

2018

# Designing Without Privacy

Ari Ezra Waldman

# ARTICLE

## DESIGNING WITHOUT PRIVACY

*Ari Ezra Waldman*[*]

ABSTRACT

In *Privacy on the Ground*, the law and information scholars Kenneth Bamberger and Deirdre Mulligan showed that empowered chief privacy officers (CPOs) are pushing their companies to take consumer privacy seriously by integrating privacy into the designs of new technologies. Their work was just the beginning of a larger research agenda. CPOs may set policies at the top, but they alone cannot embed robust privacy norms into the corporate ethos, practice, and routine. As such, if we want the mobile apps, websites, robots, and smart devices we use to respect our privacy, we need to institutionalize privacy throughout the

* Associate Professor of Law and Director, Innovation Center for Law and Technology, New York Law School. Affiliate Scholar, Princeton University, Center for Information Technology Policy. Ph.D., Columbia University; J.D., Harvard Law School. This Article won the International Association of Privacy Professionals Best Paper Award at the 2017 Privacy Law Scholars Conference (PLSC) in Berkeley, California. Special thanks to B.J. Ard, Jack Balkin, Kenneth Bamberger, Ann Bartow, Jacqueline Beauchere, Franziska Boehm, Jill Bronfman, Stuart Brotman, Ryan Calo, Danielle Keats Citron, Ignacio Cofone, Julie Cohen, Rebecca Crootof, Mary Culnan, Deven Desai, Amit Elazari, Tonya Evans, Roger Ford, Brett Frischmann, Sue Glueck, Seda Gurses, Woodrow Hartzog, Chris Jay Hoofnagle, Kristy Hughes, Ian Kerr, Cameron Kerry, Anita Krishnakumar, Irina Manta, Bill McGeveren, Deirdre Milligan, Joe Miller, Paul Ohm, W. Nicholson Price, Helen Nissenbaum, Priscilla Regan, Joel Reidenberg, Neil Richards, Alexandra Roberts, Ira Rubinstein, Rachel Sachs, Andres Sawicki, Paul Schwartz, Victoria Schwartz, Jeremy Sheff, Jessica Silbey, Daniel J. Solove, Luke Stark, Eva Subotnik, Harry Surden, Joseph Turow, Ryan Vacca, Josh Whitford, and Aaron Wright. This Article benefited greatly from the comments and suggestions of participants at several conferences and workshops, including the 2017 Privacy Law Scholars Conference, the St. John's University School of Law Faculty Colloquium, the UCLA School of Law Faculty Colloquium, the Intellectual Property Scholars Conference at Stanford Law School, the University of New Hampshire IP Roundtable, and the Yale Information Society Project Ideas Lunch at Yale Law School. Thank you to all conference participants for their questions, comments, and important feedback. Special thanks to Kenneth Bamberger and Deirdre Mulligan for blazing a rich and important research path. I stand on their shoulders. All errors are, of course, my own.

corporations that make them. In particular, privacy must be a priority among those actually doing the work of design on the ground—namely, engineers, computer programmers, and other technologists.

This Article presents the initial findings from an ethnographic study of how, if at all, those designing technology products think about privacy, integrate privacy into their work, and consider user needs in the design process. It also looks at how attorneys at private firms draft privacy notices for their clients and interact with designers. Based on these findings, this Article suggests that Bamberger's and Mulligan's narrative is not yet fully realized. The account among some engineers and lawyers, where privacy is narrow, limited, and barely factoring into design, may help explain why so many products seem to ignore our privacy expectations. The Article then proposes a framework for understanding how factors both exogenous (theory and law) and endogenous (corporate structure and individual cognitive frames and experience) to the corporation prevent the CPOs' robust privacy norms from diffusing throughout technology companies and the industry as a whole. This framework also helps suggest how specific reforms at every level—theory, law, organization, and individual experience—can incentivize companies to take privacy seriously, enhance organizational learning, and eliminate the cognitive biases that lead to discrimination in design.

TABLE OF CONTENTS

## I. INTRODUCTION

In *Privacy on the Ground*, Kenneth Bamberger and Deirdre Mulligan showed that empowered chief privacy officers (CPOs) are creating strong data protection policies that put users and user trust first.[1] Their research opened our eyes to the fact that American privacy law today is more than just statutes,[2] Federal Trade Commission (FTC) enforcement actions,[3] and the litigation and policymaking of state attorneys general.[4] Rather, where the laws on the books remain as fragmented and incomplete as ever, corporate CPOs are going further, filling in gaps on the ground.[5]

---

1. KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 6 (2015) [hereinafter BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND]. Bamberger and Mulligan also published their initial research and preliminary arguments in the Stanford Law Review. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011) [hereinafter Bamberger & Mulligan, *Privacy on the Books*]. This Article pulls from both sources.

2. State privacy laws are too numerous to list. Federal privacy laws include, but are not limited to, the Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681 et seq. (credit histories), the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §§ 1221, 1232g (school records), the Privacy Act of 1974, 5 U.S.C. § 552a (personal information maintain by government), the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709 (protection against federal surveillance and electronic searches), and the Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710–2711 (video rentals), among many others. For a more comprehensive list, please see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 37–39 (4th ed. 2011).

3. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 135–305 (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 627–28 (2014).

4. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 758 (2017). Bamberger and Mulligan's research was international in scope; they interviewed CPOs from the United States and several countries in Europe. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 6. They found that American (and German) CPOs expressed a robust, user-focused and trust-based vision of privacy. *Id.* at 6–7. Because that narrative existed in the United States and seemed counterintuitive given the many gaps in U.S. privacy law on the books, this Article focuses exclusively on U.S.-based technologists and lawyers and makes recommendations for changes to U.S. law and corporate organization. *Id.* at 6.

5. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 6.

Their research, which is described in Part II, changed the privacy law discussion: previously, privacy scholarship mostly ignored the contributions of privacy professionals.[6] But their work raises additional research questions. Have the CPOs' efforts been fully realized? Are these robust, user-focused privacy norms embedded throughout the technology industry? And, are these norms being integrated into technology product design?

Bamberger and Mulligan argued that American CPOs are taking advantage of gaps in U.S. privacy law to innovate and solve problems creatively, adopting a far more user-friendly approach to their companies' data privacy obligations than the law on the books would seem to require.[7] But that user-friendly approach does not always make its way into design; Snapchat,[8] the initial version of Pokémon Go,[9] and Uber's mobile app,[10] among others, seem to have been designed without our privacy in mind. In these cases, any "company law" of privacy is not being operationalized on the ground.

This Article explores that divergence, some of the reasons for it, and how to fix it. CPOs may set policies at the top, and they may have the ears of corporate executives,[11] but they alone cannot embed robust privacy norms into the corporate ethos, practice, and routine. Nor do they design the very data hungry products that scream out for privacy protection. There are other people involved. Engineers, coders, and other technologists create the platforms and products that sweep in user data. Attorneys work with their corporate clients to turn internal data use practices into privacy policies. A phalanx of product managers shepherd concepts from beginning to end. For a CPO's vision of privacy to make its way into her company's products, these workers have to implement it. As such, any narrative of privacy on the ground cannot stop with

---

6. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 249.

7. *Id.* at 250–51, 304–05. Their research was international in scope. They found that German and American CPOs were able to innovate in ways their counterparts in other countries could not. *Id.* at 6–7. I focus on the domestic side of their work because my ethnographic research was restricted to the United States.

8. Complaint, *In the Matter of Snapchat, Inc.*, FTC File No. 132 3078, Docket No. C-4501 (F.T.C. May 8, 2014) [hereinafter, Snapchat Complaint], *available at* https://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf.

9. *See* Laura Hudson, *How to Protect Privacy While Using Pokémon Go and Other Apps*, N.Y. TIMES (July 12, 2016), http://www.nytimes.com/2016/07/14/technology/personaltech/how-to-protect-privacy-while-using-pokemon-go-and-other-apps.html?_r=0.

10. *See* Lily Hay Newman, *Uber Didn't Track Users Who Deleted the App, but it Still Broke the Rules*, WIRED (Apr. 24, 2017 6:58 PM), https://www.wired.com/2017/04/uber-didnt-track-users-deleted-app-still-broke-rules/ (discussing the Uber app's use of fingerprinting to identify users even after they have deleted the app from their phones).

11. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 12.

CPOs.[12] If we want the mobile apps, websites, robots, and smart devices we use to respect our privacy, we need to institutionalize robust privacy norms throughout the corporations that make them, including among those designing the products we use every day.

What follows are the preliminary and partial results[13] of an interdisciplinary study about the ways some designers and lawyers think about privacy and the factors that prevent—and those that foster—the institutionalization of robust privacy norms throughout a corporation. Relying on scholarship on management structure, the sociology of organizations, and my own field research in the form of semi-structured interviews and observations of product development, this Article makes three arguments. First, the designers and lawyers I interviewed think about user privacy narrowly and in starkly different terms than the CPOs in Bamberger and Mulligan's study.[14] Second, it is the designer's vision of privacy that is operationalized into the products they create because they are the ones tasked with design. Third, factors both exogenous and endogenous to the corporation hinder the diffusion of robust privacy norms. Those factors are ambiguous privacy theory, lax U.S. legal approaches to privacy, siloed organizational structure, and isolated and homogeneous design teams. Changes in those four areas can provide the necessary incentives, enhance organizational learning, and help embed strong privacy norms throughout a company. In short, this Article suggests that a robust, user-focused vision of privacy can only translate into design if the designers are on board.

The interviews on which this Article is based focused on technologists and lawyers in the high technology sector, including those working at leading technology companies, mobile apps, and tech start-ups. Many of them had similar views on privacy, the role of the user, and design. At the same time, their views were

12. *Id.* at 83.

13. This Article is part of a larger research project on the role played by engineers, lawyers, marketing professionals, venture capitalists, and other workers in considering privacy protections and privacy principles in design. Interviews with these research subjects is ongoing. This Article focuses exclusively on interviews with engineers and coders designing technology products and lawyers who work on privacy notices. Future research will consider the broader population of workers on the ground.

14. This conclusion is not surprising, though this Article is the first to describe technologists' vision of privacy and how that vision factors into design. In the intellectual property context, at least, there is evidence to suggest that creative actors tend to think about their work, process, and goals differently than those who make laws and policies about creative artifacts. *See* JESSICA SILBEY, THE EUREKA MYTH: CREATORS, INNOVATORS, AND EVERYDAY INTELLECTUAL PROPERTY 9 (2015).

remarkably different from the views of the CPOs in Bamberger and Mulligan's study. To many, "information privacy" boiled down to giving users notice, much like privacy law on the books.[15] Many thought privacy was synonymous with encryption: that is, internal security priorities crowded out any consumer-focused privacy concerns. Few engineers remembered meeting with lawyers or privacy professionals one-on-one to discuss integrating privacy considerations into their work; some attended short assemblies on security, generally. Many found it difficult to design with user needs in mind; therefore, engineer-only design teams not only minimized the importance of privacy, but also missed how their designs impacted consumers.[16] This research, discussed in more detail in Part III, suggests that, at least among most of the interviewees, Bamberger and Mulligan's narrative about privacy has not yet been fully realized.

There could be many explanations for this divergence of views. Part IV proposes a framework for understanding how factors exogenous (theory and law) and endogenous (corporate organization and employee experiences) to the corporation are hindering norm diffusion. Fortunately, changes in all four of these areas can help fully realize the more robust privacy norms from *Privacy on the Ground*.

As a matter of privacy theory, the dominant rights-based notion of privacy, or the idea that privacy is about giving users choice and control over the dissemination of their data, reduces corporate privacy obligations to posting privacy policies. Any ambiguity as to how to conceptualize privacy among those that recognize that privacy can mean different things to different people at different times makes it difficult for practitioners on the ground to turn theory into practice.[17] However, conceptualizing privacy as based on relationships of trust would not only ground the CPOs' vision of privacy with theoretical rigor, but also create a robust privacy-as-trust discourse to compete with the governing autonomy- and rights-based notions of privacy.[18]

---

15. Telephone interview with former engineer at LinkedIn (Oct. 5, 2016) (notes on file with Author).

16. *See* Steve Woolgar, *Configuring the User: The Case of Usability Trials*, *in* A SOCIOLOGY OF MONSTERS: ESSAYS ON POWER, TECHNOLOGY AND DOMINATION 70–74 (John Law ed., 1991) (noting users are constrained and "configured" by designs of new technologies).

17. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1090 (2002) ("The difficulty in articulating what privacy is and why it is important has often made privacy law ineffective and blind to the larger purposes for which it must serve.").

18. *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 11–45 (2018); Neil Richards & Woodrow Hartzog, *Taking Trust*

Law has a significant role to play, as well. Sectoral federal laws and the autonomy-based notion that users only need notice of data use practices in order to make disclosure decisions[19] provide little incentive for profit-seeking corporations to treat consumer privacy as anything more than a marketing gimmick. Treating some technology companies as fiduciaries of our data will change that.[20] And, as we have seen with the automobile industry, a strong privacy tort regime can play a critical role in incentivizing corporations to fully integrate consumer safety demands into their culture.[21] On a more immediate and practical level, my research shows that companies who have been the subjects of strong regulatory intervention are more successful at embedding the importance of consumer privacy into design. This opens a pathway

---

*Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, at 451–57 (2016) (protecting privacy can build trust between online platforms and consumers); Ari Ezra Waldman, *Privacy as Trust: Protecting Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 563–64 (2015) (arguing that privacy should be conceptualized as based on relationships of trust between individuals); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1308–10 (2000). For a discussion of how traditional conceptualizations of privacy are based on notions of autonomy, please see *infra* Part II.A.

19. United States data privacy law at the federal level is "sectoral." That is, rather than a single comprehensive data privacy law, data is regulated only in some industries—health, financial, or children's data, for example. Even where it is regulated, the laws only protect certain data in certain circumstances. *See, e.g.*, Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 904–05 (2009); DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 404–05 (1992). Notably, state laws are filling gaps left by a gridlocked Congress. The California Online Privacy Protection Act (CalOPPA), for example, regulates almost all platforms that collect data on California residents. CAL. BUS. & PROF. CODE §§ 22575–22579.

20. Many scholars, including Jack Balkin, Jonathan Zittrain, Dan Solove, Danielle Citron, and others, have recommended a shift toward a fiduciary or trustee model to ensure corporations take consumer privacy seriously. *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).

21. Scholars have long argued for a more robust privacy tort regime. *See, e.g.*, Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1848 (2010); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L. J. 123, 182 (2007); Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 143 (2003).

for using robust FTC enforcement to make a difference.

Endogenous factors also play a role. As a long literature on organizational structures and routines suggests, bureaucratic barriers within corporations may impede the spread of privacy norms.[22] In the design context, siloed privacy structures and engineer-only design teams make it impossible for privacy professionals to raise and address privacy issues during the design process. And demographic homogeneity in design teams and the lack of ethics, diversity, and privacy education in technology curricula make it difficult for engineers to learn new perspectives and overcome discriminatory implicit biases. However, changes to corporate structure, hiring practices, employee social networks, and technology education can make organizational learning possible and help embed privacy norms among technologists.

This research is limited. Ethnographic research—especially ongoing, preliminary research—always is. This Article is based on a subset of interviews conducted with engineers in the high technology sector. The views about privacy discussed herein reflect the views of the interviewees, and even though this Article is based on interviews with forty technologists and lawyers, the findings can only point to a vision of privacy among some designers and lawyers. Further research is necessary,[23] and I consciously offer only modest conclusions as a result. But this research opens several scholarship and policy fronts in the fight to protect data privacy. A rich account of privacy on the ground adds something new to the privacy law discussion, highlighting the role lawyers and designers play in implementing privacy on the ground and the work that may still be necessary to fully realize the vision of CPOs.

## II. PRIVACY ON THE GROUND TODAY

Bamberger and Mulligan conducted their research on corporate CPOs for two main reasons. First, most critiques of the American approach to privacy law had focused on the laws on the books and ignored the contributions of privacy professionals. Many of those critiques, furthermore, recommended a shift toward a more European-style comprehensive privacy regime without

22. *See, e.g.*, Michael T. Hannan & John Freeman, *Structural Inertia and Organizational Change*, 29 AM. SOC. REV. 149, 154–55 (1983) (routines as a source of inertia in organizations); Howard M. Weiss & Daniel R. Ilgen, *Routinized Behavior in Organizations*, 14 J. BEHAV. ECON. 57, 62 (1985) (discussing how routinization can cause inflexibility). *See also* MAX WEBER, THE THEORY OF SOCIAL AND ECONOMIC ORGANIZATION 153 (A. M. Henderson & Talcott Parsons, trans. 1947).

23. That additional research will be discussed in the Author's forthcoming book, tentatively titled, *Designing with Privacy*.

investigating the on-the-ground effects of the current approach. Second, there had been only one previous study of corporate privacy practices, and it was published in 1994. Much had changed since then.[24] Their research not only updated our appreciation for an industry that was barely in its infancy in 1994, it also helped explain a paradox. In the twenty years between 1994 and *Privacy on the Ground*, which was published in 2015, the United States had not moved any closer to Europe's privacy regime. And yet, the data privacy situation on the ground did not seem as bleak as the law's harshest critics expected. Rather, a dynamic professional class of privacy leaders had emerged to create corporate privacy programs that seemed attuned to user needs. In this section, I briefly review the current approach to data privacy law in the United States and its critiques to put Bamberger and Mulligan's research in context. I then briefly summarize their work. As I discuss later, however, their groundbreaking research focused primarily on CPOs and executives, leaving open a door to dig further into the privacy work of technologists, product managers, and lawyers on the ground.

### *A. Notice-and-Choice and Its Critiques*

European and American approaches to data privacy are largely based on a series of Fair Information Practices Principles (FIPPs) that developed out of a 1973 report from the federal Department of Housing, Education, and Welfare (HEW).[25] The HEW Report recommended that users be informed of data use practices, have the opportunity to correct their data, and consent to any secondary uses of their information.[26] Several years later, the Organization for Economic Cooperation and Development issued similar guidelines, requiring, for example, that data gatherers disclose the purpose and scope of data collection, any security protocols, and all user rights.[27] The FTC got in on the act

---

24. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 249, 251.

25. 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).

26. HEW REPORT, *supra* note 25, at 41–42.

27. 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.

in 2000, urging Congress to require commercial websites to disclose a similar what-when-how of user data.[28] In so doing, the FTC identified "notice" as the most important FIPP, and notice-and-choice then became the dominant approach to consumer privacy.

The federal laws that regulate the collection, transfer, and use of some of our data reflect this primary focus on notice-and-choice. For example, the Health Information Portability and Accountability Act (HIPAA), which helps protect the privacy of medical information,[29] and the Gramm-Leach-Bliley Act, which gives individuals notice and some control over information held by certain financial institutions,[30] require covered entities to provide notice of data use practices. State laws follow suit. For example, California's Online Privacy Protection Act (CalOPPA) is a groundbreaking law that requires commercial websites and other online service operators that collect information about California residents to, among other things, post a data use policy.[31] Like the policies envisioned by Gramm-Leach-Bliley and HIPAA, CalOPPA-compliant policies must contain specific substantive disclosures: what information is collected, with whom it may be shared, how the data will be used, and how individuals will be notified about policy changes.[32]

Notice-and-choice is premised on the notion of the autonomous user. As a doctrine of informed consent,[33] it is supposed to give us control over our data by giving us the

28. FTC, PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON "PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE", BEFORE THE SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION § III(1) (May 25, 2000), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-online/testimonyprivacy.pdf.

29. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 100 Stat. 2548 (1996) (codified as amended at 42 U.S.C. §§ 1320d(1)–(9)); 45 C.F.R. 164.528 (2016).

30. Gramm–Leach–Bliley Act (GLBA), Financial Services Modernization Act of 1999, Pub. L. 106–102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. §§ 6801–6809).

