UC Irvine Law Review

Volume 9
Issue 5 *Women, Law, Society, & Technology*

Article 8

7-2019

# Privacy's Law of Design

Ari Ezra Waldman

# Privacy's Law of Design

Ari Ezra Waldman*

Introduction ..... 1240
I. Privacy by Design as Law ..... 1245
A. Design: Who and When? ..... 1246
1. Corporate Responsibilities During Design ..... 1246
2. The Sociology of Technology ..... 1249
B. Privacy: What, Why, and How? ..... 1253
1. Privacy by Design's Many Definitions (What?) ..... 1253
2. Privacy by Design's Many Values (Why?) ..... 1256
3. The Effects of Confusion (How?) ..... 1257
II. Interpreting Design Law ..... 1259
A. The Products Liability Parallel ..... 1260
B. Products Liability and Design ..... 1263
C. Applying the Products Liability Analogy ..... 1266
1. Who? ..... 1266
2. When? ..... 1269
3. What? ..... 1271
a. Balancing Test During Design ..... 1272
b. Foreseeable Uses ..... 1274
c. A Reasonable Alternative Privacy-Protective Design ..... 1276
d. Privacy Notices and Design ..... 1278
4. Why? ..... 1281
5. How? ..... 1283
6. Privacy's Design Law Summary ..... 1285

---

* Microsoft Visiting Professor of Information Technology and Microsoft Visiting Scholar, Princeton University. Professor of Law and Director, Innovation Center for Law and Technology, New York University Law School. Affiliate Fellow, Information Society Project, Yale Law School. Ph.D., Columbia University; J.D., Harvard Law School. Versions or portions of this paper were presented or workshopped at the AI and the Law Conference at Seton Hall University School of Law, at the Privacy Law Scholars Conference in Washington, D.C., at the Berlin Center for Consumer Policies Annual Forum in Berlin, Germany, and at Fordham University School of Law. Thanks to Kendra Alpert, Michael Birnhack, Danielle Keats Citron, Mary Culnan, Nico van Eijk, Sue Glueck, Woodrow Hartzog, Mike Hintze, Cameron Kerry, Jonathan Mayer, Sean McDonald, Neil Richards, Ira Rubinstein, James Rule, Stuart Shapiro, Jed Shugerman, Olivier Sylvain, Felix Wu, Tal Zarsky, and Ben Zipursky for their helpful and insightful comments. Lauren Davenport provided essential research assistance.

Conclusion.....1287

*Privacy by design is about making privacy part of the conception and development of new data collection tools. But how should we interpret "privacy by design" as a legal mandate? As it transitions from an academic buzzword into binding law, privacy by design will, for the first time, impose real responsibilities on real people to do specific things at specific times. And yet, there remains significant disagreement about what privacy by design actually means in practice: we have yet to define its who, what, when, why, and how. Privacy by design is unmoored and unclear. This Article fills that void. More specifically, this Article offers a new paradigm, based on the law of products liability for design defects, for thinking about privacy by design as a law. This Article shows how privacy by design and products liability arose in similar socioeconomic contexts to answer similar questions and to achieve similar goals. It makes sense, then, to look to products liability to explain the proactive obligations of technology companies to design technology products with privacy and the needs of consumers in mind.*

## INTRODUCTION

The European Union's General Data Protection Regulation (GDPR), which took effect on May 25, 2018, calls for privacy "by design and by default."[1]So-called "privacy by design" has also been endorsed by the Federal Trade Commission (FTC)[2] and the Office of the Attorney General of California.[3] Privacy by design is now the law. But beyond a general understanding that it refers to making privacy part of the design process for new technologies, what privacy by design means in practice is far from clear.[4] That uncertainty is fatal to its transition from an academic buzzword to a legal mandate: If neither regulators nor the regulated know what

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

2. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 22 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/Y575-Q9CE] [hereinafter FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY].

3. CAL. DEP'T OF JUSTICE, OFFICE OF THE ATT'Y GEN., PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM 1, 4 (2013), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf [https://perma.cc/2TFV-DDK7] ("Our recommendations, which in many places offer greater protection than afforded by existing law, are intended to encourage all players in the mobile marketplace to consider privacy implications *at the outset* of the design process.") (emphasis added).

4. The word "design" can mean many different things, from intentions (something is done "by design") to aesthetics (a room can be designed to be visually appealing). But, for the purposes of this Article, I follow the broad definition outlined by Woodrow Hartzog in his book, *Privacy's Blueprint*, which defines design as the "processes that create consumer technologies and the results of their creative processes instantiated in hardware and software." WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 11 (2018).

privacy by design means, they can neither enforce it nor comply with it. This Article fills this void, situating privacy by design in the sociological and legal literatures and ultimately providing a model for what a privacy by design statute should look like in practice.

Any effective privacy by design statute has to answer five questions—namely, the who, what, when, why, and how of design law. *Upon whom are we imposing the responsibility for privacy by design?* Most definitions place the burden on data collectors, processers, and technology companies.[5] But this approach presumes a particular, value-laden definition of "design" that sees it as entirely the company's responsibility.[6] Sociologists of technology, many of whom have shown how the design process is far more complex, would challenge that presumption.[7]

*When do privacy by design's obligations apply?* The obvious answer—namely, during "design"—is circular and implies that we can identify design's clear beginning and endpoint. But social scientists who study technology argue that design is an ongoing, iterative social process that involves engineers and corporate actors, users, exogenous social forces, and even the state. It also continues long after widget version 1.0 is available for sale.[8]

*What does privacy by design look like in practice?* Academics and regulators have offered a variety of visions for privacy by design, but none offer clear practical guidance to industry or the courts. To some, a privacy by design law would list a set of privacy principles;[9] to others, it would require coding those principles into technology's architecture.[10] Yet for others, it would mandate that technology embody certain values.[11] This uncertainty is not just fertile grounds for scholars. Inside technology companies, the effects are real, contributing to frustration,

---

5. *See, e.g.*, Regulation 2016/679, *supra* note 1, art. 25, at 48, which states that "the controller shall, . . . implement appropriate technical and organisational measures . . . ." "Controller" is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data," that is, the company behind a technology product or website. *Id.* art. 4, para. 7, at 34.

6. *See infra* Part I.A.

7. *See* THE SOCIAL CONSTRUCTION OF TECHNOLOGICAL SYSTEMS (Wiebe E. Bijker et. al eds., 2012).

8. For a good summary of this literature, please see *id.*

9. *See* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE SEVEN FOUNDATIONAL PRINCIPLES (2009), https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf [https://perma.cc/U7FH-BPED].

10. *See, e.g.*, Seda Gurses, Carmela Troncoso & Claudia Diaz, *Engineering Privacy by Design*, *in* COMPUTERS, PRIVACY & DATA PROTECTION 1, 3 (2011) (arguing that privacy engineering has the potential to turn privacy by design goals into reality); *see also* Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1341–42 (2013) (arguing that privacy by design requires translating privacy principles into code, both in the back-end infrastructure of data collection and front-end user interfaces).

11. *See, e.g.*, HARTZOG, *supra* note 4 (laying out a series of guidelines for compliance with privacy by design, including a series of pro-consumer social values); HELEN NISSENBAUM & MARY FLANAGAN, VALUES AT PLAY IN DIGITAL GAMES (2014) (discussing the way in which game designers integrate values into their products).

inefficiencies, and confusion.[12] Plus, the breadth of possible interpretations of privacy by design leaves American and European courts, the FTC, and European data protection authorities completely unbounded when they inevitably confront the first design law questions.

*Why are we imposing privacy by design mandates?* Design's significant, yet invisible, capacity to manipulate those who exist inside its ecosystem requires us to consider the values we want design to promote.[13] There are a number of values that could be at the center of privacy by design, ranging from enhancing user control to protecting justice, fairness, and equality.[14] A better understanding of the normative goals of privacy by design can help companies and regulators determine if corporate actions comply with both the letter and spirit of a privacy by design statute.

*How can users pursue their right to privacy by design?* Vindicating privacy rights is an ongoing problem in the United States,[15] where federal courts have gone out of

---

12. Several surveys have shown that organizations remain confused about GDPR compliance, generally. *See, e.g.*, Commvault, *Global Survey Shows That 89% of Organisations Are Still Confused by GDPR*, BUS. COMPUTING WORLD (Dec. 14, 2017), https://www.businesscomputingworld.co.uk/news-post/global-survey-shows-that-89-of-organisations-are-still-confused-by-gdpr/ [http://web.archive.org/web/20180712205117/https://www.businesscomputingworld.co.uk/news-post/global-survey-shows-that-89-of-organisations-are-still-confused-by-gdpr/]; *Survey Finds That GDPR Is Still Confusing Global Organizations; And Preparations Are Lacking*, CONTINUITY CENT. (Sept. 25, 2017), http://www.continuitycentral.com/index.php/news/erm-news/2318-survey-finds-that-gdpr-is-still-confusing-global-organizations-and-preparations-are-lacking [https://perma.cc/74FU-5KTW] (37% of companies report not knowing if they need to comply with the GDPR).

