacy scholar, Dan Solove, and "provides privacy and security training by the leading subject-matter expert … that is engaging, memorable, and understandable. *See* TeachPrivacy, https://teachprivacy.com/ (last visited Sept. 1, 2018).

[404] *See* TeachPrivacy, Training Course Pages, https://teachprivacy.com/privacysecurity-training-course-pages-2/ (last visited Sept. 7, 2018).

[405] Research, DataGuidance, https://www.dataguidance.com/ (last visited Dec. 28, 2018).

[406] Interview with Miltiadis Tsartsidis, International Business Executive, Data Guidance, Washington, D.C. (Feb. 27, 2018) (notes on file with Author); *see also* Global

experts"[407] globally to provide clients with these regulatory updates, explanations, webinars, and videos on specific areas of privacy law.[408] In doing so, DataGuidance fills an important role in the privacy compliance ecosystem: it does not handle compliance for any of its clients, but offers them the tools to do so.

BigID is a data tool that scans all the information a company has and identifies personal information.[409] As noted earlier, this may require engineers to identify what does and does not constitute "personal information," but BigID addresses this problem in two ways. Its leading privacy professional, Debra Farber, is a privacy lawyer and directly involved in the design of the product.[410] In addition, a demonstration of the product shows that the platform allows the business user to determine what information constitutes "personal information" under the law. The tool creates a map that the client can adjust and specify based on her needs and the client's, not BigID's, interpretation of the applicable law.[411] That may not automatically solve the problem of interpretive mistakes, but it does avoid the engineerization of legal conclusions.

In occupying more modest approaches than promising compliance with the GDPR, the CCPA, HIPAA, or any number of privacy laws, information providers like TeachPrivacy, DataGuidance, and BigID do not run the risk of promising too much or providing underinclusive solutions that pose risks to their clients. They also do their work with lawyers at the helm. And, as DataGuidance recognizes, the inclusion of legal experts helps inspire user "trust" and "confidence,"[412] and, as such, may provide a competitive advantage in a crowded market.

But the privacy compliance market is not closed to technology vendors, including start-ups, which may not be able to afford full- or part-time legal expertise. Aircloak, for example, is a Berlin-based start-up with

---

Privacy Compliance Solutions, DataGuidance, https://www.dataguidance.com/solutions/ (last visited Dec. 28, 2018).

[407] Experts, DataGuidance, https://www.dataguidance.com/experts/contributors/africa/ (last visited Dec. 28, 2018).

[408] Tsartsidis interview, *supra* note 406.

[409] Advanced PII/PI Discovery, BigID, https://bigid.com/ (last visited Dec. 28, 2018).

[410] Telephone interview with Debra Farber, Senior Director, Privacy Strategy, BigID (TBD) (notes on file with author).

[411] Online product demonstration, BigID (Dec. 31, 2018) (notes on file with author).

[412] *See* Experts, DataGuidance, *supra* note 407.

only 7 employees,[413] none of whom are lawyers.[414] It markets itself as the "first GDPR-grade anonymisation solution" that can provide "instant privacy compliance."[415] In other words, it promises that its anonymization tool will help companies avoid GDPR restrictions by creating truly anonymous data. That's a legal conclusion made by technologists.[416] To address any concern about its product, Aircloak took a three-pronged approach. It launched a worldwide "bug bounty" program that challenged technology experts to attack the system and identify any single user in the anonymized data set.[417] After 33 million attacks, 2 groups found pieces of identifying information, which allowed Aircloak to rewrite its code to fix the problem.[418] Aircloak is also working with the Max Planck Institute for Software Systems[419] to apply a General Data Score to measure the level of anonymity of a data set.[420] Perhaps most importantly, the Aircloak team worked with the Commission Nationale de L'informatique et des Libertés (CNIL), the French data protection authority, and determined that the company's anonymization tool complied with the 3-part anonymization standard laid out in the Article 29 Working Party's Working Paper 216.[421] In fact, even though there is no official certification system for anonymization tools, CNIL is willing to work with any technology vendor,

---

[413] *See* VENDOR REPORT, *supra* note 152, at 29.