31. *See* CAL. BUS. & PROF. CODE §§ 22575–22579. The law sets a de facto national standard because companies have an incentive to comply with the strictest law rather than navigating 50 different requirements. *See* Citron, *supra* note 4, at 762.

32. CAL. BUS. & PROF. CODE §§ 22575(b)(1), (3).

33. 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, 518 (2015). The principle of informed consent, as in the analogous contexts of medical procedures and scientific research, flows directly from Kant's categorical imperative: "Act in such a way as to treat humanity, whether in your own person or in that of anyone else, always as an end and never merely as a means." IMMANUEL KANT, GROUNDWORK FOR THE METAPHYSIC OF MORALS 29 (2005), http://www.stolaf.edu/people/huff/classes/GoodnEvil/Readings/kantgw.pdf. *See also* Jorge L. Contreras, *Genetic Property*, 105 GEO. L.J. 1, 18 (2016).

information we need to make rational disclosure decisions. Autonomy and choice animated the FIPPs and the Clinton Administration's "Framework for Global Electronic Commerce," which stated that "[d]isclosure by data-gatherers is designed to simulate market resolution of privacy concerns by empowering individuals . . . . Such disclosure will enable consumers to make better judgments about the levels of privacy available and their willingness to participate."[34] And the FTC has explained that notice is "essential to ensuring that consumers are properly informed before divulging personal information."[35] In other words, notice-and-choice was meant to give us the tools we needed for perfectly rational decision-making about our privacy.[36]

Critiques of the sectoral and notice-and-choice approaches to data privacy focus on its underlying theory, substance, and effects in practice. As a theoretical matter, the notion of the autonomous user is a myth.[37] And scholars have shown that we do not make perfectly rational disclosure decisions.[38] For example, Alessandro Acquisti, Leslie John, and George Loewenstein have found that disclosure behavior is based on comparative judgments:[39] if we perceive that others are willing to disclose, we are more likely to disclose;[40] if we perceive that the information asked of us is particularly intrusive, we are less likely to disclose.[41] Other scholars have found that disclosure can be emotionally

34. HEW REPORT, *supra* note 25, at 41–42. *See also* President William Jefferson Clinton, *A Framework for Global Electronic Commerce* at 13, THE WHITE HOUSE (July 1, 1997), http://clinton4.nara.gov/WH/New/Commerce/read.html).

35. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf. Notably, these same Kantian principles animate the doctrine of informed consent in the medical and research contexts.

36. *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1049 (2012).

37. *See, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 16–21 (2012) [hereinafter, "CONFIGURING THE NETWORKED SELF"] (as part of the governing principles of cyberspace); Julie E. Cohen, *Cyberspace As/And Space*, 107 COLUM. L. REV. 210, 225–27 (2007) (users are constrained by the built online environments around them); MICHAEL J. SANDEL, DEMOCRACY'S DISCONTENT: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY 25–28 (1996) (as the foundation of political philosophy).

38. *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363–64 (Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, & Sabrina di Vimercati eds., 2008); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE SEC. & PRIVACY 26 (2005).

39. Alessandro Acquisti, Leslie K. John, & George Loewenstein, *The Impact of Relative Standards on the Propensity to Disclose*, 49 J. MARKETING RES. 160, 160 (2012).

40. *Id*. at 160, 165, 172.

41. *Id*. at 160, 171–72.

manipulated: positive emotional feelings about a website, professional website design, the type of information requested, and the presence of a privacy policy correlate with a higher willingness to disclose.[42] The law of notice-and-choice today ignores such contextual factors.[43]

Notice-and-choice is also hopelessly underinclusive. It reflects an arbitrary and selective approach to the FIPPs, which also included limitations on data collection, security requirements, a rejection of black boxes, user rights to data, and robust accountability policies.[44] Even in regulated sectors, current law does not cover all data. For example, HIPAA only protects certain health data held by certain covered entities, like health insurance plans, clearinghouses, HMOs, and company health plans. And it only applies to doctors if they electronically transfer information in connection with a transaction for which the Department of Health and Human Services has adopted a standard.[45] It is no wonder that words like "patchwork" and "tangled web" are often used to describe the current state of data privacy law in the United States.[46] As Bamberger and Mulligan pointed out, many scholars and advocates suggested that the best way to solve these problems is to enact a comprehensive data privacy law and shift toward the more robust data protection regulatory regime of the European Union.[47]

### *B. Chief Privacy Officers*

One commentator recommending such a shift was H. Jeff Smith, a management scholar who published a study of privacy professionals in 1994.[48] In the seven U.S. companies he studied,

---

42. Han Li, Rathindra Sarathy, & Heng Xu, *The Role of Affect and Cognition on Online Consumers' Decisions to Disclose Personal Information to Unfamiliar Online Vendors*, 51 DECISION SUPPORT SYS. 434, 435 (2011).

43. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, PRIVACY, AND THE INTEGRITY OF SOCIAL LIFE 236–37 (2010).

44. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD), OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, Part II (2001), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

45. 45 C.F.R. §§ 160.102–160.103. *See also Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/covered-entities/ (last visited Jan. 10, 2018).

46. *See, e.g.*, Jay P. Kesan, Carole M. Hayes & Masooda M. Bashir, *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 27–78 n.61 (2016); Priscilla M. Regan, *Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows*, 59 J. Soc. Issues 263, 275 (2003).

47. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 259–60.

48. H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE

he found that few paid any attention to privacy and none dedicated significant resources to privacy protocols. While some corporations had no internal policies on privacy, others disregarded the ones they had. Smith also found that privacy considerations were noticeably absent in decisions about technology or business development. Privacy was, at best, an afterthought, and at worst, ignored completely.[49] Smith argued that these failures could be traced back to the law's "ambiguity" regarding what privacy meant and how companies are supposed to comply.[50] Because privacy, like corporate social responsibility, generally, can sometimes conflict with more primary corporate goals,[51] Smith suggested that a stronger, European-style regulatory approach was needed to force companies to take privacy seriously.[52]

But Bamberger and Mulligan noticed that even as U.S. privacy laws on the books had retained their underinclusive approach, a lot had changed on the ground since Smith's bleak narrative in 1994. An entire professional class of privacy professionals, led by CPOs and organized into large professional associations, had emerged.[53] Many of them were C-suite executives, and they were being hired in all industries, from the financial and health sectors to retail.[54] Law firms and many corporations now had robust privacy law practices. Privacy seals became sought after symbols of legitimacy.[55] And extensive audits of corporate privacy practices were now part of the corporate routine.[56] If these changes were not due to the Europeanization of American privacy law, what caused this shift?

Bamberger and Mulligan asked the CPOs themselves. Through a series of interviews with privacy professionals recognized as leaders in their fields,[57] they found that rather than

---

AMERICA 15, 25, 50–51, 209 (1994).

49. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 249–50 (*citing* SMITH, *supra* note 48, at 4, 82, 135–36, 139, 207, 213).

50. SMITH, *supra* note 48, at 139. *See generally id.* at Ch. 6.

51. *See, e.g.*, Peter Arlow & Martin J. Gannon, *Social Responsiveness, Corporate Structure, and Economic Performance*, 7 ACAD. MGMT. REV. 235, 236 (1982).

52. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 250 (citing SMITH, *supra* note 48, at 212–13, 217–18, 220).

53. *Id*. at 261–62.

54. *Id*. at 262.

55. Organizations such as TRUSTe issue privacy "seals" to websites that notify users about "what information is gathered/tracked; [h]ow the information is used; [and] [w]ho information is shared with." Solove & Hartzog, *supra* note 3, at 593.

56. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 263.

57. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 11–12, 40–43, 59 (on research methodology, including the focus on corporate executives and privacy leads).

having a corrosive effect on privacy on the ground, some ambiguity in the law allowed privacy leads to innovate and fall back on their creativity and judgment.[58] They found that CPOs understood privacy to be more than just giving users notice[59] and saw their companies' responsibilities as more than just compliance. To the CPOs, legal rules provided a floor.[60] And privacy was a constantly evolving user-focused concept about which they had to think proactively and strategically. Many of the interviewees felt that corporate privacy strategy was about maintaining user trust and being sufficiently flexible, adaptive, and forward-looking to meet consumer expectations whatever they may be.[61] It was not about doing the least they could to prevent a lawsuit. Rather, they had to engage in ongoing management of risk and keep up with consumers' changing expectations.[62] Several CPOs talked about their jobs in fiduciary terms: they were "steward[s]" of data and "responsibl[e]" to consumers.[63] They saw their primary objective as creating and maintaining "the company's trusted relationship" with customers, employees, and society.[64] In short, Bamberger and Mulligan found a profession of privacy officers earnestly working hard to advance the cause of consumer privacy within their companies.

The CPOs saw three seminal developments that contributed to their robust approaches to privacy: the emergence of the FTC as a privacy regulator, the passage of state data breach notification statutes, and the rise of strong advocates and media interested in privacy.[65] The FTC stepped into the role of de facto privacy regulator in the late 1990s pursuant to its authority in Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[66] Its growing portfolio of privacy actions has had a real effect on the ground: some of

58. *Id.* at 12.

59. *Id.* at 61. To many of them, notice was not even a helpful concept. When dealing with ongoing use and analysis of data, notice as a legal requirement ceases to be relevant. *Id.* at 63.

60. *Id.* at 60, 64.

61. *Id.* at 59, 65, 67. *See also* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 280.

62. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 67, 68.

63. *Id.* at 66.

64. *Id.* at 67.

65. *Id.* at 69–74.

66. 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).

Bamberger and Mulligan's interviewees owed their jobs to FTC enforcement actions against their employers. But more broadly, the CPOs recognized that operationalizing privacy law meant more than just looking at federal and state laws; they also had to consider "FTC cases and best practices, including 'all the enforcement actions [and] what the FTC is saying.'"[67] And since the FTC has been adept at enforcing consumers' evolving privacy expectations, especially as it has expanded its work from broken promises litigation to a broad range of consumer privacy protection cases,[68] CPOs implementing this new "common law of privacy" followed suit.[69] Together with the political and media attention that came with data breaches,[70] this incentivized companies to take privacy seriously. An increasingly active, engaged, and professional privacy community then helped newly placed CPOs develop practices that would both respond to FTC requirements and help ensure public trust.[71]

Bamberger and Mulligan also came away with some recommendations from their interviewees about how best to operationalize robust privacy practices throughout a company. The CPOs recognized two common threads: a powerful privacy lead at the top, with access to executives and the board, and distributed privacy responsibilities throughout a company's business units.[72] The most successful CPOs have the ear of the chief executive, report directly to the Board, and are accorded professional deference. They focus on developments in privacy in the wider legal and consumer space and translate what they learn into internal policies.[73]

But to push privacy as a priority throughout a company, CPOs need to involve "business-line executives" to develop specific privacy practices for their units. This collaboration creates a distributed network of accountability. A majority of the interviewees told Bamberger and Mulligan that "senior executives in the business units" had primary privacy responsibility.[74] Some companies also embedded employees trained in privacy issues throughout business units or employed unit-specific privacy

67. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 69.
68. *See Solove* & Hartzog, *supra* note 3, at 585–86, 590, 627–28, 649, 667, 672, 676.
69. *Id*. at 619–27.
70. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 71–73.
71. *Id*. at 73–74.
72. *Id*. at 76.
73. *Id*. at 77, 78, 80.
74. *Id*. at 83.

leads.[75] Since they would always be closer to the action than the CPO at the top, distributed privacy representatives could spot issues early, respond to them, and integrate privacy into design.[76]

## III. TWO PRIVACY NARRATIVES

Bamberger and Mulligan's important and insightful research suggests that empowered and innovative CPOs are creating and operationalizing a robust, flexible, and user-focused conception of privacy on the ground. They are heeding cues from the FTC, from each other, and from users, and embedding privacy into the products their companies create. As powerful as that narrative is, it leaves two questions unanswered, both of which suggest that *Privacy on the Ground* was a first step in a wider research agenda.

First, if the privacy leads that participated in Bamberger and Mulligan's research are approaching consumer privacy as thoroughly as they describe, to what extent have they been successful at integrating privacy throughout the culture of their companies? Second, how are CPOs, business-line executives, and unit-specific privacy leads "baking" privacy into design if none of them actually design anything?[77] That is, Bamberger and Mulligan revealed an important piece of the privacy by design puzzle, but the engineers and other technologists actually responsible for integrating corporate mandates into design must also be part of this story.[78] In this section, I tell the privacy narrative of some technology product designers. That story

75. *Id.* at 84–85.

76. *Id.* at 86.

77. Ann Cavoukian, the Information and 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); *see also* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE SEVEN FOUNDATIONAL PRINCIPLES (2009).

78. This distinction reflects the two aspects to every corporation's routine. In this context, a "routine" refers to a repetitive, recognizable pattern of interdependent actions, carried out by multiple actors. Martha S. Feldman & Brian T. Pentland, *Reconceptualizing Organizational Routines as a Source of Flexibility and Change*, 48 ADMIN. SCI. Q. 94, 95–96 (2003). Every organization deploys routines. *See* Paul J. DiMaggio & Walter F. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOC. REV. 147, 147 (1983). Adopting Bruno Latour's distinction between the "ostensive" and the "performative" aspects of behavior, Feldman and 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. Feldman & Pentland, *supra* note 78, at 95, 101. *See also* Bruno Latour, *The Powers of Association*, 32 SOC. REV. 264, 266–68, 271–73 (1984). Understanding the diffusion of norms through the routine requires studying both aspects, not just one.

suggests that perhaps Bamberger's and Mulligan's narrative has yet to be fully realized. From the user's perspective, the CPO's trust-based and forward-looking vision of privacy seems to run counter to both our experiences with technology products and privacy notices. And from the perspective of some of the lawyers and technologists in the trenches, it is not often part of the daily practice of design. In short, the vision of privacy held by some technologists and lawyers, particularly those in the high technology sector, is less robust, more reactive, and less central to their work than their CPO might hope.

### *A. Designing Without Privacy*

As Woodrow Hartzog describes in his book, *Privacy's Blueprint*, many of our favorite technology products are designed without our privacy in mind.[79] They may not always be willfully and purposely designed to manipulate us or invade our privacy (although some are). Many of them just ignore us and fail to take account of our privacy needs and expectations. Either way, they may reflect an institutional approach that has yet to fully realize their CPO's vision of privacy. There are countless examples. I will touch on four here.

Snapchat sold itself as a privacy-protective platform.[80] Beloved by its core base of Millennial users in part because any image or video, or "snap," sent across it automatically disappears after several seconds, the app theoretically offers powerful privacy protections for its users. Except, it was not originally designed that way. Before sending a snap, users were shown a screen that required them to designate the amount of time the snap will survive before disappearing.[81] Snaps could not be sent without selecting an option. But, in fact, there were several ways snaps sent could be saved, downloaded, or copied.[82] This gave users the

79. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (forthcoming 2018). Selections of this forthcoming text were presented at the Privacy Law Scholars Conference on June 3, 2016 at the George Washington University Law School.

80. Snapchat is an image messaging and multimedia mobile app with more than 100 million active users and 400 million "snaps" (audio or video messages) sent every day. Jason Abbruzzese, *Report: Snapchat Valued at $10 Billion in Latest Investment*, MASHABLE (Aug. 26, 2014), http://mashable.com/2014/08/26/snapchat-10-billion-valuation/#rVMZROnUy5qQ.

81. Snapchat Complaint, *supra* note 8, ¶ 6.

82. Snapchat Complaint, *supra* note 8, ¶¶ 9–17. Much of the FTC's case against Snapchat focused on the company's failure to disclose certain data collection practices in its privacy statement. *See id*. ¶¶ 8–33. But broken promises litigation is just one part of the FTC's privacy jurisprudence. *See* Solove & Hartzog, *supra* note 3, at 667. As Solove & Hartzog point out, the FTC has developed a broader view of unfair or deceptive practices,

false impression, reinforced in the platform's product descriptions and Frequently Asked Questions,[83] that they actually had control over what their recipients could do with their snaps.

Other aspects of Snapchat's original design also reflected an institutional approach that neglected privacy. Until October 2013, it stored all videos in unprotected spaces on users' phones, which allowed recipients to simply search for and download a video they wanted to save.[84] Snapchat also allowed any third-party application to access its application programming interface and download or copy videos and images.[85] Not only were these vulnerabilities not conveyed to users, but the platform's design created contrary expectations.

More recently, the wildly popular Pokémon Go app was also designed without privacy in mind.[86] In its initial release, the platform accessed players' smartphone cameras, collected location data, and, most notably, gained full access to players' Google accounts, including email, calendars, photos, stored documents, and any other data associated with the login.[87] The app was designed this way. In order to play Pokémon Go, players need an account. Accounts could be created in two ways: through pokemon.com or through Google. Normally, when an app user signs in using a Google account, a pop-up explains what data the app will be able to access, allowing the user to decide to go ahead or decline based on the app's data use practices.[88] That was not

---

including, for example, "deception by omission," *id*. at 631, "inducement" to share personal information, *id*. at 632–33, and "pretexting," *id*. at 633, to name just a few. Their persuasive argument is that "through a common law-like process, the FTC's actions have developed into a rich jurisprudence that is effectively the law of the land for businesses that deal in personal information." *Id*. at 589.

83. Snapchat Complaint, *supra* note 8, ¶¶ 7–8.

84. *Id*. ¶ 10.

85. *Id*. ¶ 11.

86. Pokémon Go is a location-based augmented reality game where players locate, capture, and engage with virtual creatures called Pokémon who appear on screen as if they were really in front of the player. *See* POKÉMON GO, http://www.pokemon.com/us/pokemon-video-games/pokemon-go/ (last visited Jan. 10, 2018).

87. *See* Valerie Strauss, *Pokémon Go Sparks Concern About Children's Privacy*, WASH. POST (July 19, 2016), https://www.washingtonpost.com/news/answer-sheet/wp/2016/07/19/pokemon-go-sparks-concern-about-childrens-privacy/ (including a letter from Common Sense Media Founder James Steyer detailing some of the app's privacy challenges).

88. These are called "just in time" notifications, and they are popular among privacy regulators. The FTC recommends them: "Providing such a disclosure at the point in time when it matters to consumers, just prior to the collection of such information by apps, will allow users to make informed choices about whether to allow the collection of such information." FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 15–16 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-

the case with Pokémon Go. Rather, users signed in using Google and immediately proceeded to the game interface. The default permissions, which were hidden by design, gave Pokémon Go full access to the player's Google account. The app's developers said the broad permissions were "erroneous,"[89] but even if that were true, Pokémon Go was still designed without privacy as a priority.

Uber went even further. Uber designed its app to give the company the power to identify its users even after they had deleted the program. The technique Uber used, known as fingerprinting, leaves a small piece of code on a phone after deletion so the app developer can know if the same device ever reinstalls the app. It has non-invasive users: In Uber's case, fingerprinting allowed the company to crack down on drivers who were downloading the app over and over again, creating new dummy accounts, and racking up ride volume. But it also allowed the company to individually identify specific users even after they had deleted the app.[90]

Finally, although not an online platform like Snapchat or Pokémon Go, privacy notices are also designed without users in mind. Joel Reidenberg, Lorrie Cranor, and others have shown that privacy policies are difficult to read and understand. They are often written to be confusing, obscure, and inscrutable.[91] They are also presented to users in ways that deter us from trying to read them in the first place.[92] For the most part, privacy policies today are presented in small type sizes, without sufficient spaces between lines or necessary white spaces in the margins, without

---

federal-trade-commission-staff-report/130201mobileprivacyreport.pdf. There is also evidence to suggest that just in time notifications work. *See, e.g.*, Rebecca Balebako et al., *"Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones*, Proceedings of the Ninth Symposium on Usable Privacy and Security 2–3, 8, 10 (2013).

89. *See* Laura Hudson, *How to Protect Privacy While Using Pokémon Go and Other Apps*, N.Y. TIMES (July 12, 2016), http://www.nytimes.com/2016/07/14/technology/personaltech/how-to-protect-privacy-while-using-pokemon-go-and-other-apps.html?_r=0.