13. *See, e.g.*, HENRI LEFEVBRE, THE PRODUCTION OF SPACE 224 (Donald Nicholson-Smith trans., 1991) (1984) (the nature of a space is determine by what designers want to happen to not to happen in it); LUCY A. SUCHMAN, HUMAN-MACHINE RECONFIGURATIONS 186–92, 257–84 (2d ed. 2007) (arguing that users interact with technologies in ways defined by design); Steve Woolgar, *Configuring the User: The Case of Usability Trials*, *in* A SOCIOLOGY OF MONSTERS: ESSAYS ON POWER, TECHNOLOGY, AND DOMINATION 59, 67–69 (John Law ed., 1991) (users are limited in what they can do with a product given its design); Julie E. Cohen, *Cyberspace As/and Space*, 107 COLUM. L. REV. 210, 225–27 (2007) (the design of online built environments limit user behavior just like the design of physical environments).

14. Equality can be designed in. *See, e.g.*, Rena Bivens & Oliver L. Haimson, *Baking Gender Into Social Media Design: How Platforms Shape Categories for Users and Advertisers*, SOCIAL MEDIA + SOCIETY, Oct. 12, 2016, at 3–7 (gender binaries are baked into the design of social media platforms); Rena Bivens, *The Gender Binary Will Not Be Deprogrammed: Ten Years of Coding Gender on Facebook*, 19 NEW MEDIA & SOCIETY 880, 880–81 (2017) (even with changes and developments, gender remains designed into social media platforms).

15. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 750–56 (2018) (showing how courts conceive of data breach harms exceedingly narrowly and deny standing to breach victims). In Europe, victims of privacy and data harms have the benefit of national data protection authorities (DPAs). DPAs are regulatory agencies that can enforce the data protection rights of EU citizens. They were created by the EU Privacy Directive in 1995 as part of a multilayered approach to privacy enforcement in the European community. *See* Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data, 1995 O.J. (L 281).

their way to put up barriers to privacy plaintiffs.[16] Not knowing what privacy's design law requires of companies erects two more hurdles: it removes a benchmark by which consumers and their lawyers can judge compliance and makes it difficult to know how to litigate a potential case.

Without answers to these who, what, when, how, and why questions, design law is at risk. The law would be open to wildly different interpretations from jurisdiction to jurisdiction, allowing companies to escape liability by fleeing to friendly territories.[17] Vague statutes also give corporate bureaucrats the chance the define the law in ways that benefit their bottom line rather than consumers, putting a thumb on the scale by the time the first court has its say.[18]

Such interpretive problems are nothing new. The limitations of language and the legislative drafting process often result in statutes that leave their meaning and details to those interpreting them.[19] In those cases, courts and regulators look to doctrinal guides and analogies to make sense of vague terms.[20] Corporations, investors, and other stakeholders need some manner of predictability as they plan for a future within the confines of new legal requirements, like privacy's law of design.[21]

---

16. *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545, 1550 (2016) (denying standing to data breach victims because of an inability to demonstrate "concrete and particularized" harm resulting from the breach).

17. *See* Ian Burrell, *Billy Hawkes: The Irishman with a Billion People's Privacy to Protect*, INDEPENDENT (Feb. 7, 2014), http://www.independent.co.uk/life-style/gadgets-and tech/news/billy-hawkes-the-irishman-witha-billion-people-s-privacy-to-protect-9115818.html [https://perma.cc/D6TS-K57X]; Leo Mirani, *How a Bureaucrat in a Struggling Country at the Edge of Europe Found Himself Safeguarding the World's Data*, QUARTZ (Jan. 7, 2014), http://qz.com/162791/how-a-bureaucrat-in-a-struggling-country-at-the-edge-of-europe-foundhimself-safeguarding-the-worlds-data/ [https://perma.cc/LDR6-SVAY].

18. LAUREN B. EDELMAN, WORKING LAW: COURTS, CORPORATIONS, AND SYMBOLIC CIVIL RIGHTS (2016) (discussing how the internal systems created by regulated companies are often taken as evidence of compliance with the law even when companies are actively resisting the goals of the law).

19. *See e.g.*, Victoria F. Nourse & Jane S. Schacter, *The Politics of Legislative Drafting: A Congressional Case Study*, 77 N.Y.U. L. REV. 575, 594–96 (2002) (documenting "deliberate ambiguity" in statutes); Adam C. Pritchard & Joseph A. Grundfest, *Statutes with Multiple Personality Disorders: The Value of Ambiguity in Statutory Design and Interpretation*, 54 STAN. L. REV. 627, 640 (2002)*; see also* FREDERICK REED DICKERSON, THE INTERPRETATION AND APPLICATION OF STATUTES 43–53 (1975) (discussing how the inherent limitations of language create ambiguity in statutes).

20. *See, e.g.*, Larry Alexander, *The Banality of Legal Reasoning*, 73 NOTRE DAME L. REV. 517 (1998); Scott Brewer, *Exemplary Reasoning: Semantics, Pragmatics and the Rational Force of Legal Argument by Analogy*, 109 HARV. L. REV. 923, 937 (1996); Ronald Dworkin, *In Praise of Theory*, 29 ARIZ. ST. L. J. 353 (1997); James R. Murray, *The Role of Analogy in Legal Reasoning*, 29 UCLA L. REV. 833 (1982); Frederick Schauer, *Precedent*, 39 STAN. L. REV. 571 (1987); Cass R. Sunstein, *On Analogical Reasoning*, 106 HARV. L. REV. 741 (1993).

21. *See, e.g.*, Richard Craswell & John E. Calfee, *Deterrence and Uncertain Legal Standards*, 2 J.L. ECON. & ORG. 279, 279–80 (1986) (showing that uncertainty in the law creates negative externalities); Kevin V. Tu, *Regulating the New Cashless World*, 65 ALA. L. REV. 77, 109–13 (2013) (regulatory and legal uncertainty deters investment and development of new business models); *see also* JAMES MADISON, THE FEDERALIST No. 62, at 317–18 (Ian Shapiro ed., 2009) ("What farmer or manufacturer will lay himself out for the encouragement given to any particular cultivation or

This Article fills this gap by proposing that a privacy by design statute should incorporate the principles of products liability for design defects. This makes sense because design is an exercise of power. Its strength comes from its breadth and its invisibility (we often do not realize the myriad ways in which design affects our lives).[22] Good design can make our lives better, easier, or safer; bad design can cause insecurity, pain, and inequality. As Don Norman wrote in *The Design of Everyday Things*, "[w]ell-designed objects are easy to interpret and understand . . . . Poorly designed objects can be difficult and frustrating to use. They provide no clues—or sometimes false clues. They trap the user."[23] Predatory corporations have exercised this power of design for years. When manufacturers built products with designed-in dangers that consumers were unable to see, thus causing harm, the common law developed the law of products liability to help victims obtain justice. This area of the law, a tort-based regime that holds producers liable for the harm caused by products they put on the market, addressed the same questions raised by privacy by design, from who bears the responsibility of design to what those responsible should have done to the values those obligations were meant to serve. And judges imposed liability on corporate actors despite fuzzy definitions of design, in part because of the social values—namely, fairness, justice, and the alleviation of power imbalances—in the common law. Because designing for data collection creates similar power imbalances and has the capacity to take advantage of users, privacy's law of design should be defined by analogy to products liability for design defects.[24]

Several scholars have already proposed using strict or products liability to address some privacy and data breach harms.[25] My argument is different. I am not

---

establishment, when he can have no assurance that his preparatory labors and advances will not render him a victim to an inconstant government?").

22. *See* HARTZOG, *supra* note 4, at 21–55; *see also* Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L. J. 1039, 1043 (2002) (discussing how architecture and design can "increase the cost of perpetrating crime, facilitate law enforcement, promote development of social norms of law-abiding and law-reinforcing behavior, and shape tastes against crime" without anyone knowing).

23. DONALD A. NORMAN, THE DESIGN OF EVERYDAY THINGS 2 (1988)*; see also* HENRI LEFEBVRE, THE PRODUCTION OF SPACE 224 (Donald Nicholson-Smith trans., 1991) (1984). For a summary of how the design of both offline and online built environments can manipulate the behavior of those within those environments, see, e.g., HARTZOG, *supra* note 4, at 27–51; Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210 (2007); Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 99–107 (2018) (collecting and discussing examples from fine art, architecture, interior design, and urban design and comparing them to how companies design privacy notices).

24. *See infra* Part II.A.