[414] Telephone interview with Felix Bauer, CEO and Managing Director, Aircloak (Dec. 21, 2018) (notes on file with author).

[415] *See* Aircloak, https://aircloak.com/ (last visited Dec. 5, 2018).

[416] Mr. Bauer studied at the University of Cambridge and the Max Planck Institute for Software Systems in Germany. Sebastian Probst Eide, Aircloak CTO is a computer scientist who studied at Cambridge and previously worked at Google. *See* Aircloak Founders, About Us, https://aircloak.com/company/about-us/ (last visited Dec. 28, 2018).

[417] Aircloak Attach Challenge, https://aircloak.com/solutions/attack-challenge-en/ (last visited Dec. 28, 2018).

[418] Bauer interview, *supra* note 414.

[419] The Max Planck Institute is a research institution in Munich, Germany that conducts research in natural sciences, life sciences, and the humanities. *See* Max-Planck-Gesellschaft, Profile and Vision, https://www.mpg.de/11761628/profile-visions (last visited Dec. 28, 2018).

[420] Bauer interview, *supra* note 414.

[421] Art. 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques 3 (Apr. 10, 2014), *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (requiring anonymization tools be assessed based on three criteria: "(i) is it still possible to single out an individual, (ii) is it still possible to link records relating to an individual, and (iii) can information be inferred concerning an individual?").

even without a specific use case, to discuss compliance with the GDPR.[422] And, according to Aircloak, it does this for free.[423] Similarly, Anonos's BigPrivacy tool is certified by the EU Data Protection Board, formerly the Article 29 Working Party, as meeting anonymization requirements under the GDPR. [424]

Hiring in-house attorneys and privacy professionals and, critically, involving them in the design process of privacy compliance technologies,[425] may enhance the credibility of vendor products. But it is also expensive. And restricting vendors to just providing information may seem too narrow and unrealistic. If privacy technology vendors would like to venture into the compliance marketplace and guarantee that their products meet legal requirements, working with regulators may be an optimal approach. Alongside changes in law, these strategies may help keep the discourse of privacy compliance closer to where it should be: among the lawyers and policymakers directly involved in building and implementing pro-consumer privacy laws in the first place.

C. Responses to Objections

In highlighting the risks of legal endogeneity posed by some privacy technology vendors, I have argued for changes in the legal status quo, more modest approaches from vendors, a focus on providing information rather than guaranteeing compliance, hiring lawyers and privacy professionals, and close relationships with regulators who can certify that technologies meet legal standards. These arguments have engendered several objections, some of which I address here.

Some might argue that the legal endogeneity narrative described in this article is more a systemic problem with compliance culture rather than a problem unique to privacy. That is both 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

---

[422] Telephone interview with CNIL Helpline, +33 (0)1.53.73.22.22 (Dec. 20, 2018) (notes on file with author).

[423] Bauer interview, *supra* note 414.

[424] *See* Telephone interview with Steve LeFever, CEO, Anonos, Dec. 6, 2018 (notes on file author).

[425] *See* Waldman, *Designing Without Privacy*, *supra* note 24, at 714-16 (noting the importance of integrating lawyers into the design process to help spot privacy issues as they come up).

"their professional training and roles,"[426] 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."[427] These are problems 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 privacy law. 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,[428] the exogenous legal system sees itself less competent to intercede and decide difficult questions for itself.[429] Moreover, privacy law's series of flexible and sometimes ambiguous standards make even incomplete heuristics extraordinarily attractive.[430] Relying on simple, underinclusive rules is easier, faster, and a convenient process-oriented way to adjudicate cases, while opening up courts to errors.[431]

---

[426] EDELMAN, *supra* note 18, at 31.

[427] *Id*. at 82.

[428] 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 HUMAN FACTORS 407, 409-28 (2015) (collecting the literature on trust in automation and technology).

[429] This phenomenon exists in other areas of the law, not just in privacy. *See, e.g.*, NEIL K. KOMISAR, LAW'S LIMITS: THE RULE OF LAW AND THE SUPPLY AND DEMAND OF RIGHTS 22 (2001) ("courts fail … when '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 qualitative different than *Chevron* deference, where it is appropriate and expected for judges to defer to agency experts. *See* Chevron U.S.A. Inc. v. Natural 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").