90. Mike Isaac, *Uber's C.E.O. Plays With Fire*, N.Y. TIMES (Apr. 23, 2017), https://nyti.ms/2pSAyyu.

91. *See, e.g.*, R Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L. J. 39, 40, 87–88 (2015) (presenting results of an experimental study showing that average internet users do not understand privacy policies and that even experts cannot agree on the meanings of certain terms). 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* Cranor, *supra* note 11, at 274 (2012). This translates to about fifty-four billion hours per year for every U.S. consumer to read all the privacy policies he or she encountered. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. POL'Y FOR INFO. SOC'Y 543, 563 (2008).

92. *See* Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 129, 164–74 (forthcoming 2018) (showing how website and mobile app privacy policies are designed and presented to users in unpleasant ways that make it difficult for users to interact with them).

distinguishing headings or subheadings, and in colors that make them difficult to see.[93] Privacy policies are written by lawyers, for lawyers. Users are ignored.

Technologies like Snapchat, Pokémon Go, and the Uber app, as well as most privacy notices today, do not reflect the vision of privacy of the CPOs in Bamberger and Mulligan's study. Rather, our privacy was, at best, a secondary consideration in design. This does not challenge the Bamberger and Mulligan narrative, but it does question whether the vision of the CPOs they interviewed has been fully realized throughout technology companies. Undoubtedly, many privacy leads are hard at work encouraging their employers to take user privacy seriously. I do not mean to suggest otherwise. But there is another, parallel process at work. While many corporate CPOs may be nudging their boards, raising privacy issues in executive-level meetings, and collaboratively creating privacy protocols with unit vice presidents,[94] technologists and lawyers are doing the work of privacy on the ground, designing products and notices for user consumption. The next section is based on qualitative research into how lawyers and designers in the high technology sector incorporate privacy into their work. It presents an account of a far narrower vision of privacy that is factored into design, suggesting that more work may need to be done to fully implement Bamberger and Mulligan's research.

### *B. Technologists and Lawyers Discuss Privacy*

Over a 16-month period in 2016 and 2017, I conducted semi-structured interviews with nearly 80 technologists, all of whom are either current or former employees of technology companies of varying sizes, from Google and Facebook to start-ups, or technologists with product design experience at other companies, from home goods to online retail.[95] This group included engineers, computer scientists, programmers and coders, and web designers. This Article is based on a subset of those interviews, reflecting designers who work or have worked for high tech companies.

I identified these interviewees first via snowball sampling, a

93. *Id.* at 136–39 (describing, among other things, the results of an informal canvas of 191 privacy policies from popular websites in a variety of industries, from media and entertainment to retail, from sports to news).

94. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 76–86.

95. Though the interviews all began with questions about the interviewees' background, education, and work responsibilities, the discussions rarely followed a set script. That said, some of the questions I asked are attached at Appendix A (on file with Author).

non-probability sampling technique where existing study subjects recruit additional study subjects from among their friends, acquaintances, and social networks.[96] It can help researchers with limited resources identify target populations within a large, diffuse community,[97] i.e., technology workers. Because network-based sampling techniques like this tend to identify individuals with particularly thick social networks—people who know a lot of other people in the same field[98]—the individuals identified have a high likelihood of being well connected, experienced, and knowledgeable in the research subject. Snowball sampling also has downsides; it tends to identify research targets that are similar to each other. Given that potential for bias, other methodologies were used. I attended technology conferences and approached random attendees, some of whom agreed to short conversations. By the end of my ethnographic research in the Summer of 2017, snowball sampling likely accounted for only one-third of the total interviewees.

I do not purport to argue that my sample is representative of the entire designer community.[99] The interview responses cannot be generalized to cover all technologists or all lawyers. That, however, is not my goal. Like Bamberger and Mulligan, who used snowball sampling to find insight into the behavior of leading privacy professionals,[100] I hope to open a window into how some technologists and lawyers factor privacy considerations into their work and how, if at all, some corporate structure can embed privacy norms into design. This research is intended to suggest that the role of engineers and other designers and their privacy narratives need to be studied further in the research agenda on privacy by design. I do not suggest that all engineers or firm lawyers think the same way.

The interviewees all earned technology-related degrees, like computer science or engineering. The sample included no African American technologists—an ongoing problem in the technology

96. *See* Leo A. Goodman, *Snowball Sampling*, 32 ANNALS OF MATHEMATICAL STAT. 148, 148–70 (1961); James S. Coleman, *Relational Analysis: The Study of Social Organizations with Survey Methods*, 17 HUMAN ORG. 28, 28–29 (1958–1959).

97. Susan Welch, *Sampling by Referral in a Dispersed Population*, 39 PUB. OP. Q. 237, 237–38 (1975).

98. *See* Mark Granovetter, *The Strength of Weak Ties*, 78 AM. J. SOC. 1360, 1361 (1973).

99. Snowball sampling also comes with certain biases. Because it relies on social networks starting with the researcher and branching out from subject to subject, snowball sampling can underrepresent isolated or unique individuals or over represent those with similar characteristics to the original researcher. Welch, *supra* note 105, at 238.

100. Bamberger & Mulligan, *supra* note 1, at 264.

community[101]—but did include diversity on other identity-based metrics, including ethnicity, gender, and sexual orientation.[102]

I also interviewed 14 lawyers at private firms whose portfolios included privacy and cyber security. I also reached out to attorneys at AmLaw Top 100 firms who listed privacy as part of their practices. These interviewees were particularly diverse along gender lines: 9 of the 14 who agreed to speak with me were women. They earned their degrees at a variety of law schools. All worked for firms with more than 50 employees.[103]

I offered every interviewee the opportunity to discuss their views anonymously, pseudonymously, or with their real name and affiliation. All interviewees except one preferred some level of anonymity, either because they could not honestly respond without obscuring their identities or because they were in the process of or planning to apply for jobs in the technology sector. Therefore, I worked with each of them to find a descriptor that made them comfortable. All consented to some mention of the type of company they worked for—"a coder at a large technology company," for example. Lawyers chose this option, as well, opting to be identified only as "a partner at an AmLaw Top 100 law firm," or something similar. Pursuant to a confidentiality agreement, I respected all of these preferences in order to engage in honest discussions about their privacy-related work.

Many of the interviewees described similar views on privacy and alluded to personal and educational biases and corporate barriers that, as discussed in more detail in Part IV, could hinder the institutionalization of robust privacy norms from the CPO's office. Other interviews revealed ways in which privacy can factor

---

101. *See, e.g.*, Mark Milian, *The Silicon Valley Diversity Numbers No One is Proud Of*, BLOOMBERG (Aug. 12, 2014, 11:18 PM), https://www.bloomberg.com/news/2014-08-12/the-silicon-valley-diversity-numbers-nobody-is-proud-of.html; Vauhini Vara, *Why Doesn't Silicon Valley Hire Black Coders?: Howard University Fights to Join the Tech Boom*, BLOOMBERG (Jan. 21, 2016), http://www.bloomberg.com/features/2016-howard-university-coders/.

102. I was able to include gender, sexual orientation, and gender expression diversity in the sample of technologists through my participation in Out in Tech, a nonprofit that provide resources and mentorship to ensure career access for LGBTQ individuals interested in technology industries. Several of the interviewees in this study responded to a request for participation sent through the organization's mailing list. They helped connect me with other technologists, as well. *Who We Are*, OUT IN TECH, https://outintech.com/about/ (last visited Jan. 10, 2018).

103. This Article does not reflect interviews with in-house attorneys, although my ongoing research since has. My rationales for excluding in-house lawyers from this stage of the research project are as follows. First, Bamberger and Mulligan included the perspective of some in-house lawyers in their research. Second, the goal of this project was to reach to the very front lines of privacy work. That includes the products we use and the interfaces we see. Both of them are created by designers and technologists. And outside lawyers draft the privacy policies that form the legal relationship between technology platforms and their users.

into design and highlighted structural changes that make privacy more likely to be a priority in other companies.[104] But, for the most part, technologists and firm lawyers thought about privacy in narrow ways, either as synonymous with encryption or limited to notice-and-choice. Many engineers found user privacy difficult to integrate into design, and many thought it was beyond the scope of their employment mandates. Corporate privacy structures, especially those set up as independent departments, tended to take laissez faire approaches to consumer privacy. Therefore, privacy decisions were made on the fly by engineers and engineer-only teams, while privacy took on a compliance, check-the-box approach.

*1. The Meaning of "Privacy".* When Bamberger and Mulligan spoke to CPOs at leading multinational corporations, they found a vision of privacy far more robust than the autonomy-based conception of privacy embedded in the law on the books.[105] The CPOs recognized that privacy was not just about notice, control, or compliance. Rather "customer or . . . individual expectations" governed the corporate approach to privacy. The interviewees most frequently couched their understanding of privacy in fiduciary terms: privacy was about "respect[ing]" their customers, being "steward[s]" of their data, and "protect[ing]" the information they collected. Notably, the CPOs felt that privacy "equated to trust" or was a "core value associated with trust."[106]

To the extent that the technologists I interviewed had an understanding of privacy as a substantive concept—and many of them did not—it was fundamentally different from that of the CPOs in Bamberger and Mulligan's work. Several current and former engineers at major technology companies said that "privacy was not a helpful concept."[107] One was particularly incredulous: "What does the word 'privacy' mean? I don't know."[108] A former

104. It is worth noting what I mean by "factoring privacy into design" or "taking privacy seriously in design" or "integrating privacy protections into the design of new technologies," phrases that I use throughout this Article. This project is primarily concerned with the design process and how, if at all, privacy issues are raised and solved at the design stage. It is true that design teams can consider privacy issues, but for whatever reason, do not code in a fix to the privacy problem. Although that is better than ignoring privacy wholesale, I am still concerned with the cultural, legal, structural, and social forces, if any, that prevented a privacy fix from making it into the final product design.

105. *See supra* Part II.A.

106. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 270–71.

107. Telephone interview with engineer at Silicon Valley technology company (4) (Aug. 18, 2016) (notes on file with Author).

108. Telephone interview with engineer at fitness technology company (Sept. 16, 2016) (notes on file with Author).

engineer at LinkedIn agreed: "We all think about privacy, but I don't think anyone has a clear idea of what it means."[109]

These responses could reflect the fact, noted often in privacy scholarship,[110] that privacy is an ambiguous concept hard to pin down. Or it could be based on the lack of any privacy-specific education in many major technology degree programs.[111] But many technologists did have a conception of privacy. I noticed two running themes during the interviews: privacy-as-notice-and-choice and the conflation of privacy and security. Some, particularly programmers or engineers who had been promoted to team leader or product manager positions, thought that privacy was about "giving users notice about what was happening with their data." A former product manager at Google now running his own start up agreed: "Privacy is definitely important. We have to give users the information they need to make decisions."[112] When an engineering team leader at a New York technology company responded similarly, he added, "or else how can you decide if you want to use my app or some Silicon Valley copy?"[113] A senior engineer who used to work for Uber said that "we have to make sure you know what's going on. I think that's what we think about when privacy comes up: your ability to make the right decisions [about information] for you."[114]

Perhaps the best reflections of the technologists' understanding of privacy were two responses on the issue of behavioral targeting, or the process by which advertisers track Internet users' online activities and use that information to identify what kinds of ads they want to see.[115] A former technologist at Facebook raised the issue on his own: "Look at ad

109. LinkedIn engineer interview, *supra* note 15.

110. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2009) ("Privacy, however, is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."); Waldman, *supra* note 18, at 565–88 (reviewing the literature on different conceptions of privacy).

111. *See infra* Part IV.D.

112. Telephone interview with start-up CEO (Sept. 19, 2016) (notes on file with Author).

113. Interview with engineer in New York (Sept. 23, 2016) (notes on file with Author).

114. Interview with senior engineer at Uber (Sept. 23, 2016) (notes on file with Author).

115. Behavioral targeting is "the tracking of a consumer's activities online . . . in order to deliver advertising targeted to the individual consumer's interests." FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES 2 (2007) [hereinafter, ONLINE BEHAVIORAL ADVERTISING], https://www.ftc.gov/sites/default/files/documents/public_statements/online-behavioral-advertising-moving-discussion-forward-possible-self-regulatory-principles/p859900stmt.pdf.

targeting. People love it. Someone living in Southern Kentucky doesn't want to see an ad for some artisanal cheese place in SoMa [the South of Market neighborhood in San Francisco]. Privacy to me means giving people the choice to get the best ads possible or to see things irrelevant to their lives."[116] Despite the privacy risks inherent in behavioral targeting,[117] this technologist saw privacy as much more limited, as the seemingly easy choice between opting in and opting out. A former engineer at Google and Microsoft referred to this as a "dogma" that most engineers "actually believe."[118] Under such a dogma, consumer privacy must be relatively narrow: it misses the privacy concerns associated with data tracking and is, therefore, limited to notice-and-choice.

Notably, this definition of privacy was shared by almost every lawyer I interviewed. A partner at an AmLaw Top 100 law firm saw privacy "as the notion that you should have some control over your data."[119] Her colleague followed up: "Exactly. Privacy is about companies giving you the tools you need to control dissemination of your data. We can help our clients do that by clearly and adequately laying out data use practices."[120] A senior associate at a small law firm specializing in internet and privacy matters agreed, stating that "privacy is about giving internet users notice about what will happen to their data. This allows them to go to another website if they want to." An experienced partner at a New York law firm thought the question was straightforward: "Privacy is whatever the law says it is." Though I found that response unsatisfying, this partner disagreed. "We spend a lot of time reviewing statutes, FTC actions, and anything we can get our hands on. The law is clear. Our clients have to provide users with notice and choice. It's repeated over and over. And we help them do that."[121]

Another theme running through the interviews with technologists was the association of privacy with encryption. Nine technologists stated it explicitly; several others used words or

116. Telephone interview with former technologist at Facebook (June 4, 2016) (notes on file with Author).

117. *See, e.g.*, ONLINE BEHAVIORAL ADVERTISING, *supra* note 115, at 2–6.

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

119. Telephone interview with partner at AmLaw Top 100 law firm (11) (Sept. 30, 2016) (notes on file with Author).

120. Telephone interview with associate at AmLaw Top 100 law firm (Sept. 30, 2016) (notes on file with Author).

121. Interview with senior partner at AmLaw Top 50 law firm, in New York, NY, (Sept. 23, 2016) (notes on file with Author).

phrases like "de-identify"[122] or "add noise"[123] or "security,"[124] and one said that privacy was about "making data impossible to hack."[125] A programmer at a publishing company said that he "was taught that part of my job was going to be to encrypt the data we collected." Another engineer stated plainly that many of his colleagues believed that "if I encrypt the data, it's private."[126] The Linked In engineer stated: "My job was to prevent us from getting hacked."[127] An app developer said that his job was to "tell my engineers, my programmers, my data guys that the shit would hit the fan if we ever got hacked. Security had to be an important priority. Sure, we all need to make money and we all want to make money. But we're not going to do that if we don't secure the data."[128]

These two themes—privacy-as-notice and privacy-as-security—are different from the motifs that came through Bamberger's and Mulligan's interviews. Trust, though a watchword among scholars and CPOs, only came up in terms of providing users with notice. The latter group, which consistently defined a "company" definition of privacy as consistent with user expectations and evolving notions of responsibility and trust,[129] wanted their organizations to go beyond notice, choice, and security. Indeed, several of Bamberger's and Mulligan's interviewees felt that discussions about "security," "notice," and "consent,"[130] the outer limits of the firm lawyers' and technologists' understanding of privacy, played "limited role[s]" in the ways their companies approached privacy questions,[131] especially when it came to the ongoing use and manipulation of collected data.[132] This divergence suggests that the CPO's vision of privacy has not yet been fully realized among the lawyers and technologists doing the

122. Interview with member of trust and security team at Bloomberg LP, in New York, NY (Oct. 17, 2016) (notes on file with Author). De-identification is a common security and encryption tool. It does not always work. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 U.C.L.A. L. REV. 1701, 1716–31 (2010) (discussing the failure of anonymization and the implications for privacy law).

123. Silicon Valley engineer (4) interview, *supra* note 107.

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

125. Interview with member of trust and security team at Bloomberg LP, *supra* note 122.

126. Google and Microsoft engineer interview, *supra* note 124.

127. LinkedIn engineer interview, *supra* note 15.

128. Telephone interview with app developer (Aug. 19, 2016) (notes on file with Author).

129. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 270.

130. *Id.* at 266–67.

131. *Id.* at 266.

132. *Id.* at 267.

work of privacy on the ground. The ways, if any, in which these understandings of privacy impacted the design process is the subject of the next section.

*2. Privacy and the Design Process.* The CPOs interviewed in *Privacy on the Ground* earnestly wanted to include their concern for privacy into the design process. They created robust and integrated policies to do so. They embedded privacy personnel into different business units or geographic centers to "position[ ] privacy as a design requirement."[133] In addition, the CPOs worked with unit vice presidents and others trained in privacy issues to "identify items for consideration" and develop "appropriate business-level policies."[134] Some companies went further, creating privacy "checkpoints" and "privacy impact assessment" tools that included questions to ask and answer during the design process to elevate privacy on the priority ladder.[135]

These are excellent ideas that could, theoretically, help embed privacy norms throughout a company.[136] However, at least at many of the companies represented in my interviews with technologists, these policies and tools either existed, but were never used, or did not exist at all. The integration of privacy issues into technologists' work was often limited to the onboarding process. Privacy professionals or other personnel trained in privacy rarely met with engineers and programmers, even during weeks of intense design work. At companies that created privacy teams that were supposed to "insinuate" themselves into design,[137] high turnover, a laissez-faire attitude, and corporate silos kept privacy mostly orthogonal to design. And where privacy concerns were flagged, decisions were made on the fly by engineers with no privacy training.[138]

Engineers working at start-ups "didn't really think about

133. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 85–86.

134. *Id*. at 84–86.

135. *Id*. at 86.

136. However, they reflect a rather superficial understanding of the weaknesses of organizational routines. As discussed in more detail in Part IV.C, structural changes to corporate organization can help diffuse and embed robust privacy norms if they focus on increasing organizational learning and rely on interpersonal trust.

137. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 85–86.

138. When responding to questions about corporate privacy and integrating privacy into design, many technologists were particularly concerned about their anonymity. Several respondents noted the high level of turnover at many technology companies and the possibility that they could return to their former employers. As such, these technologists requested that when it came to talking about company policies, that they not be identified at all. All interviews, with appropriate redactions are on file with the Author.

privacy." Nor did the executives, for that matter.[139] Larger companies that say they take privacy seriously had a different problem: prioritization. Privacy was simply not a top priority for engineers because it was crowded out by other mandates. Engineers and start-up executives repeatedly spoke of the need to collect data to optimize user experience: "we looked at data to see what people are interested in, what they're clicking on, and where they're going so we can make the site better. When we had some privacy issue come up, it was added to the engineering queue. But engineers had to prioritize speed, agility, functionality."[140] A computer programmer with experience at start-ups and at larger companies noted that "we would work nonstop. I had a thousand things to do, and this (privacy) was one of them. It wasn't essential to our success, so it didn't get done."[141]

Many more established companies that are supposed to have policies to ensure customer privacy factored into design work did not always implement them: "does asking [a] question mean there were policies?"[142] Sarcasm aside, many engineers were simply not aware of checklists or assessments to help them integrate privacy concerns into their work. The response from an engineer formerly at a sharing economy company represented the views of a plurality of the interviewees:

> [Such policies] would have been great. That really could have helped us avoid some problems and think more globally or holistically about our work. But I can tell you that nothing like that ever existed. If it did, I have to imagine I would have heard about it. But I never did, and no one ever stopped me and said, 'here, use these.'[143]

That said, eleven interviewees recalled that privacy was discussed, but only during onboarding. "I remember being told at some point that we should think about privacy issues, but I think that was limited to the first week,"[144] one said. A web designer said that she "was told to think about privacy during a five-minute talk during onboarding. I don't think the word, or anything like it,

---

139. Interview with former general counsel at New York technology company, New York, NY (Oct. 28, 2016) (notes on file with Author).