25. Various scholars have called for at least some version of a strict liability agenda to combat data privacy harms. *See, e.g.*, Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 296 (2007) (arguing for imposing strict liability on those who securely store and process our data); James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L. J. 793, 827 (2010) (arguing for applying some strict liability principles to data privacy, though cautioning against "import[ing] the full details of [products liability] doctrines, warts and all, into privacy law"); Benjamin R. Sachs, *Consumerism and Information Privacy: How Upton Sinclair Can Again Save Us from Ourselves*, 95 VA. L. REV. 205, 231 (2009) (noting the inability of users to protect themselves).

suggesting a new products liability tort for privacy-invasive design through which individuals could sue technology companies and data collectors. Rather, privacy by design is now a bare-bones statute that requires detail. Products liability has untapped potential as a set of norms that can help define what that statute should look like in practice. Several tort doctrines that have come to set the standard for corporate behavior are helpful: risk-utility balancing, reasonable alternative design (RAD), foreseeable unintended uses, and the duty to warn can all help describe what a privacy by design statute should require.[26]

This Article answers the who, what, when, why, and how of privacy by design as a legal mandate, providing a doctrinal and practical approach to what I am calling privacy's law of design. Part I lays out the problem: questions remain unanswered. This Part challenges the assumptions embedded in some of the formulations of privacy by design to date, particularly with respect to the meaning of design and the role of companies, users, and others in that process, and highlights the uncertainty remaining for companies and regulators to resolve. Part II proposes a new analogy: products liability for defectively designed products. This analogy makes sense because both design laws emerged in similar contexts and both are meant to address the same underlying problem—namely, products that, outside of our view and knowledge capacity, pose dangers that we cannot avoid. This Part applies products liability principles to privacy by design and develops a concise, yet detailed vision of what a privacy by design statute should look like. This Part concludes by discussing the advantages to the approach and responding to objections. The Article concludes with a short summary and avenues for future research.

## I. PRIVACY BY DESIGN AS LAW

The various definitions of privacy by design in the academic literature agree only that (1) design is a corporate responsibility; (2) corporations have to take technological and structural steps to comply; and (3) they have to do so ex ante, or before something goes wrong.[27] But details remain hazy: calls for "privacy by design"[28] or "data protection by design and by default"[29] leave the who, what, when, why, and how of design law unclear.

Sociologists and science and technology scholars tell us that design is complex, nuanced, and multifaceted.[30] Design extends beyond meetings, coding, or product

---

26. *See infra* Part II.C.

27. *See infra* Parts I.A.1, I.B.1.

28. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY, *supra* note 2.

29. *See* Regulation 2016/679, *supra* note 1, art. 25, at 48.

30. Science and technology studies (STS) and sociologists of technology argue that technology occupies space in society in ways that affect individuals and in ways that individuals affect technology. In this field, technology products are cultural artifacts; our iPhones are not just hand-held computers and telephones, but also exercises of social power and reflections of social needs. *See, e.g.*, BRUNO LATOUR, REASSEMBLING THE SOCIAL: AN INTRODUCTION TO ACTOR-NETWORK THEORY 9–16 (2005); SERGIO SISMONDO, AN INTRODUCTION TO SCIENCE AND TECHNOLOGY STUDIES (2d ed. 2010); THE SOCIAL CONSTRUCTION OF TECHNOLOGICAL SYSTEMS, *supra* note 7.

release dates to users and other social groups operating outside the company but who nevertheless have the power to influence how products work. If that scholarship, described in detail in Part I.A, is correct, design law's allocation of responsibility to companies loses its intellectual foundation and could be subject to challenge.

In addition, saying that companies need to take technical and structural steps to implement privacy by design stops far too soon. As described in Part I.B., scholars and experts have developed myriad definitions for privacy by design. That very diversity poses practical and doctrinal risks. Technology companies trying to comply with design law could choose any approach without any clear guidance as to whether it will satisfy their obligations. Similarly, judges in different jurisdictions trying to determine what the statute requires could opt for different approaches, making enforcement arbitrary.

On top of this confusion is the question of values; in fact, current design law appears to reflect a cacophony of values, described in Part I.B., as well. Therefore, when judges and regulators turn to the purposes underlying a design law mandate to answer new questions,[31] their picture is hopelessly unclear. This Section explores these gaps in more detail, arguing that privacy's design law is open to so much interpretation that it risks losing much of its power and potential.

### *A. Design: Who and When?*

A law's first job is to allocate responsibility: who is on the hook for compliance? Each formulation of privacy by design answers this question in the same way: the technology company. In this section, I argue that reflexively allocating design law responsibilities this way rests on shaky intellectual grounds and that confusion over when "design" occurs creates doctrinal incoherence in privacy's design law.

#### *1. Corporate Responsibilities During Design*

It seems obvious to almost everyone that technology companies should be responsible for implementing privacy by design. The GDPR places design obligations on data "controllers"[32] and, to a lesser extent, the "producers of the products" that "process personal data."[33] Ann Cavoukian, the former Information

31. This is particularly important in Europe, where courts are far more willing than those in the United States to interpret a statute in line with its underlying purposes, or *telos*, and how it fits within the overall aims of the European Union. *See* Jens C. Dammann, *The Right to Leave the Eurozone*, 48 TEX. INT'L L. J. 125, 137 (2013); Nial Fennelly, *Legal Interpretation at the European Court of Justice*, 20 FORDHAM INT'L L. J. 656, 664 (1997); *see also* Case C-173/06, Agrover Srl v. Agenzia Dogane, 2006 E.C.R. I-8810, ¶¶ 21–22 (giving "the purpose and general scheme" priority over the wording).

32. Article 25, section 1 states that a "controller shall" implement privacy by design. Section 2 puts the onus on controllers to ensure that that their platforms only process user data when necessary. *See* Regulation 2016/679, *supra* note 1, art. 25, at 48.

33. *Id.*, recital 78, at 9.

and Privacy Commissioner of Ontario, Canada and one of the earliest proponents of privacy by design, placed the burden of implementing her "seven foundational principles of privacy by design," or PbD, on technology companies, as well.[34] The FTC says that privacy by design refers to companies "promot[ing] consumer privacy throughout their organizations and at every stage of the development of their products and services."[35] Further, Woodrow Hartzog has written about "design boundaries in the form of flexible standards for companies."[36]

Corporate responsibility has intuitive appeal. Currently, we bear the burden of protecting our privacy.[37] And we are notoriously ill equipped to do so effectively.[38] Data collectors, on the other hand, have considerable power that, in the absence of regulation, can be wielded against our interests.[39] Indeed, for many platforms that depend on a steady stream of personal information for targeted advertising, their business interests conflict with privacy.[40] Their data use practices can also be used to discriminate against marginalized populations.[41] Focusing privacy by design

---

34. CAVOUKIAN, *supra* note 9.

35. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY, *supra* note 2, at 22.

36. HARTZOG, *supra* note 4, at 121.

37. *See id.* at 21-25; *see also* Julie Brill, Comm'r, Fed. Trade Comm'n, Remarks at the Trans Atlantic Consumer Dialogue 4 (Apr. 27, 2010), available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-julie-brill/100427tacdspeech.pdf [https://perma.cc/EG3M-3QHW] (expressing dissatisfaction with the "traditional opt-out, 'notice and choice' model" that "inappropriately places the burden on consumers to read and understand lengthy, complicated privacy policies that almost no one reads, and no one understands").

38. *See* Ari Ezra Waldman,
*There is No Privacy Paradox: How Cognitive Biases and Design Dark Patterns Affect Online Disclosure*, CURRENT ISSUES IN PSYCH. __ (forthcoming 2020) (manuscript on file with author).

39. This is why Jack Balkin, Jonathan Zittrain, and others have proposed changing the legal relationship between users and data collectors from one purely based on notice to one based on fiduciary law. Under this approach, data collectors could not collect our data and use their power to abuse, harm, or violate our trust. *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://perma.cc/K5CA-8M4C]; *see also* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 79–92 (2018) (arguing that understanding privacy as a norm based on trust is essential for justifying the information fiduciaries approach); Frank Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, 72 MD. L. REV. 682, 684 (2013) ("The increasing power of data to be used for both good and ill arises from powerful trends within industry and computing science . . . [a]n era of 'big data' promises exhilarating and frightening opportunities to cure and exploit human vulnerabilities.").

40. *See, e.g.*, Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 630 (2014) (noting that "Facebook's business model is focused on attracting third parties into monetized agreements for personal information").

41. *See, e.g.*, Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 13–16 (2014) (showing how predictive analytics can discriminate against marginalized populations); Sharona Hoffman, *Employing E-Health: The Impact of Electronic Health Records on the Workplace*, 19 KAN. J.L. & PUB. POL'Y 409, 422 (2010) ("[C]omplex scoring algorithms . . . [can] determine which individuals are likely to be high-risk and high-cost workers"); Frank Pasquale & Tara Adams Rogone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 636–37 (2014).

mandates on corporate actors interposes necessary friction between consumers and powerful data collectors to stop this kind of predation.

Despite some contrary incentives, technology companies are also most efficiently situated to make pro-privacy changes in design. As Guido Calabresi argued in the context of allocating responsibility for accidents, liability should be laid at the feet of the party who can most easily identify and inexpensively fix the problem.[42] Between asking users to navigate the labyrinthine path of privacy management[43] or hack into a platform's code to protect their privacy, on the one hand, and a company's ability to integrate pro-privacy elements from the ground up, on the other, the company has the capacity to more efficiently and effectively make a difference.