[430] Heuristics can be important in decision-making, especially given humans' bounded rationality. *See* MAX BAZERMAN, JUDGMENT IN MANAGERIAL DECISION MAKING 5 (4th ed. 1998) (noting that "the systematic and time-consuming demands of rational decision making are simply not viable. … [Instead] people rely on a number of simplifying strategies … called heuristics. … They serve as a mechanism for coping with the complex environment surrounding our decisions. In general, heuristics are helpful, but their use can sometimes lead to severe errors.").

[431] *See, e.g.*, Stephen M. Bainbridge & G. Mitu Gulati, *How do Judges Maximize? (The Same Way Everybody Else Does – Boundedly): Rules of Thumb in Securities Fraud Opinions*, 51

Others may argue that this Article's argument is misdirected. When Edelman described legal endogeneity in the employment discrimination context, she focused on the work of compliance professionals and lawyers in building merely symbolic structures that frustrated the civil rights of employees.[432] The equivalent players in the privacy market are not technology vendors, on which I have focused, but privacy professionals and lawyers, both at firms and in house. Undoubtedly, privacy professionals and lawyers aiming to do the least necessary to comply with the law in name only can contribute to legal endogeneity and the erosion of privacy law's effectiveness. But many professionals are active advocates for privacy within their organizations,[433] and even when they are, the technological solutionism of some technology vendors can undermine their efforts. Focusing on that space is, therefore, warranted and overdue.

Finally, technology vendors may argue that my argument and its correlative proposals may stifle innovation in an active marketplace where there is great demand. There is indeed great demand.[434] But creativity and innovative thinking often thrive within constraint.[435] And even if that were not the case, I am unwilling to surrender to the intellectual hegemony of innovation. Not all innovation is good innovation. Companies that develop shoddy products may lose out in the market in the long term, but in the short and medium term, they risk putting millions of persons' data at risk. Besides, the legal changes and vendor recommendations in this Article are meant to help vendors do their jobs better, and help data collectors adequately and substantively comply with privacy laws as they are.

Conclusion

A booming market of technology vendors is practicing privacy law. They develop their own vision of what the law requires and instantiate it into the code of technology products that promise compliance with the law. Taking a ground-up, analytical approach, this Article used a variety of methods to highlight the impact of third-party technology vendors on

---

EMORY L.J. 83, 118-36 (2002) (describing flawed decision-making heuristics in securities fraud cases).

[432] EDELMAN, *supra* note 18, at 77-82.

[433] BAMBERGER & MULLIGAN, *supra* note 23, at 66-68.

[434] *See* MEASURING PRIVACY, *supra* note 178, at 2 (noting that many companies are investing in technologies to help them comply with privacy laws).

[435] *See, e.g.*, Joseph P. Fishman, *Creating Around Copyright*, 128 HARV. L. REV. 1333 (2015) (the constraints imposed by copyright law promote the creativity of subsequent authors).

privacy compliance, including primary source research, qualitative interviews, product demonstrations, review of industry literature, webinars, blogs, and research on every vendor identified by the IAPP. As this article has attempted to show, these vendors are contributing to a process of what Lauren Edelman has 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 from law to technology, all to the detriment of consumer privacy.

It is important to note what this article is not arguing. It does not argue that all technology vendors 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 privacy technology vendors is both significant and underexplored. This article has endeavored to demonstrate the former while addressing the latter, filling a gap in the legal, sociological, and interdisciplinary privacy literatures.

But more work needs to be done. Future research will situate 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 privacy law inside and outside technology companies. 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 third-party technology vendors highlights a creeping problem of both private and public governance—faith in technology to solve problems—that requires significantly more scholarly attention. Privacy laws are not the only social responses to social problems that inspire both private and public sector organizations to reach for new artificial intelligence tools to make their problems go away. The more that happens, however, the more we run the risk of undermining both the progressive project of legitimate governance and the Enlightenment commitment to human dignity. Stopping the erosion of privacy law is a first step. Even harder work comes next.