140. *Id*.

141. Interview with former programmer at New York start-up, New York, NY (June 24, 2016) (notes on file with Author).

142. Telephone interview with former computer programmer at online retailer (June 18, 2016) (notes on file with Author).

143. Telephone interview with engineer at large sharing economy company (Sept. 22, 2016) (notes on file with Author).

144. Telephone interview with engineer at Silicon Valley technology company 2 (Sept. 9, 2016) (notes on file with Author).

was ever mentioned again."[145] Another "watched a 5-minute video about handling sensitive information;"[146] yet another recalled that her entire privacy orientation boiled down to "a warning: don't carelessly leave sensitive stuff at the gym, even in our gym."[147] Other interviewees reported similar problems at other companies. Interviewees used words and phrases like "hands off," "absent," "uninvolved," and "not really a factor," to describe their employers' approach to privacy. And, according to media reports, privacy is not even part of Facebook's famous bi-monthly "bootcamp" for new engineers.[148]

Interviewing several former designers at Google offered a deeper picture of the company's approach to privacy from 2010 to 2016. In reaction to several privacy failures, Google created a privacy team in 2010,[149] and the company has routinely pointed to the team's large footprint as evidence of its commitment to user privacy.[150] But according to several interviewees, privacy at Google was much more oriented toward compliance and security than a robust, user-focused vision of privacy in design.

Google says that it has a privacy infrastructure that appears similar to a variant described by Bamberger and Mulligan described in *Privacy on the Ground*. Their interviews with CPOs revealed that some companies try to embed privacy norms with "full-time privacy subject-matter experts" that help business units with privacy issues in real time.[151] Google does that through a privacy team, which, until recently, was run by Alma Whitten, who earned a doctorate in computer science from Carnegie Mellon.[152] It is now run by another security-focused technologist,

145. Interview with web designer, (Oct. 9, 2016) (notes on file with Author).

146. Google and Microsoft engineer interview, *supra* note 124.

147. Telephone interview with computer programmer (June 27, 2016) (notes on file with Author).

148. *See* J. O'Dell, *Bootcamp! How Facebook Indoctrinates Every New Engineer It Hires*, VENTURE BEAT (Mar. 2, 2013, 11:25 AM), http://venturebeat.com/2013/03/02/facebook-bootcamp/.

149. Google's privacy infrastructure was created as part of a $22.5 million settlement with the FTC for breaking various privacy promises. *See* Decision and Order, *In the Matter of Facebook, Inc.*, F.T.C. File No. 0923184, Docket No. C-4365 (F.T.C. July 27, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; Press Release, Fed. Trade. Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

150. *See* Glenn Chapman, *New Google Security Chief Looks for Balance with Privacy*, PHYS.ORG (Apr. 18, 2015), http://phys.org/news/2015-04-google-chief-privacy.html ("We have made a tremendous effort to focus and double-down on privacy issues.").

151. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 85.

152. *See* Frederic Lardinois, *Google's Director of Privacy Alma Whitten Steps Down*,

Lawrence You, an experienced Google hand with a doctorate in computer science from the University of California at Santa Cruz and an undergraduate degree in electrical engineering from Stanford.[153] Both technologists became privacy leads from a cyber security background, which makes sense given that some technologists conflate privacy and security.[154]

Several former Google employees interviewed noted that the team was almost entirely focused on security and generally isolated from any engineering work and product design. For example, a job posting for an engineer for Google's privacy "red team" conflated privacy and security:

> As a Data Privacy Engineer at Google you will help ensure that our products are designed to the highest standards and are operated in a manner that protects the privacy of our users. Specifically, you will work as member of our Privacy Red Team to independently identify, research, and help resolve potential privacy risks across all of our products, services, and business processes in place today.[155]

One interviewee said that these jobs were akin to "penetration testing, which is like hiring a hacker to test your security."[156]

Beyond developing cyber security structures, Google's privacy team often operated like a separate corporate department that had to clear products at the end of the design process even though privacy representatives were supposed to be integrated into design teams. As one former engineer put it, "we would need to run our design by privacy, legal, and marketing."[157] But three factors prevented that process from having any real impact on consumer privacy in design. First, the team was entirely "focused on security. They wanted to know if what I did could be hacked. And I told them no." Second, the process was "compliance-style. I remember being told by my manager that 'privacy checked the boxes, so we can go ahead.'"[158] And third, there was a sense among three interviewees that even though the privacy team, like the

---

TECHCRUNCH (Apr. 1, 2013), https://techcrunch.com/2013/04/01/googles-director-of-privacy-alma-whitten-steps-down/.

153. *See* Lawrence You, Google+ Profile, https://plus.google.com/115317725503531115879 (last visited Jan. 10, 2018).

154. *See supra* notes 122–128 and accompanying text.

155. *See* Thomas Claburn, *Google 'Red Team' To Test Product Privacy*, INFORMATIONWEEK: DARKREADING (Aug. 23, 2012, 2:59 PM), http://www.darkreading.com/risk-management/google-red-team-to-test-product-privacy/d/d-id/1105950?.

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

157. Google and Microsoft engineer interview, *supra* note 124.

158. Google employee interview, *supra* note 156.

legal and marketing departments, were seen as hindrances to design, the team did not really want to get in the way. "Nobody at Google wants to stop creativity," one former engineer said.[159] "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."[160] This narrow, compliance focus from a team that, some suggested, wanted to get out of the way of the design process, is quite different from the more robust, deeply embedded vision that emerged from Bamberger and Mulligan's interviews. More specifically, it appears that the structures the CPOs tried to put in place were insufficient.

Given the breakdown in operationalizing privacy through dedicated corporate structure, either because such structures did not exist or because of their narrow focus on security, privacy decision-making fell to the engineers themselves. Any "decision we ever had to make about privacy, when it did come up, was made according to our best intuition," one engineer noted.[161] And these engineers rarely, if ever, could turn to a privacy expert or even a lawyer for advice. Rather, as many technologists reported in their interviews, they do their work in teams, many of which included only other designers, an artist and, perhaps, a business-oriented liaison. The team leader was also a coder; his—and they are almost all men[162]—supervisor was also a coder, promoted because he was particularly good at his job, not because he had any leadership skills or strategic planning perspective. Plus, many engineers repeatedly noted the high degree of turnover within their teams.[163] In this environment, privacy decisions were made ad hoc, without any clear guidance, and by technologists not necessarily in the best position to make them.

*3. The Role of the User.* Users played an outsized role in the narrative teased out by Bamberger and Mulligan. To the CPOs interviewed, the user was at the center of their flexible and adaptive approach to privacy. The model let "customer or . . . individual expectations" guide corporate behavior above and beyond the limited requirements of the law of notice-and-choice.[164]

159. Google and Microsoft engineer interview, *supra* note 124.

160. Google employee interview, *supra* note 156.

161. Telephone interview with engineer at Silicon Valley technology company (6) (June 20, 2016) (notes on file with Author).

162. *See e.g.*, Kate Crawford, *Artificial Intelligence's White Guy Problem*, N.Y. TIMES (June 25, 2016), http://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html (discussing the existence and effects of implicit bias in future technology design given that most technology designers are white men).

163. Interview with Silicon Valley engineer (6), *supra* note 161.

164. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 270.

As noted above, CPOs saw themselves as "steward[s]" of their customers' data, and focused their work on earning and maintaining user trust: "[T]he end objective," one CPO reported, "is always what's the right thing to do to maintain the company's trusted relationship with our employees, with our clients, with any constituency in society that has a relationship to us."[165]

This fiduciary, trust-based approach to privacy is the gold standard for users. If implemented, it would change users' traditionally limited role in the design of new technologies, from one in which users rarely factor into and yet are constrained by design[166] to one in which users become part of the design process.[167] However, as my interviews revealed, how real people use the products that technologists create is less important than legal or professional mandates that govern design.[168]

Fifteen of the designers I interviewed noted it was difficult in practice to consider user needs. As one engineer noted, "there was always an idea that we were designing for customers, many of them loyal to [the company], but it's difficult to consider that in any practical way as I was actually doing my work."[169] An experienced engineer who became a senior product manager in Silicon Valley summed up six interviewees' thoughts on how users factored into their work: "[The company] really cared about customers trusting us. But that wasn't my job. My job was to make unhackable infrastructure, to design a platform that worked and

165. *Id*. at 271.

166. *See* Woolgar, *supra* note 16 (ethnographic study of a company developing one of the first microcomputers showing that structural forces at play prevented users from truly being considered in design). *See also* LUCY A. SUCHMAN, HUMAN-MACHINE RECONFIGURATION 186–93, 257–84 (2d ed. 2007) (users configured by design); Cohen, *supra* note 38, at 210, 221, 225, 233–36 (the design of built online environments constrains user behavior).

167. As several sociologists have argued, users can be part of the social construction of new technologies. *See, e.g.*, Ronald Kline and Trevor Pinch, *Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States*, 37 TECH. & CUL. 763, 768–94 (1996) (cars); CLAUDE S. FISHER, AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940 82 (1992) (telephone). But in these narratives, users factor into the post-design social process by which inventions situate themselves into society. Integrating robust privacy norms into the companies that create new technologies would ensure that users and user needs are considered every step of the way during the design process.

168. The notion that technology and related law and policy should consider the embodied experience of real users was raised, most notably, by Larry Lessig, Julie Cohen, and others. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 24–29 (1999) (the design of the digital technologies that make up "cyberspace" make it impossible for it to be a completely free space); CONFIGURING THE NETWORKED SELF *supra* note 37, at 24–31 (2012). *See also* MAURICE MERLEAU-PONTY, PHENOMENOLOGY OF PERCEPTION, xi (Ted Honderich ed., Colin Smith trans. 1962).

169. Telephone interview with engineer at Silicon Valley technology company (2) (June 24, 2016) (notes on file with Author)

worked well."[170] Some technologists went further. One said: "There is no possible way I could factor users into design. How would that even be possible? There is no single user."[171] Four interviewees voiced the same problem. Their response was to "design for the only person I know: myself" or to "design based on the higher ups' message."[172]

There was another recurring theme: in seven interviews, technologists recalled that the concepts of the user and user trust did come up, but most often with respect to the company's bottom line. The former Google and Microsoft engineer said it best. After recalling the 2010 Chinese hack of Google servers[173] and the 2011 FTC action against Google for misleading customers about the privacy implications of Google Buzz,[174] it became clear that "Google was concerned about users, but only as it affected the bottom line." He continued:

> We were told, 'Don't let [the China hack or the Google Buzz action] happen again.' The company's perspective was: we want to protect our customers so they feel comfortable sharing their data so we can still sell them adds. If Google has a major breach, Google is done.[175]

This perspective seems in line with many companies' and technologists' focus on security as the sum total of their privacy priorities. But it reduces the impact users can have on the design process.

Users factored only nominally into the privacy work of lawyers at private firms, as well. In the last ten years, at least 90 of the AmLaw Top 100 law firms have created privacy and security practices.[176] Their attorneys' work is varied, ranging from complex

---

170. Telephone interview with senior product manager (Oct. 4, 2016) (notes on file with Author).

171. This problem was echoed by several of the engineers interviewed by Steve Woolgar for *Configuring the User*. *See* Woolgar, *supra* note 16.

172. Telephone interview with game platform designer (Aug. 15, 2016) (notes on file with Author).

173. *See, e.g.*, Ellen Nakashima, *Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, WASH. POST (May 20, 2013), https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

174. Complaint, *In the Matter of Google, Inc.*, F.T.C. File No. 102 3136, Docket No. C-4336 (F.T.C. Oct. 13, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf.

175. Google and Microsoft engineer interview, *supra* note 124.

176. Ninety of the AmLaw Top 100 law firms included specific reference to their firm's privacy practices, alternatively called "Privacy and Cybersecurity," "Security and Privacy," "Data Security," or some variation. Because attorneys at the few top law firms that did not

litigation to ongoing risk counseling. They also draft and update their clients' privacy policies, which, ostensibly, are supposed to give users notice of platforms' data use practices.[177] Most attorneys follow the same procedure when updating privacy policies: after researching relevant federal and state laws, FTC settlements, and any other applicable guidance, they meet with in-house counsel and discuss data use practices in more detail. Few would speak to their clients' engineering team leaders to learn precisely how the company uses customer data; most rely on in-house counsel or the company's chief technology officer to obtain the information for them. They would then take this information and determine if updates to privacy notices were necessary. Although some might argue that in-house counsel is supposed to play this intermediary role, their involvement in the process creates friction between engineers and privacy policies that can end up weakening notice.

Although all attorneys interviewed recognized that privacy policies "provided notice to users" and some encouraged their clients to keep policies "short" and "comprehensible,"[178] the vast majority of their work focused on privacy policy content. Most of the attorneys were not concerned that privacy policies have become long, legalese documents that users cannot understand.[179] As one attorney told me directly: privacy policies "are legal documents and we treat them as such."[180] Another admitted that she "write[s] privacy policies for the FTC. They are the only people who read them."[181] When probed further, the head of a top law firm's privacy practice stated that "users know exactly where they are. If they wanted to read privacy policies, they know where to find them. But they don't. The FTC does, and they are the ones who determine if our clients are at risk."[182]

This last point reflected a common theme in most of the attorneys' responses. They saw their job as primarily "protect[ing] clients from litigation" from the FTC and state attorneys general. User expectations were absent. As one attorney with ten years'

---

differentiate a privacy-specific practice may still work on privacy issues on a more informal basis, it is more accurate to say "at least 90" rather than 90.

177. *See supra* Part II.A.

178. Telephone interview with partner at 5-person privacy/internet boutique law firm (Mar. 26, 2016) (notes on file with Author).

179. *See, e.g.*, Reidenberg, *supra* note 91, at 72 (presenting results of experiment showing average internet users do not understand privacy policies).

180. Telephone interview with partner at AmLaw Top 50 law firm (1) (Sept. 16, 2016) (notes on file with Author).

181. Telephone interview with partner at AmLaw Top 50 law firm (2) (July 8, 2016) (notes on file with Author).

182. Telephone interview with partner at AmLaw Top 50 law firm (4) (July 15, 2016) (notes on file with Author).

experience as outside privacy counsel noted, "When it comes to privacy policies, we look to the law and we make sure we disclose everything we need do." Like their narrow, notice-based conception of privacy,[183] firm attorneys' take on their limited responsibilities with respect to privacy policies contrasts with the robust "company law" created by the CPOs in *Privacy on the Ground*. In the latter, privacy leads not only found the law on the books unhelpful, they went far beyond the letter of the law to develop robust privacy structures throughout their companies.[184] Outside counsel, however, relied almost exclusively on the law on the books to inform their work. The kind of creativity displayed by the CPOs interviewed by Bamberger and Mulligan was absent.

*4. Technologists, Lawyers, and Privacy Professionals.* The CPOs Bamberger and Mulligan interviewed alluded to extensive interaction down the corporate hierarchy between full- or part-time privacy professionals and other decision-making employees. CPOs and their direct subordinates would often work with business-line executives, in-house counsel, risk management teams and other functional groups to both internal privacy infrastructures. This teamwork was important, the CPOs agreed, because privacy needed a "buy-in" from key stakeholders across the company.[185] Some of these companies also embedded privacy professionals within business units, with each having subject matter and privacy expertise, so they could interact with the businesses more directly and provide decision-making guidance and training on the ground.[186] Therefore, some CPOs deployed privacy officers across departments, from marketing and sales to finance and operations, that reported directly to their unit executives and to the CPO.[187] The interviewees agreed that this diffuse structure was critical to "positioning privacy as a design requirement rather than a legal matter."[188]

Ostensibly, the goal of this embedded network of privacy employees is to keep privacy decision-making as close as possible to the trenches of day-to-day work. That requires ongoing interaction and cooperation among privacy professionals and business unit workers. At least with respect to the designers I interviewed, however, that cooperation did not always exist. Several engineers recalled "never once" meeting with "a privacy person the entire time

183. *See supra* Part III.B.1.

184. *See supra* notes 57–64 and accompanying text.

185. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 83.

186. *Id*. at 84.

187. *Id*. at 85.

188. *Id*. at 86.

[they were] there."[189] Another acknowledged that "there was a person or a team who was supposed to be our privacy and security contact, but I never heard from him."[190] A senior technologist in Silicon Valley recalled that he "made all the decisions when they came up. I'm sure there was someone, on paper, that I was supposed to talk to, but no one ever said anything, no one made a push for it, and it just never came up."[191] Lawyers, too, were alien to technologists. "If you hadn't mentioned that there were lawyers there, or if I didn't know independently, I could easily assume that [the company] employed zero attorneys," said one engineer.[192] Outside counsel, one interviewee noted flatly, "doesn't have the ability to [talk to] engineers."[193] This lack of interaction is not necessarily a meaningful thing; one interviewee suggested that "having to take a meeting with a lawyer was a bad thing because it probably meant you did something wrong."[194]

But the interviews suggested that the lack of interaction between the technology teams, on the one hand, and everyone else, on the other, was a pattern. As noted above, many technologists at these companies work in teams that consist primarily of other engineers. The teams are also run by engineers, and the tech lead's supervisor is also an engineer. "It was very easy," one former employee at Facebook noted, "for me to go an entire year without talking to anyone who wasn't also an engineer or computer programmer."[195] A product manager who started as a coder for a large technology company said that although "I didn't realize this when I started, but I've found it to be true and was probably true of me: programmers don't want to be bothered by other people at their job."[196] An engineer who has been through several job transitions in Silicon Valley and elsewhere also noted that independence is part of how these jobs are marketed to computer science graduates. As she explained, "They will give you money, food, and ping pong tables, you know what I mean, but the most important thing, at least to me, they tell you is that you will be independent. You will have time to be

189. Silicon Valley engineer (4) interview, *supra* note 107.

190. Interview with former programmer at New York start-up, New York, NY (June 24, 2016) (notes on file with Author).

191. Telephone interview with senior Silicon Valley engineer (Oct. 8, 2016) (notes on file with Author).

192. Google and Microsoft engineer interview, *supra* note 124.

193. Former general counsel at New York technology company interview, *supra* note 139.

194. Interview with web designer, *supra* note 145.

195. Telephone interview with former Facebook employee (Oct. 12, 2016) (notes on file with Author).

196. Telephone interview with former coder at large technology company (Sept. 12, 2016) (notes on file with Author).

creative, and you will solve these awesome engineering problems, and we're not going to get in your way."[197] This resonates with what we know about leading technology companies like Google. The company is famous for a nonhierarchical structure,[198] independent engineering teams, and the so-called "Google 20% time," or the promise that technologists can set aside 20% of their time to work on their own creative projects.[199] It makes sense, then, that technologists might just not interact with lawyers and privacy professionals, but also remain separated from other types of employees, as well.

This lack of interaction has effects on the design process. During my talks with attorneys, many of them ably recognized even subtle privacy issues associated with new technologies, particularly their retail clients' strategy to link loyalty programs with facial and biometric tracking. But when asked how they advise their clients about their privacy obligations, they took a passive role. "Unless someone raises the issue to me, there's nothing I can do," noted a partner with several years of privacy counseling experience.[200] In-house lawyers who are naturally closer to the design process than outside counsel admitted this, as well. "We would let them come to us," several attorneys employed by technology companies said. Although the attorney's "door was always open, and I'm there to help," many in-house attorneys tasked with advising design teams waited for the designers themselves to take the first step.[201] But if the technologists are not equipped to do so, then privacy issues never get to a privacy professional's desk. Another attorney stated, "It's not my job to challenge the design process. My job is to make sure what they tell me they're doing is compliant with the law." And outside

197. Telephone interview with former engineer at Silicon Valley technology company (1) (May 30, 2016) (notes on file with Author).