And corporate decisions made during the lifecycle of data collection—from conception, through design, to implementation—affect our privacy.[44] Technology products are not built in vacuums. They are built and sold by corporations, collections of real persons working toward shared goals[45] that can be influenced by the people[46] and ideas around them.[47] New ideas at Microsoft, for example, are influenced by CEO Satya Nadella's deep personal commitment to accessibility.[48] "Move fast and break things," like the "hacker culture" that inspired that mantra, inspires different design values.[49] Scholars have shown that companies that consider

---

42. *See* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS (1970); Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts*, 81 YALE L.J. 1055, 1060 (1972) (the party that could avoid an accident at lowest cost should be liable for the accident even if he took due care).

43. *See* HARTZOG, *supra* note 4, at 21–55.

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

45. *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).

46. *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).

47. Adopting Bruno Latour's distinction between the "ostensive" and the "performative" aspects of behavior, see Bruno Latour, *The Powers of Association*, 32 SOC. REV. 264, 264 (1984), Martha Feldman and Brian Pentland argue that executives are responsible for the "ostensive" aspect of routines: setting the tone for action, laying out a mission, and creating policies that form best practice guides. Then, routines are "performed" by workers on the ground: real people doing real work translating ideas into action. Martha S. Feldman & Brian T. Pentland, *Reconceptualizing Organizational Routines as a Source of Flexibility and Change*, 48 ADMIN. SCI. Q. 94, 101 (2003).

48. *See* Satya Nadella, *The Moment that Forever Changed Our Lives*, MICROSOFT (Oct. 21, 2017), https://blogs.msdn.microsoft.com/accessibility/2017/10/21/satya-nadella-the-moment-that-forever-changed-our-lives/ [https://perma.cc/YPP5-JAD3]; *see also* Interview with Jules Cohen, Principal Program Manager, Privacy, in Redmond, WA (Aug. 8, 2017) (notes on file with author) (noting that accessibility is one of four factors always considered when developing new ideas particularly because of Nadella's personal commitment to the issue).

49. *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 93 (2014) ("Engineers should be mindful of the fact that products and services that they design are intended (also) for non-engineers. The Silicon Valley culture,

user privacy concerns from day one are more likely to have respect for privacy integrated into their corporate culture and, as a result, the products they sell.[50] Therefore, encouraging corporate-wide respect for privacy by making corporations responsible for design law during a broad timeline of design encourages the entire company to take privacy seriously.

*2. The Sociology of Technology*

But that argument has a blind spot. It presumes the process of design is complete by the time the manufacturer starts selling its product and, thus, is entirely within the corporation's control.[51] However, science and technology scholars teach us that design itself is not limited to teams of engineers working for a company. It is a long-term, iterative social process that incorporates everything from a company's ethos to user innovations post product release. As a result, the technology company does not always have the last word in design.[52] This raises two important questions that scholars, judges, and regulators working in design law have yet to answer: First, if design is not exclusively a corporate project, why should corporations be exclusively responsible for designing for privacy before users ever see the product, especially since different users have different privacy preferences?

---

dubbed the 'hacker way' by Mark Zuckerberg, founder of Facebook, whose corporate credo is 'move fast and break things,' is not always aligned with broader societal values and expectations.").

50. 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 135 (finding that a corporate climate dedicated to privacy has a more significant effect on engineers' approach to privacy than internal policies, law, or corporate education programs).

51. Such control is often an important factor in the allocation of civil responsibility. In certain jurisdictions, for example, the tort doctrine of *res ipsa loquitor*, which helps victims prove liability when an accident could not have happened without negligence. *See* Cal. Evid. Code § 646 cmt. (West 1970); RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM § 17 cmt. a (AM. LAW INST. 2005) (requiring that the instrumentality of harm be under the defendant's control); *see also* Schmidt v. Gibbs, 807 S.W.2d 928, 931 (Ark. 1991); Hall v. Chastain, 273 S.E.2d 12, 14 (Ga. 1980) (quoting Chenall v. Palmer Brick Co., 43 S.E. 443 (Ga. 1903)). Premises liability, or the duty to take affirmative steps to protect individuals coming onto one's land, is predicated on the idea that landowners and occupiers are the ones in control or possession of land. *See, e.g.*, Rogers v. Jones, 56 Cal. App. 3d 346, 350 (1976). And in copyright law, we hold some third parties vicariously liable for the infringements of others only if they had the "right and ability to control" the infringer's behavior. *See, e.g.*, A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023–24 (9th Cir. 2001); *see also* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 930–31 (2005).

52. And where control and its effects are not so easily assigned, the civil law often declines to hold only one party responsible. The doctrine of comparative fault, for example, metes out liability only according to the defendants' level of harm caused. *See, e.g.*, Weidenfeller v. Star & Garter, 1 Cal. App. 4th 1, 6 (1991) (stating that the purpose of comparative fault is "to prevent the unfairness of requiring a tortfeasor who is only minimally culpable as compared to the other parties to bear all the damages"); *see* KENNETH S. ABRAHAM, THE FORM AND FUNCTIONS OF TORT LAW 144 (1997). Market share liability is another example of civil law refusing to hold someone fully responsible when fault cannot be easily assigned; it limits generic drug manufacturers' exposure based on the likelihood their particular drug caused harm. *See, e.g.*, Allen Rostron, *Beyond Market Share Liability: A Theory of Proportional Share Liability for Nonfungible Products*, 52 UCLA L. REV. 151, 154 (2004).

Second, what if users are at least partly responsible for the harm caused by technology, like when racists on Twitter hijacked Microsoft's AI chatbot and turned it into a Hitler-quoting Nazi?[53]

Indeed, presumptive corporate responsibility reflects actor-network theory, a particular, value-laden view of design that assigns agency to engineers, and according to critics, erases users. Actor-network theory generally posits that artifacts (like machines) do not just emerge out of nowhere; rather, they come into existence as products of social relations, or actor-networks.[54] A good example of an actor-network in this context is a technology company like Google, Apple, Dropbox, or any other small or large corporation. Executives, designers, marketers, and other stakeholders interact with each other through corporate protocols and horizontal teams to achieve a unitary goal of a new product, version, or platform. Users barely factor into this model.

But as Susan Leigh Star has argued, this approach ends up focusing almost entirely on the efforts of (mostly male) designers, or the ones that have the power to position themselves with the right tools, with the right allies, and at the right moment to push their designs to the forefront.[55] Designers, then, become the heroes of technology and society and the obvious bases of responsibility for design law.[56] This model, however, is overwhelmingly wealthy, white, and male, and ignores the contributions of marginalized groups, social movements and activism, and other social forces.[57]

The sociologist Steve Woolgar took a small step toward recognizing a broader conception of design.[58] He argued that designers "configure" users by learning from beta tests and designing technology so it can only be used in certain ways, thus limiting mistakes or other barriers to use.[59] For just two examples, think of how our computer ports are designed for specific inputs (a USB cable, for example, will not

---

53. *See* Elle Hunt, *Tay, Microsoft's AI Chatbot, Gets a Crash Course in Racism from Twitter*, GUARDIAN (Mar. 24, 2016, 2:41 AM), https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter [https://perma.cc/4QKP-RPMT].

54. *See* Albena Yaneva, *Making the Social Hold: Toward an Actor-Network Theory of Design*, 1 DESIGN & CULTURE 273 (2009); *see also* LATOUR, *supra* note 30, at 9–16.

55. *See* Susan Leigh Star, *Power, Technology and the Phenomenon of Conventions*, *in* TECHNOSCIENCE: THE POLITICS OF INTERVENTIONS 88–99 (Kristin Asdal, et. al eds., 2007).

56. This is reminiscent of the so-called "great man" theory of history. *See, e.g.*, THOMAS CARLYLE, ON HEROES, HERO-WORSHIP AND THE HEROIC IN HISTORY (1840) (seeing men like Muhammad, Shakespeare, Martin Luther, Rousseau, and Napoleon as the primary movers of history); FREDERICK ADAMS WOODS, THE INFLUENCE OF MONARCHS (1913) (studying 386 rulers in Western Europe from the 12th century until the French revolution to show their influence on history).

57. *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 [https://perma.cc/DN8Y-TA5D] (discussing the existence and effects of implicit bias in future technology design given that most technology designers are white men).

58. *See generally* Steve Woolgar, *Configuring the User: The Case of Usability Trials*, *in* A SOCIOLOGY OF MONSTERS: ESSAYS ON POWER, TECHNOLOGY AND DOMINATION (John Law ed., 1991).

59. *Id.* at 59, 61.

fit in a Parallel Port) or the restrictions imposed by digital rights management.[60] Users exist in this model; their input is, in fact, essential to the design process. But they are, at best, represented by designers in a process that takes place entirely within the walls of the technology company.[61] Male designers, and their employers, still remain the center of attention.