198. *See, e.g.*, DOUGLAS EDWARDS, I'M FEELING LUCKY: THE CONFESSIONS OF GOOGLE EMPLOYEE NUMBER 59, 224–27 (2011) (discussing the early years of Google including a now-famous firing of all project managers in 2001); STEVEN LEVY, IN THE PLEX: HOW GOOGLE THINKS, WORKS, AND SHAPES OUR LIVES 158–60 (2011) (covering the origins of the nonhierarchical structure and its effects on creativity and innovation).

199. *See* LASZLO BOCK, WORK RULES!: INSIGHTS FROM INSIDE GOOGLE THAT WILL TRANSFORM HOW YOU LIVE AND LEAD 135–36 (2015). Notably, the "20 percent time" may be mostly imaginary. But, as Bock explains in his book, the "idea" of the 20 percent time is more important than its actual existence or use. "It operates somewhat outside the lines of formal management oversight, and always will, because the most talented and creative people can't be forced to work." *Id*. at 136. *See also* Nicholas Carlson, *The 'Dirty Little Secret' About Google's 20% Time, According To Marissa Mayer*, BUS. INSIDER (Jan. 13, 2015), http://www.businessinsider.com/mayer-google-20-time-does-not-exist-2015-1.

200. Interview with senior associate at AmLaw Top 100 law firm (2) (July 29, 2016) (notes on file with Author).

201. Interview with in-house attorney at major technology company (Aug. 8, 2017) (notes on file with Author).

lawyers rarely talk to engineers to get that information. That same attorney noted that he spends most of his time "talking to the CPO and the general counsel. No one wants me talking to an engineer. I need the CPO filter to translate what the engineer does into language I can understand."[202]

*5. Implications.* These interviews allude to a narrative running in parallel to that of the CPOs in *Privacy on the Ground*. Although not all technologists and lawyers think about and operationalize privacy in the same way, this research suggests that the narrative describe in *Privacy on the Ground* may not yet be fully realized. Rather, at some companies, a narrow understanding of privacy may be factoring into the design on the ground. That may help explain the privacy gaps in platforms like Snapchat and Pokémon Go. In addition, the very existence of this trend has several implications for privacy law and privacy's place in society. I will touch on four related points here, focusing on the impact on theory, law, organizations, and individuals.

First, although some scholars rightly argue that privacy means different things in different contexts, thus making a single definition of privacy hard to pin down, the concept's continued ambiguity is having real effects on the ground. Daniel Solove, for example, has argued that reducing privacy to a single common denominator misses important aspects of privacy that are relevant in some contexts and not others.[203] Therefore, we should recognize that different invasions of privacy implicate a series of privacy values, sometimes overlapping and sometimes distinct.[204] More recently, Helen Nissenbaum further developed this point. Like Solove, who argued that privacy was a part of social practice, Nissenbaum noted that the propriety of revelation of someone else's information varies with context. Because different social interactions are governed by evolving norms informed by law, history, and culture, our expectations as to what should happen to our information varies by context, as well.[205]

These theories of privacy aptly capture a decidedly contextual phenomenon, but they leave privacy open to attack as ambiguous. And ambiguous concepts are hard to administer in the courts and on the ground. When it comes to the law on the books, the lack of strong,

---

202. Interview with partner at AmLaw Top 50 law firm (2) (Aug. 19, 2016) (notes on file with Author).

203. *See* Solove, *Conceptualizing Privacy*, *supra* note 17, at 1092, 1127–29.

204. *See id.* at 1145–47; SOLOVE, UNDERSTANDING PRIVACY, *supra* note 117, at 8–11, 171–98.

205. *See* NISSENBAUM, *supra* note 43, at 134–35; Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 138 (2004).

well-defined privacy norms allows competing rights, like free speech, take precedence.[206] And by leaving a vacuum that notice-and-choice has seemed to fill, robust conceptions of privacy have generally failed to benefit from law's powerful expressive capacity.[207] When it comes to privacy on the ground, privacy's complexity hypnotizes technologists and lawyers. To many, privacy is too complex, "amorphous,"[208] and "subjective."[209] As such, it is difficult to integrate into product design. One of two simpler concepts—notice or security—fills the void: it is harder for a company to wrestle with evolving notions of consumer privacy than it is to draft a privacy policy, add encryption on the back end of a product, and claim its privacy responsibilities are complete. This suggests that privacy scholarship must take into account administrability, not just with respect to judges assessing privacy claims, all of whom have the benefit of deliberation,[210] but also with respect to privacy professionals, designers, and lawyers who need a relatively simple way of understanding the value and purpose of integrating user expectations about privacy into design.

A second, but related implication of this research is that the conflation of privacy and encryption appears to be crowding out lawyers' and privacy professionals' focus on consumer privacy. The legal community has been combining privacy and cyber security for some time; law firm privacy practices are often "privacy and cyber security" practices.[211] They may have learned this from the

206. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 518 (2001); Michael Froomkin, *CCR Symposium: The Right to Remain Anonymous Matters*, CONCURRING OPINIONS (Apr. 14, 2009), http://www.concurringopinions.com/archives/2009/04/ccr_symposium_t_1.html. *But see* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 U.C.L.A. L. REV. 1149, 154–55 (2005) (discussing and then critiquing the conventional discourse suggesting free speech and privacy conflict). *See also* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1408–09 (2000) (discussing the debate of free speech and privacy).

207. *See, e.g.*, Deborah Hellman, *The Expressive Dimension of Equal Protection*, 85 MINN. L. REV. 1, 3 n.10 (2000) (law is coercive and expressive of norms); Elizabeth S. Anderson & Richard M. Pildes, *Expressive Theories of Law: A General Restatement*, 148 U. PA. L. REV. 1503, 1570–71 (2000) (what the law is establishes a set of agreed upon values); 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).

208. Senior engineer at Uber interview, *supra* note 114.

209. Telephone interview with attorney at AmLaw Top 100 firm (6) (Oct. 6, 2016) (notes on file with Author). *See also* Glenn Chapman, *New Google Security Chief Looks for Balance with Privacy*, PHYS.ORG (Apr. 18, 2015), http://phys.org/news/2015-04-google-chief-privacy.html.

210. *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 110, at 78 (discussing the need to articulate the value of privacy so judges and policymakers can effectively weight it against countervailing interests).

211. *See, e.g.*, *Privacy and Cybersecurity*, PROSKAUER, http://www.proskauer.com/practices/privacy-cybersecurity/ (last visited Jan. 11, 2018); *Litigation: Cybersecurity and*

companies they represent. At Google, for example, privacy and security are blended together.[212] At Bloomberg LP, privacy and data security are grouped together under "risk and compliance,"[213] which reflects the view of the CPOs in Bamberger and Mulligan's study that privacy is about "managing risk."[214] Industry trade conferences do the same.[215] Even state governments address the issues together.[216]

But privacy and cyber security are not the same. Privacy is, at its core, about the social relationships governing disclosure between and among individuals and between users and the platforms that collect, analyze, and manipulate their information for some purpose (often for profit).[217] That is, ostensibly, why so many CPOs say they think about privacy in terms of trust.[218] Cyber security is far more about preventing, assessing, and addressing attacks on data safety and integrity. President Obama's Cyberspace Policy Review, for example, defined cyber security as "strategy . . . regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities . . . as they relate to the security and stability of the global information and communications infrastructure."[219] Legal scholars have offered similar definitions, focused on "criminality" and "espionage"[220] or "using computer

---

*Data Protection*, PAUL WEISS, https://www.paulweiss.com/practices/litigation/cybersecurity-data-protection.aspx (last visited Jan. 11, 2018)).

212. *See supra* notes 149–160 and accompanying text.

213. Paul Wood, Chief Risk and Compliance Officer at Bloomberg LP, oversees data security and privacy. Dan Doctoroff, *Our New Chief Risk & Compliance Officer*, BLOOMBERG (Dec. 19, 2013), https://www.bloomberg.com/company/announcements/our-new-chief-risk-compliance-officer/.

214. BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 68.

215. *See, e.g.*, PRIVACY+SECURITY FORUM, https://privacyandsecurityforum.com/ (last visited Jan. 11, 2018) ("The Privacy + Security Forum breaks down the silos of privacy and security by bringing together seasoned thought leaders.").

216. *See, e.g.*, *Washington State Announces Federal Cybersecurity Partnership, Office of Privacy and Data Protection*, GOVTECH. (Jan. 6, 2016), http://www.govtech.com/security/Washington-State-Announces-Federal-Cybersecurity-Partnership-Office-of-Privacy-and-Data-Protection.html.

217. *See* NISSENBAUM, *supra* note 43, at 71, 196; Waldman, *supra* note 18, at 561, 590–601 (privacy is a social concept about how we relate to and share with others and the rest of society).

218. *See supra* notes 61–64 and accompanying text. The connection between privacy and trust is a hot topic, of late. *See, e.g.*, Waldman, *supra* note 92, at 196–97; Richards & Hartzog, *supra* note 18, at 447 (protecting privacy can build trust between online platforms and consumers).

219. U.S. DEP'T. OF HOMELAND SEC., CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 2 (2010), https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf.

220. Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the*

technology to engage in activity that undermines a society's ability to maintain internal or external order."[221] Conflating the two often means that consumer privacy gets short shrift. Technology companies understand that a lack of cyber security is a threat to the bottom line,[222] and they drill that concern into their engineers. As several of them explained, the full breadth of their privacy-related work was to prevent their products from getting hacked. The non-security aspects of data privacy and consumer expectations were, at best, secondary.

Third, these interviews reveal the potential for technologists' ongoing resistance to input from others within the same organization. Although some senior engineers noted that, upon reflection, they would have welcomed input from privacy professionals,[223] many technologists pushed back on working with lawyers on design. Several noted that they "are the experts here."[224] Several junior and senior engineers felt that "lawyers do not belong in design"[225] beyond "telling us what to do so we don't go to jail."[226] One engineer noted that "the more other people, whether they be lawyers or marketing people or a budget guy, are at every step along the way during the design process, the more it's going to get off the rails, and then my team is going to get blamed for not meeting our goals."[227] This is a common struggle in large organizations. As Renato Orsato, a sustainability scholar, has argued, employee resistance to input and change can create an "arena in which an indeterminate struggle unfolds,"[228] hampering innovation and productivity.[229] Resolving this tension undoubtedly requires more than top-down input from a CPO or general counsel. Rather, it demands building in organizational learning into the network structure of the corporation.

---

*Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 235–36 (2010).

221. Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 381 (2007). For a comprehensive summary of these and other definitions of cybersecurity, as well as a cogent critique of the conventional wisdom, please see Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 591–95 (2011).

222. Bamberger & Mulligan, *Privacy on the Books*, *supra* note 1, at 276.

223. *See, e.g.*, Engineer at large sharing economy company interview, *supra* note 143.

224. Silicon Valley engineer (4) interview, *supra* note 107.

225. Google employee interview, *supra* note 156.

226. Interview with web designer, *supra* note 145.

227. Senior product manager interview, *supra* note 170.

228. Renato J. Orsato, Frank den Hond, & Stewart Clegg, *The Political Ecology of Automobile Recycling in Europe*, 23 ORG. STUD. 639, 654 (2002).

229. *See* Dean Bartlett, *Embedding Corporate Responsibility: The Development of a Transformational Model of Organizational Innovation*, 9 CORP. GOVERNANCE 409, 414 (2009).

Finally, the interviews with technologists paint a picture of isolated design teams, staffed almost entirely by engineers, making privacy decisions on the fly. In addition to this being an organizational concern,[230] it also exacerbates technology's bias problem. Designers, most of whom are men,[231] either consciously design for themselves or subconsciously design with all the implicit biases that come with them.[232] Like artificial intelligence systems that develop biases by learning from limited inputs,[233] technology product designers translate their own biases into the devices they create: products may fit in men's front pockets, but not women's; mobile assistants understand voice commands like "I'm having a heart attack," a health crisis plaguing mostly men, but not "I've been raped," a trauma more likely to befall a woman;[234] apps may offer benefits to those who permit constant, real time location tagging, but they miss the fact that continuous tracking makes cyberstalking easier;[235] dating tools may allow users to select "male" or "female" but not "queer";[236] and engineers may design online gaming platforms to satisfy 12–18 year-old boys, but neglect to program in safeguards that prevent, identify, and punish harassment,[237] most of which is

230. *See infra* Part IV.C.

231. Women remain a distinct minority among science and technology graduates employed in inventor roles at large corporations. *See* NAT'L SCI. FOUND., WOMEN, MINORITIES, AND PERSONS WITH DISABILITIES IN SCIENCE AND ENGINEERING Tbl. 5.1 (2015) (2012 statistics show that women receive bachelor's degrees in certain science fields at far lower rates than men, including computer sciences (18.2%), engineering (19.2%), physics (19.1%), and mathematics and statistics (43.1%)); U.S. DEP'T OF LABOR, BUREAU OF LABOR STATISTICS, WOMEN IN THE LABOR FORCE: A DATABOOK 35–36 (2014) (39% of chemists and material scientists are women; 27.9% of environmental scientists and geoscientists are women; 15.6% of chemical engineers are women; 12.1% of civil engineers are women; 8.3% of electrical and electronics engineers are women; 17.2% of industrial engineers are women; and 7.2% of mechanical engineers are women).

232. *See* Crawford, *supra* note 162.

233. *See* Jeff Larson, Julia Angwin, & Terry Parris, Jr., *How Machines Learn to be Racist*, PROPUBLICA (Oct. 19, 2016), https://www.propublica.org/article/breaking-the-black-box-how-machines-learn-to-be-racist?word=cat.

234. Adam S. Miner et al., *Smartphone-Based Conversational Agents and Responses to Questions About Mental Health, Interpersonal Violence, and Physical Health*, 176 JAMA INTERNAL MED. 619, 621–22 (2016).

235. *See* Aarti Shahani, *Smartphones Are Used To Stalk, Control Domestic Abuse Victims*, NPR (Sept. 15, 2014, 4:22 PM), http://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

236. *See* Rena Bivens & Oliver L. Haimson, *Baking Gender Into Social Media Design: How Platforms Shape Categories for Users and Advertisers*, 2016 SOCIAL MEDIA + SOCIETY 1, 3–7 (2016); Rena Bivens, *The Gender Binary Will Not Be Deprogrammed: Ten Years of Coding Gender on Facebook*, 19 NEW MEDIA & SOC'Y 1–2 (2015).

237. *See* Keith Stewart, *Brianna Wu and the Human Cost of Gamergate: 'Every Woman I Know in the Industry is Scared'*, THE GUARDIAN (Oct. 17, 2014), http://www.theguardian.com/technology/2014/oct/17/brianna-wu-gamergate-human-cost.

based on gender.[238] These design omissions may not be purposeful or malicious; rather, they stem from designers' failure to appreciate the distinct needs of marginalized populations not often represented in the design process. The narrative described in this Article suggests that the demographics of technology design teams within the corporate organization may contribute to and metastasize the discriminatory effects of implicit bias in design. Therefore, embedding a robust, user-focused conception of privacy into the design of technology products would not just align data collection with user expectations. It would also have salutary effects on social norms and social equality.

## IV. EMBEDDING ROBUST PRIVACY NORMS INTO DESIGN

Bamberger and Mulligan began a research agenda about how technology companies are approaching consumer privacy. I sought to determine if the narrative they found had been fully realized. Relying on a series of interviews with technologists and lawyers, this Article has so far shown that the robust "company law" of privacy envisioned by the CPOs in *Privacy on the Ground* may not yet have trickled down to those designing technology products. At least among those interviewed, privacy was either limited to notice or crowded out by cyber security. And corporate privacy structures either encouraged the minimization of privacy or stayed out of the fray all together. The top-down approach, fueled by industry self-regulation, may not be working. Although I do not mean to suggest that every view of every technology product designer is reflected in these interviews, this research raises the question of whether more needs to be done to get engineers on board with privacy as part of the design process.

Historical evidence and sociological studies of corporate organizations suggest that embedding robust norms about consumer demands that go beyond mere compliance with legal requirements requires facilitating organizational learning. That is, both organizational structures and the people that work in them must adapt. They can do this through a multilevel comprehensive approach that addresses all barriers to norm diffusion, both within the corporation and in the social context in which it operates. This approach, illustrated in Figure 1, recognizes that organizational norms are the products of four

238. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 13–17 (2014) (cyberharassment is often a gendered and sexualized phenomenon plaguing mostly women).

outstanding influences.[239] Situated within a socio-legal context, corporations are influenced by (1) scholarship and media narratives conceptualizing their obligations, and (2) the web of laws, court decisions, rules, and real and threatened litigations that constitute the regulatory environment in which they, and their competitors, exist.[240] As a collection of individuals working toward the same goal,[241] corporations are also influenced by endogenous factors, including (3) the corporate structure that sets the frame for business routines and practice, and (4) the embodied experiences of the real people doing the real work in the company's name.[242] Of course, many of these influences overlap, but each works together to embed norms throughout the corporation. The balance of this Article approaches the problem of integrating privacy norms into design through this four-tiered lens. In each section, the Article shows how the current lack of embedded privacy norms can be partially explained by gaps at each level. Then, using historical examples of organizations adapting to meet changing legal and consumer expectations, as well as research into organizational learning, I suggest changes at each level that can help spread strong beliefs in consumer privacy among designers on the ground.

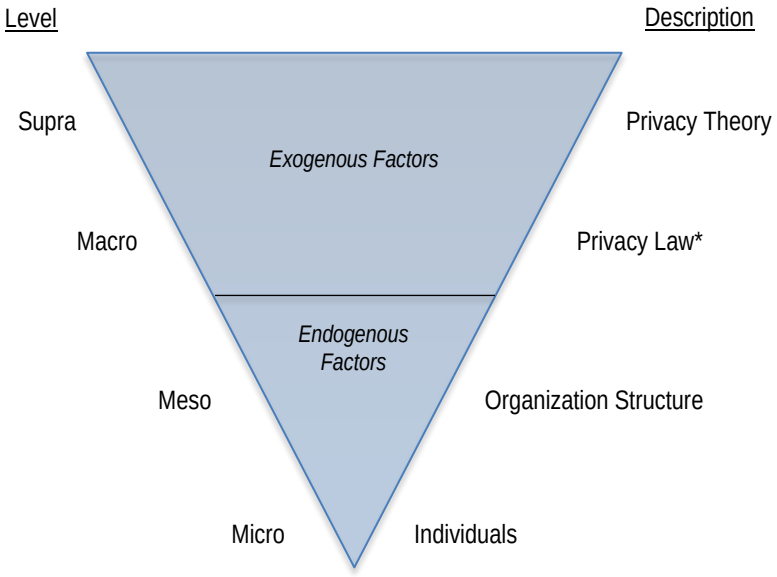
239. This framework is adapted from work by Ruth Aguilera, a sociologist of business and organizations, to understand why businesses engage in corporate social responsibility programs that are not necessarily profit-oriented. *See* Ruth V. Aguilera et al., *Putting the S Back in Corporate Social Responsibility: A Multilevel Theory of Social Change in Organizations*, 32 ACAD. MGMT. REV. 836, 836–37 (2007). Although there are differences between encouraging technology companies to embed privacy into design and, say, pushing companies to engage in socially beneficial initiatives, both require changes in organizational norms away from a strict, profit-only perspective. Therefore, organizational learning is important in both scenarios.

240. That other corporations in the same industry are similarly regulated characterizes the context in which a given corporation responds to regulatory or social demands. *See* DiMaggio & Powell, *supra* note 78, at 149.

241. *See* Andrew C. Inkpen & Eric W. K. Tsang, *Social Capital, Networks, and Knowledge Transfer*, 30 ACAD. MGMT. REV. 146, 148 (2005) (corporations are vertical, structured networks of people operating under a unified corporate identity).