Like actor-network theory, Woolgar's approach was also criticized as too one-way. The configuration and constraint in Woolgar's work was limited to the activities of heroic actors within the company that produced the technology. But other people are involved too. Designers usually have to follow mandates from executives and internal stakeholders.[62] Exogenous forces play roles as well, including journalists who call attention to design's faults or data breaches, public-sector agencies that regulate technologies, policy makers that pass laws about them, and social movements that advocate for just and fair uses of technology.[63]

And users do more than just follow restrictions laid out by designers. As Wiebe Bijker and Trevor Pinch have shown, users are one of the many social groups influencing design.[64] Whereas Woolgar used the term "encoding" to describe the mostly technological process in which engineers embed constraints on user behavior into technology products,[65] other scholars recognized that users have their own "decoding" to do, a process during which users often identify entirely new uses for machines.[66] For example, when rural farmers, who initially resisted the automobile as a threat to their way of life, started using the Model T as a stationary power source on their farms, they became "agents of technological change": the next iteration of the car better reflected the ways in which these farmers were

60. *See* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 580–88 (2003).

61. *See, e.g.*, SUSAN DOUGLAS, INVENTING AMERICAN BROADCASTING, 1899-1922 (1987) (users developed new ways to deploy radio); CLAUDE FISCHER, AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940 (1992); MICHELLE MARTIN, HELLO, CENTRAL?: GENDER TECHNOLOGY AND CULTURE IN THE FORMATION OF TELEPHONE SYSTEMS (1991) (women started using the telephone to alleviate loneliness in rural areas, surprising telephone companies and forcing changes to telephone construction); Ronald Kline & 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) (showing how farmers used the car as a stationary power source, ultimately contributing to changes in design).

62. *See, e.g.*, Kline & Pinch, *supra* note 61, at 741–44; Nelly Oudshoorn, Els Rommes, & Marcelle Stienstra, *Configuring the User as Everybody: Gender and Design Cultures in Information and Communication Technologies*, 29 SCI. TECH. & HUM. VALUES 30 (2004).

63. *See, e.g.*, Jessika van Kammen, *Do Users Matter?*, *in* BODIES OF TECHNOLOGY (A. Saetnan et al. eds., 2000); Nelly Oudshoorn, *On Masculinities, Technologies and Pain: The Testing of Male Contraceptive Technologies in the Clinic and the Media*, 24 SCI. TECH. & HUM. VALUES 265 (1999).

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

65. *See* Woolgar, *supra* note 58, at 39.

66. Hugh Mackay et al., *Reconfiguring the User: Using Rapid Application Development*, 30 SOC. STUD. SCI. 737, 739, 750, 752 (2000).

deploying it.[67] Bijker has shown that when the high-wheeled bicycle was introduced, older men refused to use it, designating it as unsafe, which paved the way for the development of a new, safer, smaller-wheeled bicycle several years later.[68] Indeed, many scholars have recognized that users identify new uses for products that designers never intended, thus ultimately changing the design.[69]

Already, the neat narrative of design as an exclusively corporate or engineering project that ends at product release is at least fuzzier. Feminist approaches to technology break down the corporate narrative entirely. Ruth Schwartz Cowan pioneered feminist considerations of technology by looking at "the consumption junction," the place and time at which consumers make choices between competing products.[70] This scholarship outright rejects the idea that design begins and ends with scientists and engineers and highlights the fact that women played extraordinarily important roles in design. Feminist scholars then showed that women helped change the design of many technological artifacts,[71] including the microwave,[72] reproductive technologies,[73] computers,[74] and household devices.[75]

The takeaway from this literature is that design is not complete until users have defined the uses and social valence of the technology in their hands. And different users may define technology's uses in different ways. Simplified models of heroic male engineers doing work on their own or standing in for some objective conception of the user risks further burdening marginalized groups and missing half the narrative of design. This speaks to the *who* and *when* of privacy's design law. If design extends beyond product release, then privacy's design law should impose design obligations throughout the entire lifecycle of technologies, from conception

---

67. *See* Kline & Pinch, *supra* note 61.

68. *See* WEIBE E. BIJKER, OF BICYCLES, BAKELITES AND BULBS: TOWARD A THEORY OF SOCIOTECHNICAL CHANGE (1995) (describing the evolution of design changes to bicycles based, in part, on impact from users and other social groups independent of designers).

69. *See, e.g.*, DOUGLAS, *supra* note 61 (amateur radio operators helped make the technology a medium for broadcasting rather than just one-to-one communication); FISCHER, *supra* note 61 (discussing how users developed new ways to use the telephone, particularly outside cities); MARTIN, *supra* note 61 (showing how rural women used the telephone in ways so unexpected to the engineers that designed it that they had to redesign it significantly); DAVID E. NYE, ELECTRIFYING AMERICA: SOCIAL MEANINGS OF A NEW TECHNOLOGY, 1880-1940 (1990) (discussing how communities used electricity and electric appliances, streetlights, and trolleys in ways that advanced social goals).

70. *See* Ruth Schwartz Cowan, *The Consumption Junction: A Proposal for Research Strategies in the Sociology of Technology*, *in* THE SOCIAL CONSTRUCTION OF TECHNOLOGICAL SYSTEMS (Wiebe Bijker et al. eds., 1987).

71. *See* Nina E. Lerman, Arwen Palmer Mohun & Ruth Oldenziel, *The Shoulders We Stand on and the View from Here: Historiography and Directions for Research*, 38 TECH. & CULT. 9, 11 (1997).

72. CYNTHIA COCKBURN & SUSAN ORMROD, GENDER AND TECHNOLOGY IN THE MAKING (1993).

73. *See, e.g.*, ADELE CLARKE & VIRGINIA OLESEN, REVISIONING WOMEN, HEALTH, AND HEALING: FEMINIST, CULTURAL, AND TECHNOSCIENCE PERSPECTIVES (1998).

74. *See, e.g.*, SHERRY TURKLE, THE SECOND SELF: COMPUTERS AND THE HUMAN SPIRIT (1984).

75. *See, e.g.*, RUTH SCHWARTZ COWEN, MORE WORK FOR MOTHER: THE IRONIES OF HOUSEHOLD TECHNOLOGIES FROM THE OPEN HEARTH TO THE MICROWAVE (1983).

to use, not just up to the moment of sale. Moreover, if users play essential roles in design, asking companies to design for privacy before users have a chance to deploy new products imposes unrealistic burdens. Engineers and users may not play identical roles in design; but the sociology of technology complicates the implicit narrative that the technology company is the sole locus of design responsibilities.

### *B. Privacy: What, Why, and How?*

If the *who* and *when* of design law are hazy, *what* design law's obligations are in practice and *why* they are imposed are entirely obscured. In this section, I review the privacy by design and values in design literatures and tease out eight different visions privacy by design in practice and a similarly diverse pool of values they are meant to promote. I then argue that this diversity of views and lack of clarity may prove fatal to privacy by design as it transitions into design law. More specifically, if no one knows either the requirements or the purposes of design law, then whether a given strategy meets a legal requirement or falls below a legal standard is either impossible to tell or entirely arbitrary. This also makes it difficult for those victimized by privacy-invasive design to know *how* to seek redress.

#### *1. Privacy by Design's Many Definitions (What?)*

Definitions of privacy by design have always started with the Fair Information Practice Principles (FIPPs), which developed out of a 1973 report from the U.S. Department of Housing, Education, and Welfare (HEW).[76] 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.[77] The Report also called on companies to be transparent about their data use practices, set limits on what data they gather (also known as data minimization), sunset data retention, and maintain appropriate levels of security.[78] Some of these same principles—data minimization, access, transparency, and, particularly, consent—are

76. *See* U.S. DEP'T OF HEALTH, EDUC., 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/ [https://perma.cc/3ATG-ABEM] [hereinafter "HEW REPORT"]. As Marc Rotenberg has explained, "[n]ot only have Fair Information Practices played a significant role in framing privacy laws in the United States, these basic principles have also contributed to the development of privacy laws around the world and even to the development of important international guidelines for privacy protection." Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 44 (2001). Unfortunately, the FIPPs inadequately protect our privacy in a digital age. *See, e.g.*, Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 485, 490–96 (2015) (discussing the drawbacks to notice and choice).

77. HEW REPORT, *supra* note 76, at 41–42.

78. Because the FIPPs are an evolving set of recommendations, this summary is based on Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2181 (2003).

embedded in the GDPR.[79] Recital 78 explicitly includes four of the FIPPs: data minimization, transparency, access, and security.[80] It would be easy, therefore, to interpret the GDPR's version of privacy by design as little more than the FIPPs.[81]

Indeed, the FIPPs are also at the core of a second definition of privacy by design. When Ann Cavoukian described her seven "foundational" principles PbD, she was either consciously or unconsciously relying on the FIPPs. The principles—Proactive not Reactive; Privacy as a Default Setting; Privacy Embedded into Design; Full Functionality; End-to-End Security; Visibility and Transparency; and Respect for User Privacy[82]—echo principles of user control and transparency that were in the HEW Report. Like the FIPPs, as Ira Rubinstein and Nathan Good have argued, these principles are either repetitive (the first three principles are siblings, if not triplets) or so broad that they provide little additional guidance beyond the general notion that privacy by design is about "considering privacy issues early in the design process."[83]

A third vision of privacy by design may be just as unhelpful. The FTC says that privacy by design refers to companies "promot[ing] consumer privacy throughout their organizations and at every stage of the development of their products and services."[84] On the ground, that has translated into requiring companies to adopt privacy programs that include design considerations. For example, in March 2011, the FTC required Google to "design and implement[] . . . reasonable privacy controls and procedures" in response to a privacy risk assessment.[85] It required the same of Facebook later that year.[86] But the FTC has never explained what that means in practice.