242. "Embodied" experience, or the idea that humans cannot divorce mental cognition from physical life, emphasizes the practical, behavioral experiences of real people interacting in contextual social situations. *See* GEORGE LAKOFF & MARK JOHNSON, PHILOSOPHY IN THE FLESH: THE EMBODIED MIND AND ITS CHALLENGE TO WESTERN THOUGHT 19, 21–22 (1999); MAURICE MERLEAU-PONTY, THE ESSENTIAL WRITINGS OF MERLEAU-PONTY 47–80, 138–81 (Alden L. Fisher ed., 1969); MAURICE MERLEAU-PONTY, PHENOMENOLOGY OF PERCEPTION 207 (Colin Smith trans., 1962). In this context, this means that engineers do not exist in vacuums: they approach the world and do their work as fully realized embodied individuals, with unique backgrounds and biases.

Figure 1:
Illustration of Multilevel Approach to Organizational Learning




* U.S. federal law and state laws with national implications.

## *A. Conceptualizing Privacy for Design*

Theory can offer professionals on the ground a solid intellectual foundation for understanding their work and its role in society at large.[243] It can also drive the media narrative that shapes consumer expectations. The CPOs that spoke with Bamberger and Mulligan recognized this implicitly when they discussed the importance of conceptualizing privacy in such a way as to allow them to influence corporate priorities.[244] To these CPOs, privacy was a constantly evolving notion bound up with user expectations and the trust between users and the company. The outside lawyers and technologists I interviewed, however, understood privacy far more narrowly, as either limited to notice or synonymous with data security. To bring the latter more in line with the former requires scholars to recognize the doctrinal connection between privacy and trust.

243. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 110, at 78.

244. *See* BAMBERGER & MULLIGAN, PRIVACY ON THE GROUND, *supra* note 1, at 59–68.

Traditional privacy scholarship, much of which has focused on the right of individuals to maintain their autonomy, control over information, and separation from the prying eyes of government and society, does not do that.[245] It should come as little surprise, then, that the law on the books[246] and practitioners on the ground[247] see privacy through an autonomy lens, as well. But in a world where sharing data is often a necessary prerequisite for online interaction and where powerful internet companies collect, use, and analyze massive amounts of information in ongoing interactions with their users, concepts like control and autonomy are inadequate. They fail to appreciate the relational aspects of data flows.[248] More specifically, as I have argued elsewhere, users hand over personal information to online platforms in contexts characterized by trust, vulnerability, and an asymmetry of power.[249] Therefore, building on Dan Solove's and Helen Nissenbaum's work on the contextual, relational aspects of privacy, I argue that, like the CPOs in *Privacy on the Ground* suggested, privacy should be understood as a social concept based on relationships of trust.

Trust is a resource of social capital between or among two or more parties concerning the expectations that others will behave according to accepted norms.[250] It is the "favorable expectation regarding other people's actions and intentions,"[251] or the belief that others will behave in a predictable manner. For example, if I ask a friend to hold my spare set of keys, I trust she will not break in and steal from me. When an individual speaks with relative strangers in a support group like Alcoholics Anonymous (AA), she

245. Samuel Warren and Louis Brandeis, whose Harvard Law Review article began the privacy discourse, understood privacy as a right "to be let alone." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890). The seminal privacy law scholar Alan Westin took a similar autonomy-based approach, seeing 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." ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). For comprehensive reviews of the autonomy roots of many traditional theories of privacy, *see generally* Cohen, *supra* note 206; Waldman, *supra* note 18, at 565–88.

246. *See supra* Part II.A.

247. *See supra* Part III.B.2.

248. *See* NISSENBAUM, *supra* note 43.

249. *See generally* Waldman, *supra* note 18.

250. Alejandro Portes & Julia Sensenbrenner, *Embeddedness and Immigration: Notes on the Social Determinants of Economic Action*, 98 AM. J. SOC. 1320, 1332 (1993).

251. Guido Möllering, *The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension*, 35 SOC. 403, 404 (2001). *See also* Ken Newton and Sonja Zmerli, *Three Forms of Trust and Their Association*, 3 EUR. POL. SCI. REV. 169, 171 (2011); J. David Lewis & Andrew Weigert, *Trust as Social Reality*, 63 SOCIAL FORCES 967, 968 (1985).

trusts that they will not divulge her secrets.[252] Trust, therefore, includes a willingness to accept some risk and vulnerability toward others and steps in to grease the wheels of social activity:[253] I cannot know for certain that my neighbor will not abuse her key privileges or that my fellow support group members will keep my confidences, so trust allows me to interact with and rely on them. And, breaches of those relationships—when neighbors break in or when AA members share outside the group—are breaches of trust.

Information is exchanged with technology products and platforms on similar terms.[254] We key in our credit card numbers, financial information, and sexual preferences with the expectation that commercial websites, online banks, and dating platforms will keep our confidences. When they do not, it is primarily our trust that has been violated, not our right to control information or keep secrets, both of which we ceded long before the breach.[255]

Conceptualizing privacy this way would bring privacy theory in line with the views of the CPOs in Bamberger and Mulligan's research. It would give them an intellectual foundation upon which to argue that protecting consumer privacy is an ongoing responsibility based on the relationship between sharers and data collectors rather than something to be crossed off a list of priorities after drafting a privacy notice. The latter is a direct reflection of autonomy-based privacy definitions. Privacy-as-trust, however, means making privacy protection an integral part of companies' ongoing relationships with their consumers.

### *B. Privacy Law as an Incentive to Act*

Several interviews alluded to the fact that gaps in U.S. law ensured that consumer privacy would remain a low priority. Even when privacy issues were raised, lawyers and executives relied on "the fairly low risk of an enforcement action from the FTC" as a rationale for not pushing engineers to change design.[256] That must change. Understanding the connection between privacy and trust

---

252. See Understanding Anonymity, https://www.aa.org/pages/en_US/understanding-anonymity (last visited Jan. 8, 2018).

253. *See* NIKLAS LUHMANN, TRUST AND POWER 4 (1979).

254. As Jack Balkin notes, obligations exist between two parties not because of the content of those obligations, but because the relationship is enforceable through some legal tool, i.e., a contract or, in the data sharing context, Balkin argues, a fiduciary relationship. *See* Balkin, *supra* note 20, at 1205 n.104.

255. Dan Solove calls this problem the "secrecy paradigm," where privacy rights are extinguished upon revelation on the theory that once a piece of information is shared with others, it can no longer be considered private. *See* SOLOVE, *supra* note 20, at 42–43, 143.

256. Former general counsel at New York technology company interview, *supra* note 139.

has several implications for privacy law that can help embed strong privacy norms into technology product design.[257] Expectations of trust form the basis for the law to treat some data collectors as fiduciaries of our information.[258] In addition, a strong privacy tort regime could vindicate our rights and incentivize companies to take our privacy seriously. We have seen this work before. Citizen tort litigation pushed the automobile and pharmaceutical industries to embed consumer safety into car and drug designs. The same can now be done for privacy. In addition, many of the interviews I conducted with technologists that took their privacy obligations seriously worked at companies that had been on the receiving end of strong, disruptive regulatory interventions. This opens a path for the FTC to play an even more significant role in incentivizing companies to design consumer privacy protections into their products.

Treating some data collectors as information fiduciaries, as Jack Balkin has suggested, would go far toward incentivizing companies to integrate privacy into design. Fiduciaries are those that have special obligations of loyalty to another.[259] Those loyalties are based on trust: a trustor, client, or beneficiary hands over money, control, and information to another, who, in turn, has a duty not to betray that trust.[260] Therefore, if we recognize that the exchange of personal information depends upon similar relationships of trust and confidence, many technology companies can be seen fiduciaries of our data.[261] This is true for the same reasons money managers, estate trustees, and doctors are fiduciaries. First, our relationship with many online platforms is asymmetrical: Facebook and Amazon, for example, know a lot about us; we know very little about how their algorithms use our data.[262] Second, we are completely dependent on these platforms for a variety of social, professional, commercial, informational, educational, and financial services. And we use them with the expectation that they will not misuse our data in the process. Third, many online platforms are experts at what they do: Google's

257. *See, e.g.*, Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 349 (1997) (discussing how law can influence norms).

258. *See generally* Balkin, *supra* note 20.

259. *See* TAMAR FRANKEL, FIDUCIARY LAW 4 (2011).

260. *Id.* at 4, 106–08.

261. Jack Balkin refers to these companies as "information fiduciaries." Balkin, *supra* note 20, at 1209. *See also* Richards & Solove, *supra* note 21, at 156–58.

262. Balkin, *supra* note 20, at 1222. *See also* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015) (discussing the "black box" of information algorithms).

search and OK Cupid's matching algorithms are supposedly the best around, and they market themselves that way. Therefore, we hand over our information—from our search histories to intimate sexual desires—to these platforms in exchange for some benefit, trusting them to use our data in ways we expect.[263] Given these similarities, it makes logical sense to treat such platforms as fiduciaries of our information and hold their feet to the fire when, if ever, they violate their duty of loyalty.

Though sometimes overlapping with fiduciary law,[264] tort law offers a parallel track for vindicating the privacy rights of victims of privacy-invasive design. To date, though, it has mostly failed in that regard: data breach and invasion of privacy victims rarely have standing to sue the companies that are supposed to keep their data private, so their cases are dismissed even when a company negligently caused a data breach.[265] This allowed Google, for example, to avoid responsibility for violating a do-not-track promise because the plaintiffs could not demonstrate how tracking actually hurt them.[266] And it has allowed companies that leave their databases open to hacks and other cyberattacks to avoid tort liability because, absent direct evidence that hackers used a plaintiff's data to harm her financially, data breach claims are merely "allegations of hypothetical, future injury."[267]

These standing problems have neutered what should be an effective incentive for companies to act on privacy. We have seen tort law serve this function before. For example, when Americans first began driving cars, they did so in a regulatory void. There was also little social demand for corporate responsibility for automotive safety.[268] Ralph Nader's 1965 book, *Unsafe at Any*

263. Balkin, *supra* note 20, at 1222.

264. *See* FRANKEL, *supra* note 259, at 240–41 (fiduciary duties and tort obligations have certain similarities, but should be considered distinct).

265. *See, e.g.*, Dwyer v. American Express, 652 N.E.2d 1351, 1352–53 (Ill. App. 1995). After learning that American Express designed a system to track cardholder spending habits, aggregate that data, and create detailed user profiles for targeted advertising, several cardholders objected, arguing that the company intruded into their private information and appropriated it without their consent. The court disagreed on both counts. The information was not private, having already been handed over to American Express every time a card was used to make a purchase. *Id*. at 1354. And, in any event, cardholders never suffered any cognizable injury: customer tracking and profiling did not "deprive any of the cardholders of any value their individual names may possess." *Id*. at 1356.

266. *In re* Google, Inc. Cookie Placement Privacy Litig., 988 F. Supp. 2d 434, 442 (D. Del. 2013).

267. Reilly v. Ceridian Corp., 664 F.3d 38, 41 (3d Cir. 2011).

268. *See* MICHAEL R. LEMOV, CAR SAFETY WARS: ONE HUNDRED YEARS OF TECHNOLOGY, POLITICS, AND DEATH xiii (2015); MARTIN ALBAUM, INS. INST. FOR HIGHWAY SAFETY, SAFETY SELLS: MARKET FORCES AND REGULATION IN THE DEVELOPMENT OF

*Speed: The Designed-In Dangers of the American Automobile*, changed that. Outraged that Chevrolet both sold the Corvair knowing its dangers and refused to design in life saving tools,[269] the public pushed Congress to act[270] and started bringing consumer safety lawsuits against carmakers. For fifty years before *Unsafe at Any Speed*, carmakers' only obligation was to make cars "free from hidden defects."[271] That changed in 1968, when, via a negligence action against General Motors, a court imposed on automakers a duty of reasonable care to design cars that would "avoid subjecting the user to an unreasonable risk of injury" during a collision.[272] Private tort litigation continued to vindicate consumer demands for safe automobiles[273] and forced carmakers to improve fuel tank safety,[274] protect drivers against side impact crashes,[275] and design better seat belts,[276] roofs,[277] doors,[278] and much more.[279] Tort cases had similar effects on drug safety.[280]

These cases pushed companies to integrate safety into design as a matter of course. It worked for three reasons. First, many of these cases resulted in significant settlement costs, incentivizing companies to take preventative action to avoid devastating,

---

AIRBAGS 1 (2005).

269. RALPH NADER, UNSAFE AT ANY SPEED: THE DESIGNED-IN DANGERS OF THE AMERICAN AUTOMOBILE 86 (1965).

270. *See* Kevin M. McDonald, *Judicial Review of NHTSA-Ordered Recalls*, 47 WAYNE L. REV. 1301, 1302 (2002). Congress passed, and President Johnson signed, the National Traffic and Motor Vehicle Safety Act and the Highway Safety Act in 1966. *See id.* at 1304. Highway safety regulation was tasked to the new National Highway Safety Bureau, later renamed the National Highway Traffic Safety Administration. *See id.* at 1305–06.

271. Evans v. Gen. Motors Corp., 359 F.2d 822, 825 (7th Cir. 1966).

272. Larson v. Gen. Motors Corp., 391 F.2d 495, 502 (8th Cir. 1968).

273. *See, e.g.*, Dyson v. Gen. Motors Corp., 298 F. Supp. 1064 (E.D. Pa. 1969) (car companies must design "a reasonably safe container within which to make [a] journey").

274. *See* Grimshaw v. Ford Motor Co., 119 Cal. App. 3d 757 (Cal. Ct. App. 1981). This case concerned the infamous Ford Pinto, which had a tendency to explode.

275. Dawson v. Chrysler Corp., 630 F.2d 950 (3d Cir. 1980).

276. AlliedSignal, Inc. v. Moran, 231 S.W.3d 16 (Tex. App.—Corpus Christi 2007, pet. granted, judgment vacated w.r.m.).

277. Shipler v. General Motors Corp., 710 N.W.2d 807 (Neb. 2006).

278. Seliner v. Ford Motor Co., No. 2002-30454 (Tex. Dist. Ct. 2004).

279. *See* AM. ASSOC. FOR JUSTICE, DRIVEN TO SAFETY: HOW LITIGATION SPURRED AUTO SAFETY INNOVATIONS 4–9 (2010).

280. *See, e.g.*, Sindell v. Abbott Labs., 607 P.2d 924, 925–27 (Cal. 1980) ("During the period defendants marketed DES, they knew or should have known that it was a carcinogenic substance, that there was a grave danger after varying periods of latency it would cause cancerous and precancerous growths in the daughters of the mothers who took it, and that it was ineffective to prevent miscarriage. Nevertheless, defendants continued to advertise and market the drug as a miscarriage preventative. They failed to test DES for efficacy and safety.").

company-threatening damages.[281] Second, private tort litigation supplemented overworked and underfunded regulatory structures. The National Highway Traffic Safety Administration, the federal agency tasked with developing rules for car and driver safety, is small, subject to budgetary and staffing limitations, and at risk of regulatory capture.[282] As recently as 2014, its few staffers were responsible for dealing with up to 80,000 complaints per year.[283] Legitimate complaints were missed. Tort litigants rushed in to fill the void. Third, the high-profile nature of tort lawsuits resulting in damage awards allowed these cases to have an expressive effect. By becoming part of the governing legal and media discourse about technology, industry, and corporate social responsibility, these cases helped solidify safety expectations among members of the public and forced even recalcitrant companies to act.[284]

Today, consumers interested in protecting their privacy do not benefit from any of these factors. Data collectors rarely pay damages in privacy tort cases, leaving the understaffed FTC to protect consumer privacy on its own. And popular opinion on corporate privacy responsibility is, like the technologist's vision of privacy, limited to data security. Data breaches that affected Target, Sony, and others receive significant press; the privacy issues associated with social networks, data aggregation, and black box and predictive algorithms do not. A robust tort regime can change that. As Dan Solove and Danielle Citron argue, courts should recognize the intangible, but no less damaging, harms associated with data breaches and invasions of privacy.[285] There is, after all, much precedent for them to follow.[286] And by

281. For example, *Grimshaw*, the Ford Pinto case, resulted in damages, later reduced, of $125 million. Grimshaw v. Ford Motor Co., 119 Cal. App. 3d 757, 771, 772 n.1 (Cal. Ct. App. 1981).

282. *See, e.g.*, Dan Becker & James Gerstenzang, *Safety Sacrificed in NHTSA Revolving Door*, USA TODAY (Feb. 25, 2015, 8:02 AM), http://www.usatoday.com/story/opinion/2015/02/25/nhtsa-revolving-door-cronyism-highway-column/23966219/ (citing inspector general report).

283. *See* Scott Evans, *How NHTSA Missed the GM Ignition Switch Defect*, MOTORTREND (June 15, 2015), http://www.motortrend.com/news/how-nhtsa-missed-the-gm-ignition-switch-defect/.

284. Famous tort cases are not only taught to all law students in their Torts or Products Liability classes. They are part of popular culture: books and movies have been made about many. *See, e.g.*, JONATHAN HARR, A CIVIL ACTION (1995) (based on the *Anderson v. Cryovac*, the trichloroethylene toxic tort case in Woburn, Massachusetts); A CIVIL ACTION (Touchstone Pictures 1998).

285. *See* Daniel J. Solove & Danielle Keats Citron, *Privacy and Data Security Harms* (forthcoming) (manuscript on file with Author).

286. Courts have been recognizing intangible, emotional, and other non-pecuniary harms for decades. Indeed, Warren and Brandeis spent most of their article, *The Right to*

vindicating these more intangible privacy rights, a renewed privacy tort regime can ensure that companies that collect data bring their privacy obligations out from under the shadow of data security.

The capacity for law to influence design does not stop at fiduciary duties of loyalty and tort duties of reasonable care. Over the course of several interviews at major technology companies, I found that many of the designers who expressed a commitment to integrating privacy into design reflected on the impact of regulatory enforcement on their employers. "I've been here a long time, and we remember what it was like" under a consent decree. "No one wants to be the one who's responsible for that happening again. We just don't want to mess this up."[287] Another designer who works in artificial intelligence said bluntly: "We take this seriously, from my team all the way up to" the CEO of the company "because we don't want that happening again, and it's on us to make sure it doesn't."[288]

But not all consent decrees are created equal. Google has been the subject of an FTC order,[289] and so has Facebook.[290] Neither have particularly good reputations for protecting user privacy and, with respect to Google, many of its current and former engineers report that the company's vaunted privacy structures are relatively weak or inert.[291] Strong regulatory interventions that require more than a "comprehensive privacy program," together with executive- and management-level commitments to compliance, appear to be more effective. My interviews showed that employees working at companies who have experienced such powerful orders were far more capable of articulating specific ways they integrate privacy into design than those at companies where regulatory orders involved simple fines or one or two new hires. This suggests that the FTC should not be shy about imposing significant penalties and demanding comprehensive, specific

---

*Privacy*, proving that the common law has evolved to recognize intangible harms. *See* Warren & Brandeis, *supra* note 245, at 193–94.

287. Interview with engineer at major technology company (Aug. 7, 2017) (notes on file with Author). The particular "consent decree" to which this interviewee referred is purposely omitted to maintain the confidentiality of the subject and his or her employer.

288. Interview with engineer focused on artificial intelligence at major technology company (Aug. 6, 2017) (notes on file with Author).

289. *See, e.g.*, Decision and Order, *In the Matter of Google, Inc.*, F.T.C. File No. 102 3136, Docket No. C-4336 (F.T.C. Oct. 13, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

290. *See, e.g.*, Agreement Containing Consent Order, *In the Matter of Facebook, Inc.*, F.T.C. File No 092 3184 (F.T.C. Nov. 29, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf.

291. *See supra* notes 149–160 and accompanying text.

structural changes to companies that violate their users' privacy expectations.

### *C. Organizational Structure and Organizational Learning*

So far, we have discussed the role played by privacy theory and the legal relationship between users and data collectors—exogenous forces that help map the context in which technology companies operate—in pushing those companies to embed trust-based privacy norms into design. The next two sections address endogenous factors—corporate organization and the embodied experiences of technology workers themselves—and show how both may hinder the diffusion of norms throughout a given company. Changes that enhance organizational learning and expose engineers to new people, new ideas, and new perspectives, however, can make it more likely all parties in the design process share the same vision for privacy.

Again, history is a guide. Sociological and management studies on the integration of social responsibility priorities into the corporate ethos, practice, and routine point to several organizational steps companies can take to change the status quo. Corporations, like all organized bureaucracies dedicated to achieving a particular purpose,[292] use routines and internal practices to achieve their desired results and reduce uncertainty, mistakes, and deviation along the way.[293] Sometimes, though, structures become ossified and stifle innovation.[294] But corporate organization can be nudged to enhance organizational learning, or the process through which workers not only learn from each other, but also spread and embed new practices, new perspectives, and new norms.[295] In these ways, organizational learning will help the CPO's vision of privacy reach her workers on the ground. Based on that research and my interviews with technologists, three

292. *See* DiMaggio & Powell, *supra* note 78, at 147.

293. The seminal work on the emergence of deviance, or behaviors that violate the norms of some group, in organizational practice is DIANE VAUGHAN, THE CHALLENGER LAUNCH DECISION: RISKY TECHNOLOGY, CULTURE, AND DEVIANCE AT NASA 58, 102–18, 148–52, 190–95, 405–09 (1996).

294. *See* DiMaggio & Powell, *supra* note 78, at 147 (bureaucracy is difficult to change once imposed).

295. *See* Amy C. Edmondson, *The Local and Variegated Nature of Learning in Organizations: A Group-Level Perspective*, *in* SOCIOLOGY OF ORGANIZATIONS: STRUCTURES AND RELATIONSHIPS 631 (Mary Goodwyn & Jody Hoffer Gittel eds., 2012) [hereinafter, ORGANIZATIONS]. *See also* François Maon, Adam Lindgreen, & Valérie Swaen, *Designing and Implementing Corporate Social Responsibility: An Integrative Framework Grounded in Theory and Practice*, 87 J. BUS. ETHICS 71, 71–72 (2008) (adoption of social responsibility strategy considered an organizational learning and change process).

structural limitations built into some corporate organizations have prevented robust privacy norms from reaching those designers: profit prioritization, departmental siloization, and instability in engineering staffing. This section addresses each in turn.

*Profit Prioritization and Company Climate*. My interviews suggested that many technology companies recognized the revenue implications of incomplete data security,[296] but not of poor consumer privacy. Indeed, the lack of internal corporate emphasis on privacy suggests that many companies approached it as another form of low-priority corporate social responsibility (CSR) while adopting the rhetoric of consumer privacy and trust.

CSR programs are company initiatives that do not necessarily generate revenue but improve social welfare in some way.[297] Companies create them for many reasons,[298] but they sometimes have to fight for attention against core corporate priorities.[299] This is particularly true for privacy. The collection, use, and sale of consumer data are often integral to technology companies' business models: Facebook and Google use personal data to sell targeted advertisements; dating websites promise compatible romantic matches in exchange for personal information and a monthly membership fee; and most online platforms collect data to optimize site performance and user experiences. Therefore, putting limitations on data collection would seem to be bad for business.

But contrary to conventional wisdom, privacy is actually good for business. Companies that rely on consumers sharing information with them and with each other need their consumers' trust.[300] Without trust, sharing stops.[301] And protecting our privacy is a central tool for gaining our trust, especially as we become more savvy Internet users. Even when privacy protections are seen as complications in a pure profit-seeking world based on data collection and analysis, protecting privacy can either give a company a competitive advantage on the market[302] or prove its

296. *See, e.g.*, *supra* notes 122–128 and accompanying text.

297. *See* Aguilera et al., *supra* note 239, at 836–37.

298. *See, e.g.*, Peter Arlow & Martin J. Gannon, *Social Responsiveness, Corporate Structure, and Economic Performance*, 7 ACAD. MGMT. REV. 235, 236 (1982) (chief executive interest, powerful social movements, for example).

299. *See, e.g.*, *id.* (reviewing literature showing only 1/5 of managers considered social responsibility a top five priority).

300. *See* Richards & Hartzog, *supra* note 18, at 454.

301. *See* Waldman, *Privacy As Trust*, *supra* note 18.

302. *See* Thomas M. Jones, *Instrumental Stakeholder Theory: A Synthesis of Ethics*

CSR bone fides. As Bamberger and Mulligan argued, it is the responsibility of the company's executives to recognizes these opportunities. The CPO or CEO must raise awareness internally about privacy, set the tone for corporate action, and establish guideposts for marking success or failure. This type of executive responsibility is nothing new: Ikea executives set the tone for addressing the company's use of child labor in the 1990s by talking about the company's responsibility in the media, embedding opposition to the practice in a mission statement, and discussing their commitment to fighting the practice with managers and other employees.[303] Apple's Tim Cook did the same during his company's fight with the FBI over the latter's attempt to conscript Apple to bypass security features on the iPhone of Syed Farook, the man who killed 14 and injured 22 people at the Inland Regional Center in San Bernardino, California.[304] In other words, executives, like the CPOs in *Privacy on the Ground*, have to establish what Martha Feldman and Brian Pentland called the "ostensive" aspect of a corporate routine on privacy, or the subjective understanding that consumer privacy is part of the corporate mission.[305]

Empirical evidence bears this out. Oshrat Ayalon, Eran Toch, Irit Hadar, and Michael Birnhack recently showed that a corporate climate dedicated to privacy has a more significant impact on designers than formal policies, legal decisions, or continuing education.[306] My interviews found the same: technologists at two different large technology companies, one with executives that take seriously issues like accessibility, social responsibility, and privacy, and one with executives that do not, had radically different approaches to integrating privacy into design. The former recognized privacy issues and evidenced a commitment to coming up with privacy fixes and even delaying or canceling product rollouts if it did not meet corporate privacy

*and Economics*, 20 ACAD. MGMT. REV. 404, 411, 421–22 (1995) (ethical behavior can help a company achieve competitive advantage on the market); Michael V. Russo & Paul A. Fouts, *A Resource Based Perspective on Corporate Environmental Performance and Profitability*, 40 ACAD. MGMT. J. 534, 535–36 (1997) (similar, focusing on environmental conduct).

303. *See* Maon, Lindgreen, & Swaen, *supra* note 295, at 78.

304. *See A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/; Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

305. Feldman & Pentland, *supra* note 78, at 101.

306. Oshrat Ayalon et al., *How Developers Make Design Decisions About Users' Privacy: The Place of Professional Communities and Organizational Climate*, *in* COMPANION OF THE 2017 ACM CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK AND SOCIAL COMPUTING (2017).

standards.[307] The latter generally found it difficult to conceptualize privacy, let alone integrate it into their work.

*Departmental Siloization*. Several engineers reported that their engineering teams were separated from other corporate departments, including privacy.[308] But siloization is fatal to the diffusion of norms throughout a company. As Andrew Inkpen and Eric Tseng showed, corporate structures that separate networks of individuals erode trust and, as a result, prevent the exchange of information.[309] We saw this happen at Google. Its large privacy and security structure was mostly separate from the engineering teams on the ground. As a result, several engineers resisted privacy professionals' input. Siloization also had a negative effect on the privacy team's work. Despite its robust structure, privacy at Google fell into a compliance role, with engineers briefly running their designs by privacy much like they would run them by the marketing or legal departments.[310]

Not all design teams are so siloed. Several technologists at a large financial services firm spoke of working on design teams that were fully integrated into the larger corporate structure. Each team included a "risk and security" representative as well as a non-technologist manager who was not only responsible for facilitating cross-departmental connections, but also "had the knowledge base and trust of the other people that [technologists] had to work with."[311] Another engineer continued:

> We worked in teams, obviously with other engineers, but also with artistic designers, security people, a product manager, and a finance guy. The finance guy actually surprised me, but his job was actually pretty essential: if we're designing for people like him, it was a great resource to have him in those [design] meetings.[312]

This comment alludes to a radically different approach to design than the one reflected in many of my interviews with technologists. Not only was this team connected to the larger network of the corporation, it also included a stand-in for users,

307. This is based on a series of interviews conducted with, among others, engineers and technologists at a large technology company over August 6 and 7, 2017 (notes on file with Author).

308. *See supra* Part III.B.2.

309. *See* Inkpen & Tseng, *supra* note 241, at 152–54.

310. *See supra* notes 157–160 and accompanying text.

311. Telephone interview with engineer at large financial services company (1) (Oct. 21, 2016) (notes on file with Author).

312. Telephone interview with engineer at financial services firm (2) (Oct. 26, 2016) (notes on file with Author).

allowing the team to design for its customer base rather than for the engineers themselves. As a result, this team's engineers learned from their coworkers.[313] One engineer explained that "it was great to have the guy with a finance background on the team; he taught me a few things about how [the product] is used."[314] That learning was reflected in design in real ways: "he was integral in changing . . . design. He told us about desk clutter, the speed with which his colleagues use [the product], when they use it and how. I wouldn't have known that stuff." Although this team's privacy member was really a "risk and security" expert, a privacy representative could raise consumer privacy issues much in the same way the finance professional raised issues from his own experience.[315]

*Instability in engineering staffing*. Engineers reported a high degree of turnover among their teams.[316] Such instability disrupts the diffusion and maintenance of strong organizational norms and culture.[317] As Amy Edmondson, an expert on the work of teams in corporate environments, has shown, frequent staffing changes make it difficult for members of teams to trust one another. And without some level of trust—in a worker' technical skill, dedication to the work, and commitment to others—team members do not have the confidence to reflect, ask challenging questions, and solve problems. Indeed, stable membership is essential for learning among team members: repeated interactions allow workers to share experiences and provide "psychological safety" for team members to challenge each other's assumptions.[318]

Attrition rates among engineers are high because of the demanding nature of the work at technology companies, where 80-hour weeks are routine.[319] Perks like Ping-Pong tables, fitness centers, on-site haircuts, and free food may attract new hires, but actually facilitate long hours in difficult conditions.[320] To date,

313. *See* Inkpen & Tseng, *supra* note 241, at 149, 154; Edmondson, *supra* note 295, at 632–33.

314. Financial services engineer (1) interview, *supra* note 311.

315. The integration of users into the design process is the subject of a long research agenda among sociologists of technology. For a collection of insightful essays on this topic, please see HOW USERS MATTER: THE CO-CONSTRUCTION OF USERS AND TECHNOLOGY (Nelly Oudshoorn & Trevor Pinch eds., 2005).

316. *See supra* note 161.

317. *See* Inkpen & Tseng, *supra* note 241, at 153.

318. *See* Edmondson, *supra* note 295, at 633.

319. *See, e.g.*, Jodi Kantor & David Streitfeld, *Inside Amazon: Wrestling Big Ideas in a Bruising Workplace*, N.Y. TIMES (Aug. 15, 2015), http://www.nytimes.com/2015/08/16/technology/inside-amazon-wrestling-big-ideas-in-a-bruising-workplace.html?_r=0.

320. *See also* David Auerbach, *I've Worked Insanely Demanding Tech Jobs*, SLATE

many technology companies approach their long hours as badges of honor and reflections of the high-achieving workers they hire. Plus, engineers can be replaced rather easily.[321] Doing so at high rates, however, makes it difficult for company norms to embed within design teams on the ground. A more effective effort at retention can help change that.

### *D. The Embodied Experience of Designers on the Ground*

Many of these organizational factors, which speak to the ability of a corporation as a whole to adapt and change, also apply to individual workers' capacity to learn from each other. Individual-level learning is, of course, essential to embracing new organizational norms up and down the corporate hierarchy.[322] Engineers are not just trained robots; they perform their jobs[323] with particular perspectives, cognitive frames, and embodied experiences that translate into the products they design. As the interviews reported in this Article suggest, that background can sometimes act as a barrier to the diffusion of robust privacy norms. Some interviewees reported rarely, if ever, interacting with coworkers who were not also engineers. Some noted that the demands on them were so significant and constant,[324] that when they were forced to make privacy-related decisions, they would fall back on their own judgment and education, the latter of which never included few, if any, references to privacy or ethics in design. Moreover, these engineers worked in teams whose members looked exactly like them: they came from the same backgrounds, schools, and family experiences.[325] Exposing engineers to new people and new ideas through changes in technology education and increased social interaction within the corporation, however, can help change that. This section addresses both of those pathways, in turn.

---

(Aug. 17, 2015, 4:02 PM), http://www.slate.com/articles/technology/bitwise/2015/08/amazon_abuse_of_white_collar_workers_i_worked_at_microsoft_and_google_and.html (noting the attrition rate among technology workers).

321. *See, e.g.*, Taylor Soper, *Analysis: The Exploding Demand for Computer Science Education, and Why America Needs to Keep Up*, GEEK WIRE (June 6, 2014, 10:51 AM), http://www.geekwire.com/2014/analysis-examining-computer-science-education-explosion/.

322. *See* Edmondson, *supra* note 295, at 632 (organizations cannot change when they ignore the experiences of their workers).

323. In Feldman's and Pentland's two-tiered framework for understanding corporate routines, executives establish the "ostensive" aspect, or guiding mission and understanding, of the routine, while workers on the ground "perform" the routine or translate the mission into practice. *See* Feldman & Pentland, *supra* note 78, at 101.

324. *See* Start-up programmer interview, *supra* note 141.

325. *See* Silicon Valley engineer interview, *supra* note 161.

The cognitive frames through which we see the world and approach new problems[326] are significantly influenced by our education. But most technology companies hire their engineers from the same schools, most of which neglect to include privacy and ethics in their curricula. I conducted a LinkedIn search for technology talent at Google, Facebook, and Apple and found that nearly 38% come from just the top 5 engineering and computer science programs in the United States, as rated by U.S. News and World Report.[327] Those curricula are quite similar, and notable in several respects.

The first notable characteristic of technology education in the United States is that there is severe demographic inequality in engineering and computer science faculties. The imbalance is worst at Stanford's electrical engineering department, where only 7 out of 63 faculty members are women (11.1%).[328] Stanford also has the worst gender imbalance in its computer science faculty, where only 5 out of 57 are women. That means there are nearly 12 men for every one woman. At the University of Illinois, which has the fifth highest ranked computer science program in the country, there are 13 women on a faculty of 74. MIT fares the best: 18.5% of its Electrical Engineering and Computer Science faculty are women.[329] Racial and ethnic diversity is even worse. There is not

326. *See, e.g.*, John L. Campbell, *Why Would Corporations Behave in Socially Responsible Ways? An Institutional Theory of Corporate Social Responsibility*, 32 ACAD. MGMT. REV. 946, 946–47 (2007) (discussing the literature).

327. To calculate this estimate, I searched for all LinkedIn members who listed "engineer" as their job and Google, Facebook, or Apple as a place of employment, either current or former. I then filtered those results by education, searching for the top 5 engineering and computer science programs, as listed by U.S. News and World Report. *See Best Undergraduate Engineering Programs*, U.S. NEWS AND WORLD REPORT, https://www.usnews.com/best-colleges/rankings/engineering (last visited Jan. 22, 2018); *Best Undergraduate Computer Engineering Programs*, U.S. NEWS AND WORLD REPORT, https://www.usnews.com/best-colleges/rankings/engineering-doctorate-computer (last visited Jan. 22, 2018). These data are imperfect: only a subset of technology talent at these companies have LinkedIn profiles and only a subset of them list their education. That said, the purpose of including this statistic is not to argue that it represents the entire population. My goal is more modest: to show that there is reason to believe there is a high concentration of engineering talent from the top 5 schools in the United States at major technology companies. This is not controversial. Max Nisen, *What Facebook, Twitter, Google, and Apple Employees Have in Common*, QUARTZ (Mar. 7, 2014), https://qz.com/183958/what-facebook-twitter-google-and-apple-employees-have-in-common/.

328. The gender imbalance at the other top 5 engineering programs is as follows: Berkeley's Electrical Engineering and Computer Science faculty and CalTech's Electrical Engineering faculty are only 12.5% women (17 out of 136 and 3 out of 24, respectively). At Georgia Tech's Electrical Engineering and Computer Science program, 13.2% of faculty are women (19 out of 143).

329. At Carnegie Mellon, 16 out of 101 (15.8%) are women. At Berkeley, 10 out of 84 (11.9%) are women.

a single black or Latino/a faculty member in CalTech's engineering department. Larger faculties are also homogeneous. At Berkeley's Electrical Engineering and Computer Science department, there is one black faculty member and not a single Latino/a. Illinois's computer science faculty has the same numbers (or lack thereof). In total, if you aggregate the faculties at the top five computer science schools, there are only seven black and twelve Latino/a faculty members. In engineering departments, there are ten black faculty members and only two Latino/as. There is not a single openly queer person on the electrical engineering and computer science faculties at any of the top five schools.[330]

But numbers tell only part of the story. Women who make it through the patriarchal gauntlet to find a technology job face hostility and discrimination when they get there. Studies show that women in technology careers are belittled, condescended to, ignored, and hear sexually harassing language in the office.[331] It is no wonder that although many young girls express interest in tech careers, only 11% of teenage women actually expect to go into the field.[332] And queer engineers are forced into the closet by

330. These imbalances manifest outside the classroom and help embed implicit biases. In March 2017, Goldman Sachs hosted a two-day technology conference in which 93% of the speakers were men. Matthew Zeitlin, *This Goldman Sachs Conference Has 76 Speakers and Only Five Are Women*, BUZZFEED NEWS (Mar. 10, 2017, 11:52 AM), https://www.buzzfeed.com/matthewzeitlin/this-goldman-sachs-conference-has-76-speakers-and-only-five?utm_term=.geNR2RKPK#.do0747ePe. The year before, there was an all-male panel on women's equality at Davos. Jessica Roy, *All-Male Panel About Women's Equality Not Exactly Equal*, THE CUT (Jan. 22, 2016, 9:00 AM), https://www.thecut.com/2016/01/davos-all-male-panel-on-womens-equality.html. PayPal did the same thing in April 2016. Dayna Evans, *Ah, Yes: Another All-Male Panel on the Issue of Gender Equality*, THE CUT (Apr. 21, 2016, 5:52 PM), https://www.thecut.com/2016/04/paypal-to-hold-all-male-panel-on-gender-equality.html. Male-only panels at technology conferences are so common that the phenomenon spawned a satirical blog ("Congrats, You Have an All-Male Panel!"), a game of Female Conference Speaker Bingo, and even a portmanteau ("manel"). *See* Congrats, You Have an All-Male Panel, http://allmalepanels.tumblr.com/;Elan Morgan, *Good Read: Jezebel's Female Conference Speaker Bingo*, GENDER AVENGER (Feb. 25, 2014), https://www.genderavenger.com/blog/2014/2/25/an-oldie-but-a-goodie-jezebels-female-conference-speaker-bingo. This isn't surprising, given the inequality that exists in the field, but it's easily remedied: there are literally thousands of women working in technology who can step in. Melanie Ehrenkranz, *Think There Aren't Any Qualified Women in Tech? Here are 1,000 Names. No More Excuses.*, MIC (May 2, 2017), https://mic.com/articles/175136/women-in-tech-1000-names-no-more-all-male-panels-conferences#.rUuZ3XO37. The continued silencing of women's voices, however, shows one way that the lack of diversity among technology faculty follows technologists wherever they go, helping to entrench and reinforce gender, racial, and sexual stereotypes.

331. *See* Nadya A. Fouad, *Leaning in, but Getting Pushed Back (and Out)*, Presentation at the American Psychology Association Annual Convention, August 2014, *available at* https://www.apa.org/news/press/releases/2014/08/pushed-back.pdf.*See also* Kate Conger, *Exclusive: Here's the Full 10-Page Anti-Diversity Screed Circulating Internally at Google [Updated]*, GIZMODO (Aug. 5, 2017, 7:25 PM ET), http://gizmodo.com/exclusive-heres-the-full-10-page-anti-diversity-screed-1797564320.