Scholars have tried to fill that void with three other approaches to privacy by design.[87] Ira Rubinstein has related privacy by design to privacy-enhancing

---

79. Indeed, Article 25 lists "data minimization" as a governing "privacy principle." Regulation 2016/679, *supra* note 1, art. 25, at 48.

*80. Id.,* recital 78, at 9.

81. *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 955–56 (2017) (calling the GDPR a "FIPs-based law . . . .").

82. CAVOUKIAN, *supra* note 9.

83. Rubinstein & Good, *supra* note 10, at 1338.

84. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY, *supra* note 2, at 22.

85. In the Matter of Google Inc., F.T.C. File No. 102 3136, at 5 (Mar. 30, 2011) (consent order), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf [https://perma.cc/S72R-WNXA].

86. In the Matter of Facebook, Inc., F.T.C. File No. 092 3184, at 6 (Nov. 29, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf [https://perma.cc/A8DX-Q7RM].

87. That project arguably began with the values in design movement. Helen Nissenbaum and Mary Flanagan have shown how designers integrate values into the products they create. Although their project focused on digital games, the lessons for privacy by design are clear: design is not neutral, and reflects normative decisions about what technology should look like. *See, e.g.*, BATYA FRIEDMAN, HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY (1997) (challenging the idea that efficiency and functionality are the central foci of design and showing how values are integrated into new products); HELEN NISSENBAUM & MARY FLANAGAN, VALUES AT PLAY IN DIGITAL GAMES (2014); Katie Shilton, *Technology Development with an Agenda: Interventions to Emphasize Values in*

technologies, or engineering tools that translate specific data protection laws into code.[88] By way of example, Rubinstein and Good explain that privacy by design should require companies not merely to promise to delete user data after a limited amount of time but rather to design a database that automatically identifies personal information and deletes it at a pre-programmed date.[89] Kenneth Bamberger and Deirdre Mulligan suggest that privacy by design includes organizational measures that integrate privacy professionals into a technology company's various business units.[90] Elsewhere, I have argued that companies need to go further, integrating lawyers and privacy professionals into design teams and acculturating designers themselves into the ethos of privacy and ethics in design.[91] This scholarship has helped privacy by design grow from a catchphrase to a doctrine. But the diversity of approaches to that doctrine means that design law is still unclear.

Woodrow Hartzog offers a seventh conception of privacy by design that leverages various legal tools to guide the design of technologies that affect our privacy. Hartzog calls on the law to "set boundaries and goals" for technology design.[92] For example, a design agenda for privacy that leverages contract, tort, and consumer protection law would respond to the problem of "extracted consent," that is, the way technology companies design interfaces, agreements, and click boxes to manipulate, nudge, and encourage us to acquiesce to a data-sucking regime.[93] This and other important steps in the ecosystem of privacy by design scholarship recognize that the law has to play a role in design. But while Hartzog identifies the legal levers that can rein in technology's data-hungry excesses,[94] judges and regulators still require a doctrinal map for answering specific privacy by design questions as they appear.

The GDPR brings the eighth and most recent formulation of privacy by design, but it is a surprisingly vague one. [95] Article 25, Section 1 of the GDPR states that data controllers have to "implement appropriate technical and organisational measures such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner."[96] Recital 78 goes into more detail, including a list of potential measures that might, if implemented, help a company comply with Article 25.[97] Such steps include

---

*Design*, *in* PROCEEDINGS OF THE ANNUAL MEETING OF THE AM. SOC. FOR INFO. SCI. & TECH. (2010).

88. *See* Ira Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1414–28 (2012).

89. Rubinstein & Good, *supra* note 10, at 1341–42.

90. *See* KENNETH BAMBERGER & DEIRDRE MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 76–86 (2015).

91. *See* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUSTON L. REV. 659 (2018).

92. HARTZOG, *supra* note 4, at 7.

93. *Id.* at 211–13.

94. *Id.*

95. Regulation 2016/679, *supra* note 1, art. 25, at 48.

96. *Id.*

97. *Id.* at recital 78, at 9.

"minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, [and] enabling the controller to create and improve security features."[98] This list of examples is helpful, but only to a point. As a incomplete list of technical measures, it offers companies a quick guide to model their own compliance mechanisms.[99] But it does not speak to any organizational measures that are necessary. Nor is the language of the GDPR at all specific. The core of Article 25's language is the requirement to take technical and organizational steps "which are designed to implement data protection principles . . . in an effective manner."[100] Those principles, from consent to data minimization to security, are covered in other parts of the GDPR. That turns Article 25's version of privacy by design into a catch-all provision with no specific requirements of its own.

*2. Privacy by Design's Many Values (Why?)*

Design is not neutral. Technologies reflect the values embedded in them.[101] That makes values particularly relevant for design law. As a product of many different views, design law today reflects a cacophony of values, some of which are conflicting. For example, Cavoukian's PbD talks about transparency, consent, and security, among other things,[102] reflecting the idea that privacy by design's purpose is to give consumers power and control over their data.[103] Woodrow Hartzog suggests that privacy by design should focus on values like trust and obscurity. That is, because trust is essential to privacy in the digital age,[104] design should focus on building trust and confidence.

---

98. *Id.*

99. *See* Jacob Scott, *Codified Canons and the Common Law of Interpretation*, 98 GEO. L.J. 341, 408 nn. 359–60 (2009) (noting legislatures giving nonexhaustive lists of rules and broad instructions).

100. Regulation 2016/679, *supra* note 1, art. 25, at 48.

101. *See, e.g.*, HARTZOG, *supra* note 4, at 95–119; *see also* Batya Friedman & Peter Kahn, Jr., *Human Values, Ethics, and Design*, *in* THE HUMAN-COMPUTER INTERACTION HANDBOOK 1177–1201 (Andrew Sears & Julie Jacko eds., 2d ed. 2008) (arguing that some values implicated in design include freedom from bias and discrimination, property, and calmness).

102. *See* CAVOUKIAN, *supra* note 9.

103. Indeed, control has become the "archetype" in privacy law. HARTZOG, *supra* note 4, at 63; *see also* ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967). Privacy-as-control is also a favorite in industry. During testimony before the United States Senate in April 2018, Facebook CEO Mark Zuckerberg talked about returning control over privacy to consumers fifty-four times. *See Facebook, Social Media Privacy, and the Use and Abuse of Data, S. Comm. on the Judiciary, S. Comm. on Commerce, Sci., and Transp. Joint Full Comm. Hearing*, 115th Cong. (2018), https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data [https://perma.cc/58AK-DVLA]; *see also Transcript of Mark Zuckerberg's Senate Hearing*, WASH. POST (Apr. 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.b7cf575c7106 [https://perma.cc/DRW5-BC86].

104. *See* HARTZOG, *supra* note 4, at 97–107 (discussing various aspects of trust in privacy law); WALDMAN, *supra* note 39, at 1–10, 47–76 (arguing that privacy is based on relationships of trust between individuals and, thus, can protect the value of trust); Jessica Litman, *Information*

Frederic Stutzman and Hartzog argue that obscurity functions as a privacy value because when our information is hard to collect—namely, when it is in disparate corners of the internet or sitting in dusty file cabinets in town halls—only a few people will actually be willing to put in the time, money, and effort to identify us.[105] Placing boundaries around data collection can make us more obscure from commercial surveillance. Obscurity, then, can also be designed in.

But so can trust, or control, or whatever value a designer, corporation, legislator, regulator, or law professor prefers. The diverse pool of sometimes overlapping and sometimes conflicting ideas about privacy and design, which mirror the patchwork state of privacy scholarship as a whole,[106] puts design law at risk.

*3. The Effects of Confusion (How?)*

When language can mean almost anything, it means almost nothing. Design law could mean anything from following the FIPPs to making technological changes to platforms to integrating lawyers into more diverse design teams. And the law's purposes and goals could be minimal or ambitious. Vague statutes have pernicious side effects that leave design law open to attack in four related ways, crippling our ability to vindicate our rights to privacy-centered design.

A vague design statute cannot guide corporate behavior appropriately.[107] If design law fails to provide sufficient notice of its requirements, companies cannot know what actions, changes, or new strategies regulators want.[108] That kind of vagueness is costly and can hamper the goals of design law in the first place. Vague requirements allow predatory companies to make minor, superficial changes and claim their obligations fulfilled.[109]

---

*Privacy/Information Property*, 52 STAN. L. REV. 1283, 1308–10 (2000); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 451–57 (2016) (protecting privacy can build trust between online platforms and consumers); Kirsten Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online*, 18 FIRST MONDAY 12 (DEC. 2, 2013), http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802 [https://perma.cc/GV7L-NDNN]; Katherine Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008).