332. *See* Jillian Berman, *Teenage Boys and Girls Are Choosing Very Different Careers*,

deeply entrenched heteronormativity.[333] Lesbian, gay, and bisexual engineering students have reported hearing frequent expressions of sexual prejudice and have to navigate demands for conformity by compartmentalizing their lives, staying in the closet, and depriving themselves of social connections.[334] Gay male engineering students often feel the need to "cover" or "pass" as heterosexual because nonconformity is frowned upon.[335] Queer engineering students reported being told that issues of sexuality and gender identity are "irrelevant" in engineering.[336] What's more, prevailing gender norms in the industry mean that they would be discredited or ignored as engineers if they came out; in other words, they would be (mis)treated by their peers the same way those peers (mis)treat women.[337] Because heterosexual students face none of these oppressive demands, their academic experiences are likely more fulfilling and less stressful.[338]

The lack of women, persons of color, and queer technologists and the absence of diverse faculty at leading engineering and computer science programs impacts designing for privacy directly and indirectly. Homogeneity directly factors into design. Many designers I interviewed suggested it was difficult to design for diverse audiences, so they excluded diversity metrics from the design process and failed to grapple with the sometimes-differing privacy needs of different social groups. This has real, demonstrable effects on the ground. According to a comprehensive study by ProPublica, software that calculated recidivism risk in criminals was racist: it was twice as likely to mistakenly flag black defendants as being at a higher risk of committing future crimes and twice as likely to incorrectly flag white defendants as low

---

MARKETWATCH (June 5, 2017, 9:32 AM), http://www.marketwatch.com/story/teenage-boys-and-girls-are-choosing-very-different-careers-2017-06-01 (reporting on a survey of 1000 13 to 17-year olds conducted by Junior Achievement, a youth-focused nonprofit organization).

333. *See* Erin A. Cech & Tom J. Waidzunas, *Navigating the Heteronormativity of Engineering: The Experiences of Lesbian, Gay, and Bisexual Students*, 3 ENGINEERING STUD. 1, 2–3 (2011).

334. *Id.* at 8–11. In many ways, the experiences of the engineering students interviewed by Cech and Waidzunas mirror the experiences of queer service members in the United States military before the repeal of the "Don't Ask, Don't Tell". In both cases, queer individuals were forced to erase their personal lives and have to constantly navigate social situations in ways that would reduce the risk of being outed. *See* National Defense Authorization Act for Fiscal Year 1994, Pub. L. 103-160, § 571, 107 Stat. 1547, 1670–73 (1993), *repealed by* Don't Ask, Don't Tell Repeal Act of 2010, Pub. L. No. 111-321, 124 Stat. 3515 (codified at 10 U.S.C. § 654 (2012)).

335. *See* Cech & Waidzunas, *supra* note 333, at 13. *See also* KENJI YOSHINO, COVERING: THE HIDDEN ASSAULT ON OUR CIVIL RIGHTS (2006).

336. *Id.* at 11.

337. *Id.* at 12.

338. *Id.* at 2.

risk.[339] Indirectly, the lack of diversity on any metric tends to stifle innovative problem solving.[340] Engineers from the same background might approach in similar ways; engineers who have had different life experiences, particularly with technology, may be able to spot privacy issues and work through them in ways others can't. And designing for privacy in a profit-seeking world often requires creative, outside-the-box thinking because companies to look at design in new ways. Two heads are better the one, but only if the heads aren't identical.

Another feature of technology education today is that both privacy and ethics are inconspicuous in engineering schools' course catalogs and curricula. The California Institute of Technology, commonly known as CalTech, is one of the highest ranking undergraduate electrical engineering programs in the United States.[341] Neither the words "privacy" nor "security", or derivations thereof, are used in the descriptions of the program's required courses or recommended electives.[342] In the school's entire course catalog, the word privacy fares a little better, but the opportunities are a little far afield. The computer science and social science curricula jointly offer an elective called "Introduction to Data Privacy," which covers several important topics, including defining privacy and the tradeoff between "useful computation on large datasets and the privacy of those from whom the data is derived," and reaches beyond the engineering silo to leverage work from "economics, statistics, information theory, game theory, probability, learning theory, geometry, and approximation algorithms" to better understand privacy from a "mathematical" perspective.[343] There is also a political science course called "The Supreme Court in U.S. History," which, among other topics, covers privacy and the Fourth Amendment.[344] And CalTech's science departments offer "Social Media for Scientists," which teaches

339. Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

340. L. Richard Hoffman & Norman R.F. Maier, *Quality and Acceptance of Problem Solving by Members of Homogeneous and Heterogeneous Groups*, 62 J. Abnormal & Social Psych. 401, 404 (1961). *See also* MARVIN E. SHAW, RHONA ROBBIN, & JAMES R. BELSER, GROUP DYNAMICS: THE PSYCHOLOGY OF SMALL GROUP BEHAVIOR (1981) (reviewing the research on the effect of group heterogeneity on problem solving).

341. *See Best Undergraduate Engineering Programs*, *supra* note 327.

342. *See Undergraduate Program*, CAL. INST. OF TECH.: DEPT. OF ELECTRICAL ENG'G, http://ee.caltech.edu/academics/ugrad; *Courses*, CAL. INST. OF TECH.: DEPT. OF ELECTRICAL ENG'G, http://ee.caltech.edu/academics/course_desc.

343. *See* CAL. INST. OF TECH., CALTECH CATALOG, at 508 (2016), http://catalog.caltech.edu/documents/85-catalog_16_17.pdf.

344. *Id*. at 596.

students how to engage with other members of their professions over social media. The class touches on personal privacy issues associated with using social media platforms.[345]

Even though these electives exist, they are easy to avoid. The Data Privacy class at CalTech was offered only once in the last three years.[346] And the course plans, recommended course schedules, and preferred electives pushed by the school do not include these classes.[347] Admittedly, CalTech may be a special case; its reputation sets it apart. But the pattern was repeated elsewhere. An engineering graduate student at Columbia University's Fu Foundation School for Engineering and Applied Scientists told me that electives focusing on privacy issues in engineering are "hidden from most students; you can avoid all of it if you want to. These are things that I am interested in, and, as a result, I've been intentional about accessing them. I can't say the same for my colleagues."[348] A graduate student at the University of Washington's Department of Electrical Engineering noted that she too "had to go out of [her] way" to find classes on policy, ethics, and privacy.[349] And that's true at most schools, even at an engineering school like Columbia's, which requires all of its undergraduate engineering students to participate in the broader college's Core Curriculum of social science, history, and other non-technical courses. In practice, the requirement may not help engineers understand the social, ethical, and legal contexts in which they do their work. As the graduate student noted, students "can take the least relevant parts of the core, like a class on salsa and reggae dance"[350] and still fulfill their graduation requirements without ever taking a course on privacy.

Hiring the same types of engineers from the same types of engineering programs with the same types of education that neglect privacy and ethics tends to make otherwise distinct companies look identical. Paul DiMaggio and Walter Powell called this "isomorphism," and it creates an environment where everyone has similar perspectives on the same problem.[351] This exacerbates

345. *Id*. at 479.

346. *Id*. at 508; CAL. INST. OF TECH., CALTECH CATALOG at 488 (2015), http://catalog.caltech.edu/documents/1-catalog_15_16.pdf; CAL. INST. OF TECH., CALTECH CATALOG (2014), at 483, http://catalog.caltech.edu/documents/14-catalog_14_15.pdf.

347. *See Undergraduate Program*, *supra* note 342.

348. Telephone interview with graduate student at Columbia University (Aug. 30, 2017) (notes on file with Author).

349. Interview with engineering doctoral student at the University of Washington, Seattle, WA (Aug. 9, 2017) (notes on file with Author).

350. *Id*.

351. DiMaggio & Powell, *supra* note 78, at 147, 149, 153.

the diversity problem within the technology community and makes individual learning and creative approaches difficult.[352] As social networks scholars know well, it is difficult for new ideas to break into tightly clustered homophilous networks.[353] We see this everyday with our echo chamber networks of friends on Facebook. In technology product design, the effect of isomorphic hiring of engineers with similar backgrounds is the silencing of new ideas, different perspectives, and privacy concerns.

Legal education may be increasingly embracing privacy, but it often remains technologically averse. Only about 20-25% of law schools offer a class in information privacy.[354] Alongside Internet Law or Cyberlaw, information privacy courses expose students to some technologies that implicate privacy issues. Dan Solove's and Paul Schwartz's privacy law casebook, for example, includes cases on networked technologies, heat sensors, GPS, wiretaps, email, computers, encryption, video surveillance, online searches, and much more.[355] But, outside of occasionally providing general summaries of how relevant technologies work, court opinions can only take law students so far. Most law students major in non-technical fields in college.[356] They may now come to law school with facility in *using* technology, but many lack a willingness to understand how they work. I found some evidence of this in my interviews with privacy lawyers in private firms. "Thank god I don't have to be an engineer to draft changes to a privacy policy," a junior attorney at a large, highly-regarded law firm in New York

352. Despite such drawbacks, employers still tend to hire from the same schools as their competitors because it offers a sense of legitimacy in the industry. Law firms, investment banks, and pharmaceutical companies do this, as well. *See id*. at 148.

353. *See* Mark Granovetter, *The Strength of Weak Ties: A Network Theory Revisited*, 1 SOC. THEORY 201, 202 (1983). *See also* Miller McPherson, Lynn Smith-Lovin, & James M. Cook, *Birds of a Feather: Homophily in Social Networks*, 27 ANN. REV. SOCIOLOGY 415, 429 (2001). The original and seminal work on homophily was from two of the most American famous social theorists of the last century, Paul F. Lazarsfeld and Robert Merton. *See* Paul F. Lazarsfeld & Robert K. Merton, *Friendship as A Social Process: A Substantive and Methodological Analysis*, *in* FREEDOM AND CONTROL IN MODERN SOCIETY 18–66 (M. BERGER ED. 1954).

354. *See* Daniel J. Solove, *Why All Law Schools Should Teach Privacy Law—and Why Many Don't*, TEACH PRIVACY: PRIVACY + SECURITY BLOG (Feb. 26, 2015), https://www.teachprivacy.com/law-schools-teach-privacy-law-many-dont/.

355. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 180–88, 318–26, 326–35, 365–410 (5th ed. 2015).

356. According to information from the Law School Admissions Council, the ten most common majors among law school applicants in the 2015–2016 academic year were, in order, political science, criminal justice, psychology, English, history, economics, philosophy, arts and humanities, sociology, and communications. LAW SCHOOL ADMISSIONS COUNCIL, UNDERGRADUATE MAJORS OF APPLICANTS TO ABA-APPROVED LAW SCHOOLS (2016), https://www.lsac.org/docs/default-source/data-(lsac-resources)-docs/2015-16_applicants-major.pdf.

City.[357] Another young lawyer at a different firm stated that "no technical background required" could be the slogan for his technology law education.[358] Partners at these firms are quick to point out that they are eagerly searching for tech talent, even outside the narrow confines of patent practice groups, which often hire law students with technical degrees.[359] They recognize that technological expertise can help: "I would love an engineer on my cases. They look at problems differently, sure, which helps, but sometimes a client has a new device or a problem that started online and my 12-year-old daughter is more equipped to understand it than I am. No joke."[360] This kind of self-deprecation and admission to a lack of technical skills was quite common.

Granted, lawyers do not need to be lawyers *and* engineers at the same time. But lawyers' lack of technical awareness limits their ability to help integrate privacy into design in several ways. First, a limited knowledge base can erode confidence in one's ability to affect positive change. Several in-house lawyers at major technology companies suggested that they were disinclined to take the initiative and reach out to engineers during design because they "couldn't contribute." "I'm not a coder. I don't want to get in the way," one lawyer conceded.[361] As a result, lawyers don't get involved even when they might be the ones most able to spot privacy issues as they come up in design. Second, an inability to speak with or relate to engineers on their level erodes trust. Trust is important among members of teams. Without some level of trust—in a worker' technical skill, dedication to the work, and commitment to others—team members do not have the confidence to reflect, ask challenging questions, and solve problems. Indeed, trust allows workers to share experiences and provides "psychological safety" for team members to challenge each other's assumptions.[362] To gain that level of trust with engineers, lawyers

357. Telephone interview with associate at AmLaw Top 100 law firm (Sept. 30, 2016) (notes on file with Author).

358. Telephone interview with junior associate at litigation firm (July 28, 2017) (notes on file with Author).

359. Technical education is a requirement of sitting for the Patent Bar Exam. *See* U.S. PATENT & TRADEMARK OFFICE, OFFICE OF ENROLLMENT AND DISCIPLINE, GENERAL REQUIREMENTS BULLETIN FOR ADMISSION TO THE EXAMINATION FOR REGISTRATION TO PRACTICE IN PATENT CASES BEFORE THE UNITED STATES PATENT AND TRADEMARK OFFICE 4–5 (2017), https://www.uspto.gov/sites/default/files/OED_GRB.pdf. Notably, one does not need a technical requirement to be a patent litigator or join patent-related cases.

360. Telephone interview with partner at AmLaw Top 50 law firm (2) (Aug. 19, 2016) (notes on file with Author).

361. Interview with in-house attorney at mid-size technology company, San Francisco, CA (Aug. 12, 2016) (notes on file with Author).

362. *See* Amy C. Edmondson, *The Local and Variegated Nature of Learning in*

need to "speak their language."[363] A senior lawyer at large technology company who serves as the legal point person for several design teams told me that it is "important to learn about the product, be passionate about it, do research on it so I can talk intelligently about what my [engineers] are doing. Otherwise, my [engineers] would see me as an impediment, not a teammate, and I *am* a member of the team."[364]

Changes in both education and within the corporation can fight isomorphism and its effects. Privacy should be integrated into required courses for undergraduate and graduate students, and it should be distinguished from security. The ethics of design, along with a basic education on the legal context in which engineers design technology products, should also be required. Although many schools are seeing higher rates of female applicants, schools must do a better job recruiting women, persons of color, LGBTQ students, and other candidates from diverse backgrounds. Notably, a similar cross-disciplinary approach to legal education can foster greater interaction between privacy lawyers and engineers. At Georgetown University Law Center, for example, Paul Ohm worked with the Staff Technologist at the school's Center on Privacy and Technology to create a course, "Computer Program for Lawyers: An Introduction," to not only train lawyers in a vital skill they can use in practice, but also to familiarize future attorneys with the technology world in which many of their clients work.[365] The Center also runs more informal seminars on law and policy issues raised by new technologies. At New York Law School, a new program, the Technology for Lawyers Working Group, exposes law students and lawyers to important and pervasive technologies and discusses the legal, ethic, and policy issues they raise. This interdisciplinary education is not meant to turn lawyers into engineers, but it can help engineers and lawyers better relate to each other and build the trust necessary for cooperation.

Norm diffusion and exposure to new ideas must also happen within a company. As large networks of people working under the

---

*Organizations: A Group-Level Perspective*, *in* SOCIOLOGY OF ORGANIZATIONS: STRUCTURES AND RELATIONSHIPS, *supra* note 295, at 633.

363. Interview with lawyer at large technology company (Aug. 8, 2017) (notes on file with author).

364. *Id*.

365. *See Computer Programming for Lawyers: An Introduction*, GEORGETOWN UNIV., https://apps.law.georgetown.edu/curriculum/tab_courses.cfm?Status=Course&Detail=2723 (last visited Jan. 11, 2018).

same umbrella,[366] corporations are perfectly suited to norm and knowledge transfer.[367] Indeed, that is what social networks do: information is exchanged through the ties that connect individuals to others in their network and in others' networks.[368] Therefore, any corporation that fosters social interaction among diverse employees from different departments will have stronger social networks among its employees and robust platforms through which trust can be built and experiences, ideas, and norms can be shared.[369] Many technology companies do not do that. Some of the engineers who work or had worked for large and mid-size Silicon Valley technology companies noted that they often only saw or interacted with other engineers. They sit together in open plans, their bosses are coders, and they are often situated in buildings that have their own cafeterias, entertainment, and fitness centers. As a result, their networks are closed, keeping out voices that could diversify design.[370]

Several concrete steps already in place in many companies can help deploy social networks to help embed strong privacy norms among technologists: integrated design teams expose engineers to other perspectives, strong affinity groups can bring together engineers and privacy professionals, and locating employees in a single location can make serendipitous interaction more likely. As more of those interactions take place, the more likely engineers will hear perspectives that challenge their cognitive frames. That can only improve a design process plagued by isolation, siloization, and implicit biases.

## V. CONCLUSION

This Article began where Kenneth Bamberger's and Deirdre Mulligan's research left off. Their book, *Privacy on the Ground*, explored how leading CPOs were moving their companies far beyond the minimal requirements of privacy law on the books. But it was not clear that their dynamic, forward-looking, and trust-based approach to privacy has been embedded throughout their companies. After all, CPOs are not designers and many of the technology products we use today seem to be designed without

366. *See* Inkpen & Tseng, *supra* note 241, at 148 (a corporation is a vertical, structured network).

367. *Id*. at 146.

368. *See* Granovetter, *supra* note 98, at 1363–66.

369. *See* Inkpen & Tseng, *supra* note 241, at 154. *See also* Carrie R. Leana & Harry J. Van Buren III, *Organizational Social Capital and Employment Practices*, *in* SOCIOLOGY OF ORGANIZATIONS: STRUCTURES AND RELATIONSHIPS, *supra* note 295, at 41–46 (companies can build social capital through robust employee social networks).

370. *See* Granovetter, *supra* note 98, at 1363–69.

our privacy in mind. Given those questions, I interviewed engineers, computer programmers, and other technologists, as well as lawyers in private firms, to determine how, if at all, the professionals creating products and user notices integrated privacy into their work. This research revealed a parallel narrative, one much more likely to make its way into design. Where CPOs wanted to push their companies to go beyond the law, their lawyers limited their conception of privacy to notice-and-choice. Where CPOs saw themselves as stewards of their customers' data in an ongoing social exchange, their engineers saw their privacy obligations as ending with data security and encryption. Where CPOs felt that users and evolving user expectations were essential to their work, many technologists resisted any role for the user in the design process. Where CPOs wanted privacy integrated into business units, the reality on the ground saw siloed privacy teams and engineers making privacy decisions on the fly.

The existence of this parallel narrative suggests that robust privacy norms are not always trickling down from the CPOs to their designers on the ground. This is not to say that those norms never reach designers. There are many technology company employees working earnestly to create exciting products and platforms while protecting privacy. This Article is not to meant to suggest otherwise. But there are still barriers to privacy by design at some companies. This Article proposed a four-tiered approach for both understanding those barriers and suggesting how to fix them. Ambiguous privacy theory, significant gaps in privacy law, siloization and misplaced priorities within the corporation, and homogenous design teams are ossifying technologists' perspectives and creating resistance to the CPOs' vision of privacy. Changes at each level, however, could both incentivize companies to take privacy seriously and enhance organizational learning and change.

This research is necessarily limited. Ethnographic research is subject to response biases where respondents try to give the answers they think the researcher wants to hear. My observations of design meetings are particularly susceptible to these biases. Also, a small group of interviews based on snowball sampling cannot represent the population of technologists as a whole, limiting the generalizability of this research. Undoubtedly, there are companies that do better than others at integrating privacy into the design process. Further research will discuss how certain businesses in certain industries manage to be more successful at making robust privacy norms part of the routine of every employee. Generalizing to the entire technology industry is not the

goal of this Article. Rather, it speaks to a world in which the privacy goals set by CPOs at the top of a corporation may not be fully realized. This may, in some cases, prevent robust privacy norms from making their way into design.

Despite any research limitations, this Article points to several avenues for future research. A longitudinal study comparing the privacy elements of products from agile design teams with those of siloed, homogenous teams could prove the impact of diversity and integrated teams on privacy by design. Additional research on technology education is needed to determine how best to integrate ethics, diversity, and privacy into computer science and engineering curricula. And quantitative research can assess the impact of organizational changes, team demographics, and other factors on user trust in a company. These projects are all planned or in progress. This Article is just one step in a larger research agenda on making privacy by design more of a reality than a buzzword.