105. *See* HARTZOG, *supra* note 4, at 110–11; Frederic Stutzman & Woodrow Hartzog, *The Case for Online Obscurity*, 101 CAL. L. REV. 1 (2013).

106. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) (calling privacy a "concept in disarray").

107. This is akin to the arguments in support of the void for vagueness doctrine. *See, e.g.*, Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926) (a law is unconstitutionally vague when people "of common intelligence must necessarily guess at its meaning").

108. The Supreme Court made this same argument in *Kolender v. Lawson*, which overturned a vague loitering statute. *See* Kolender v. Lawson, 461 U.S. 352, 357 (1983).

109. *See* EDELMAN, *supra* note 18 (showing how companies create structures that frustrate the substantive goals of anti-discrimination law); *see also* Josh Constine, *A Flaw-by-Flaw Guide to Facebook's New GDPR Privacy Changes*, TECHCRUNCH (Apr. 18, 2018), https://techcrunch.com/2018/04/17/facebook-gdpr-changes/ [https://perma.cc/J7RE-VBV6] (showing how many of the changes Facebook made to its platform to comply with the GDPR are manipulative, superficial, and not designed with ease of use in mind).

Without guidance for regulators, design law risks becoming under-inclusive. Judges, regulators, or practitioners could glom on to a single easy, understandable, or cheap-to-implement value and run with it, narrowing design law in the same way American privacy law reflects a scaled-down version of the FIPPs.[110] There is already some evidence this might happen. In the United States, for example, privacy law fetishizes consent and control while ignoring other elements of privacy.[111] Our consent obsession is one reason why privacy plaintiffs have had difficulty exercising their privacy rights in court.[112] Judges often respond to claims of data misuse by noting that users consented to share their information in the first place and assumed the risk that it would be shared with others.[113] Selectively interpreting privacy principles is happening on the ground as well. Recent research into how technology companies operationalize privacy law into the corporate practice and routine suggests that easy-to-understand and high-profile mandates like security tend to crowd out more complicated and nuanced requirements of privacy.[114] This could happen again with privacy by design.

Vague terms make it difficult for consumers to distinguish corporate malfeasance from corporate compliance, thus disempowering consumer voices both in the market and at law. This is true across a variety of areas of law. For example, confusion as what constitutes a "famous" trademark complicates trademark holders' decisions to pursue dilution claims.[115] Ambiguities in civil procedure rules make it difficult for parties to know their procedural rights and obligations.[116] Vague terms in patent claims leave future inventors unsure as to the patent's coverage[117] and encourages rent-seeking patent litigation.[118] In all of these

---

110. *See* Rotenberg, *supra* note 76.

111. *See* HARTZOG, *supra* note 4, at 62–67.

112. It isn't the only reason. Plaintiffs have also had trouble articulating "concrete and particularized" damages from privacy and data breach harms. *See*, *e.g.*, Spokeo v. Robins, 136 S. Ct. 1540 (2016). *But see* Solove & Citron, *supra* note 15 (arguing that courts should apply the long history of recognizing intangible, yet no less devastating harms, to privacy cases).

113. *See, e.g.*, *In re* Nw. Airlines Privacy Litig., No. Civ. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004); Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995).

114. *See* Waldman, *Designing Without Privacy*, *supra* note 91, at 697–99.

115. *See, e.g.*, Sandra L. Rierson, *The Myth and Reality of Dilution*, 11 DUKE L. & TECH. REV. 212, 303 n. 393 (2012) (vagueness in the term "famous" makes it difficult to know when a trademark plaintiff is entitled to sue for dilution of a famous mark).

116. *See* Arthur F. Greenbaum, *Jacks or Better to Open: Procedural Limitations on Co-Party and Third-Party Claims*, 74 MINN. L. REV. 507, 534 (1990) (discussing ambiguities in Rule 18(a) of the Federal Rules of Civil Procedure).

117. *See* Dan L. Burk & Mark A. Lemley, *Fence Posts or Sign Posts? Rethinking Patent Claim Construction*, 157 U. PA. L. REV. 1743, 1745 (2009) ("[C]laim construction may be inherently indeterminate: it may simply be impossible to cleanly map words to things. Patent attorneys seize on such indeterminacy to excuse infringement or to expand their client's exclusive rights.").

118. Jonathan L. Moore, *Particularizing Patent Pleading: Pleading Patent Infringement in a Post-Twombly World*, 18 TEX. INTEL. PROP. L.J. 451, 486 (2010) ("Further, the scope of a patent's claim is typically ambiguous and it is difficult to know with any certainty how a court will construe it. This fact benefits nuisance-value plaintiffs, as it allows them to bring actions that lack merit.") (footnote omitted).

cases, ambiguities in the law make litigation more costly and thus discourage potential plaintiffs from pursuing legal action to vindicate their rights. Unclear design law may, therefore, silence users and eliminate public interest impact litigation as a privacy enforcement tool.[119]

Further, vague laws make enforcement arbitrary. If design law can refer to no less than eight different practical requirements, each sitting somewhere on a range from lax to strict, governments, regulators, and DPAs can determine whom to investigate and what version of the law they want to apply based on their prejudices or politics. That undermines the rule of law and makes it impossible for consumers to know when and how to pursue their design law rights. Justice O'Connor made this point in a decision striking down a criminal vagrancy and loitering law as unconstitutionally vague: vague statutes permit "a standardless sweep [that] allow policemen, prosecutors, and juries to pursue their personal predilections."[120] It is not difficult to imagine a scenario where a vigorous pro-privacy enforcer in France takes an aggressive view of the design law embedded in the GDPR but a pro-business political appointee at the FTC adopts the most lax interpretation of privacy by design.[121] This eventuality could weaken the reach and dramatically undermine the power of privacy's design law, thus highlighting the need for clear, doctrinal guides to interpret its practical requirements.

## II. INTERPRETING DESIGN LAW

The current vague approaches to privacy by design leave the who, what, when, why, and how of design law open to wildly different interpretations. That much is arguably clear. That is particularly problematic for an area of law that seeks to influence behavior ex ante (before product release) rather than ex post (after something goes wrong). Those responsible for compliance need to know what the law requires of them; those responsible for interpreting the law need to know how to answer questions as they come up; those who are meant to benefit from the law need to know what to expect and how to vindicate their rights. Therefore, everyone needs doctrinal and practical guides or analogies.

Fortunately, we do not have to reinvent the wheel. This is not the first time society has been confronted with new, mass-produced technologies that can cause

---

119. Private litigation has played an important role in enhancing consumer safety before. *See* AM. ASS'N FOR JUSTICE, DRIVEN TO SAFETY: HOW LITIGATION SPURRED AUTO SAFETY INNOVATIONS 4–49 (2010); *see also* Dawson v. Chrysler Corp., 630 F.2d 950 (3d Cir. 1980) (side impact protection); Seliner v. Ford Motor Co., No. 2002-30454 (Tex. Dist. Ct. 2004) (safe doors); 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"); AlliedSignal, Inc. v. Moran, 231 S.W.3d 16 (Tex. App. 2007) (seat belts); Shipler v. Gen. Motors Corp., 710 N.W.2d 807 (2006) (safe roofs); Grimshaw v. Ford Motor Co., 119 Cal. App. 3d 757 (1992) (Ford Pinto case).

120. Kolender v. Lawson, 461 U.S. 352, 358 (1983)

121. *But see* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959 (2016) (challenging the conventional wisdom that European data regulators are aggressive and their American counterparts are lax).

harm without us knowing. The common law doctrine of products liability developed in a technological, economic, and social context analogous to current technological landscape. And it emerged to answer the same who, what, when, why, and how questions plaguing privacy's design law. Granted, products liability established norms and requirements for corporate behavior through tort litigation and focused on manufactured products that endangered our health and safety.[122] Privacy by design is a statute directed at data collection tools. But despite those differences, a privacy by design statute can learn a lot from products liability today.

This Part makes a three-step argument. First, I suggest that products liability arose in a social context similar to today's, just with different technologies, to answer similar questions plaguing privacy's law of design. Second, I establish a taxonomy of how products liability doctrines can influence design, ultimately focusing on the way in which it can operate as an effective analogy to describe, in a different context, what privacy by design should mean as a legal requirement. And third, I apply that analogy to create a model for design law, thus translating privacy by design into a clear legal mandate.

### *A. The Products Liability Parallel*

Products liability developed out of a series of court decisions to address harm caused by mass-produced goods. Though originally written in the language of "strict" liability,[123] products liability never reached the apotheosis of absolute manufacturer liability for all harms caused by products on the market.[124] Section 402A of the Restatement (Second) of Torts, which has been widely cited and

---

122. It also emerged because traditional claims for injury from faulty or defective products failed because of the privity doctrine, which stated that a party only has a duty to those with whom there was a contractual relationship. *See* Winterbottom v. Wright, 10 M&W 109, 152 Eng. Rep. 402 (1842). The fact that there is often privity between technology companies and users through agreement to terms of service or privacy policies does not alter my argument for three reasons. First, privacy policies are not always considered contracts. *See, e.g.*, *In re* Nw. Airlines Privacy Litig., No. 04-126 (PAM/JSM), 2004 WL 1278459, at *6 (D. Minn. June 6, 2004) ("The usual rule in contract cases is that 'general statements of policy are not contractual.") (quoting Martens v. Minn. Mining & Mfg. Co., 616 N.W.2d 732, 740 (Minn. 2000) (en banc))); Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (explaining that "broad statements of company policy do not generally give rise to contract claims"); RAYMOND T. NIMMER, LAW OF COMPUTER TECHNOLOGY § 17:68 (2012) ("Despite the lack of a bilateral offer and acceptance, privacy policies may become part of a contractual arrangement . . . ."). Second, even where there is privity, privacy plaintiffs have been routinely denied access to justice, much like those injured by defective products. *See, e.g.*, Solove & Citron, *supra* note 15. Third, I am not arguing that technology companies that create tools that collect our data should be subject to strict liability or products liability when something goes wrong. Others have made that argument. *See infra* notes 151–160 and accompanying text. Rather, I argue that products liability can serve as an analogy to specify privacy by design's requirements. For that argument, privity is immaterial.

123. *See, e.g.*, Escola v. Coca Cola Bottling Co. of Fresno, 24 Cal. 2d 453, 461–66 (1944) (Traynor, J., concurring) (arguing that the company's liability should not be found in negligence, but merely because it caused the harm).

124. *See* James A. Henderson, Jr., *Echoes of Enterprise Liability in Product Design and Marketing Litigation*, 87 CORNELL L. REV. 958, 958–59 (2002).

adopted,[125] holds liable one who manufactures and sells a "product in a defective condition unreasonably dangerous to the user" that causes harm after reaching the consumer in substantially "the condition in which it was sold."[126] Over time, state court judges have developed several standards, definitions, and tests for determining when a product is defective.[127] Many of those tests can also help tease out the details of privacy's law of design.

Products liability arose because judges recognized that the new socioeconomic relationship between consumers and twentieth century technologies required something more than just simple negligence. In fact, the same social factors that gave rise to products liability in the first place mirror the relationships we have with technology companies today in at least two ways.

First, data collectors are creating economic opportunities and dangers analogous to those caused by manufacturing. Danielle Citron has compared the advantages and risks posed by large databases of personal information to those created by the large reservoirs of water that powered the Industrial Age.[128] These reservoirs powered textile mills, machines that churned out mass-produced convenience goods, and large new factories.[129] But when the dams holding back the water broke, the escaping water caused significant, wide-spread property damage, unlike any that has been seen before the Industrial Age.[130] A strict liability regime, exemplified by *Rylands v. Fletcher*,[131] emerged to address the new problem of massive harm without fault. A similar story is playing out today. Companies like Facebook, Google, and Amazon are gathering terabytes of data on internet users. That data helps them and their partners identify new commercial opportunities.[132] It can connect job seekers and employers.[133] It can help us find romance.[134] It can

125. *See* James A. Henderson, Jr. & Aaron D. Twerski, *A Proposed Revision of Section 402A of the Restatement (Second) of Torts*, 77 CORNELL L. REV. 1512, 1512 n.1 (1992).

126. *See* RESTATEMENT (SECOND) OF TORTS § 402A (1977).

127. *See* Douglas A. Kysar, *The Expectations of Consumers*, 103 COLUM. L. REV. 1700, 1708–24 (2003) (discussing the history of the development of products liability for design defects).

128. *See* Citron, *supra* note 25, at 244.

129. *See* NORMAN SMITH, A HISTORY OF DAMS 169–80 (cited in Citron, *supra* note 25, at 281).

130. Citron, *supra* note 25, at 243–44.

131. Rylands v. Fletcher [1868] 3 LRE & I. App. 330 (HL).

132. Retailers and marketers use large data sets on consumer behavior to target individuals and groups of internet users with advertisements that are ostensibly tailored to user interests. *See, e.g.*, Press Release, Network Adver. Initiative, Study Finds Behaviorally-Targeted Ads More than Twice as Valuable, Twice as Effective as Non-Targeted Online Ads (Mar. 24, 2010) (quoting Howard Beales, former Director, FTC Bureau of Consumer Protection), *available at* https://www.networkadvertising.org/sites/default/files/imce/nai_beales_release.pdf [https://perma.cc/S5E6-359R].

133. *See, e.g.*, Arnie Fertig, *4 Ways to Use Big Data in Your Job Hunt*, U.S. NEWS (Feb. 4, 2014 12:10 PM), https://money.usnews.com/money/blogs/outside-voices-careers/2014/02/04/4-ways-to-use-big-data-in-your-job-hunt [http://web.archive.org/web/20160912180958/https://money.usnews.com/money/blogs/outside-voices-careers/2014/02/04/4-ways-to-use-big-data-in-your-job-hunt].

134. *See We Use Math to Find You Dates*, OKCUPID, https://www.okcupid.com/about [https://perma.cc/DA75-Y7JW] (last visited June 16, 2019).

unlock our phones,[135] turn on appliances in our homes,[136] and play our favorite songs.[137] But when the barriers protecting that information break, whether from within (unauthorized access) or without (hacking), the escaping information can cause untold damage to victims.[138] The data can be used to discriminate,[139] harass,[140] and cause intangible[141] and pecuniary harm.[142] Given the similarity between these two types of "reservoirs of danger," Citron called for strict liability regimes to address harms associated with leaking databases of personal data.[143]

Second, technological innovations have created significant power and information imbalances between technology companies and their users. Before industrialization, consumers often knew the people from whom they bought finished goods. Economic exchange was a far smaller, more intimate affair than it is today. As such, consumers could protect themselves from poorly made goods: they could see products before purchase, judge the trustworthiness of sellers, and exercise their power by buying goods from another seller.[144] After industrialization, manufacturers knew what methods they used to create everything from glass bottles[145] to children's toys[146] and heavy machinery,[147] but consumers possessed neither the know-how nor the opportunity to investigate themselves, leaving them entirely at the mercy of producers.[148] Users of digital technologies have even less power. Not only is our personal information collected and analyzed in a "black box" of proprietary algorithms and intelligent machines,[149] but the designs of technology

---

135. *See About Face ID Advanced Technology*, APPLE, https://support.apple.com/en-us/HT208108 [https://perma.cc/76MA-D2VU] (last visited June 16, 2019).

136. *But see* Woodrow Hartzog & Evan Selinger, *The Internet of Heirlooms and Disposable Things*, 17 N.C. J.L. & TECH. 581 (2016) (noting that in the rush to connect objects to the internet, connected is not always better).

137. *See* Mikey Campbell, *Apple Reveals Algorithm Behind Apple Music Mixes, Execs Discuss Past and Future of Service*, APPLEINSIDER (Sept. 26, 2016 5:33 PM), https://appleinsider.com/articles/16/09/26/apple-reveals-algorithm-behind-apple-music-mixes-execs-discuss-past-and-future-of-service [https://perma.cc/U7ZF-2GEC].

138. Citron, *supra* note 25, at 244–45.

139. *See, e.g.*, Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/F6JT-VKY8].

140. *See* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014).

141. *See* Solove & Citron, *supra* note 15.

142. *See* FED. TRADE COMM'N, INFORMATION COMPROMISE AND THE RISK OF IDENTITY THEFT: GUIDANCE FOR YOUR BUSINESS (2004), https://dwtprivsec.lexblogplatformtwo.com/files/2014/04/bus59-information-compromise-and-risk-id-theft-guidance-your-business.pdf [https://perma.cc/YYD4-JA69].

143. *See generally* Citron, *supra* note 25.

144. *See* Sachs, *supra* note 25, at 231–33.

145. *See, e.g.*, Escola v. Coca Cola Bottling Co., 150 P.2d 436, 436 (exploding bottle).

146. *See, e.g.*, Bailey v. Montgomery Ward & Co., 431 P.2d 108 (Ariz. 1967) (pogo sticks).

147. *See, e.g.*, Soule v. Gen. Motors Co., 882 P.2d 298 (Cal. 1994) (car).

148. *See* Sachs, *supra* note 25, at 219–23; *see also* Mauch v. Mfr. Sales & Service, Inc., 345 N.W. 2d 338, 345 (S.D. 1984).

149. *See* PASQAULE, *supra* note 44.

products and platforms today tilt the power balance toward the designers and away from users.[150] Therefore, much like consumers of mass-produced goods, consumers of digital products that commodify their data cannot act as successful stewards of their own data safety.

As a result of these similarities, it should come as no surprise that a variety of scholars have called for applying strict or products liability to privacy and data breach harms. William Prosser laid the groundwork for this scholarship when he published the now-definitive guides for privacy tort law[151] and strict liability in the same year.[152] Both articles have had an outsized impact on the law[153] and because Prosser also served as the reporter for the Restatement (Second) of Torts, both privacy and strict liability were incorporated at the same time.[154] Benjamin Sachs called for holding data collectors strictly liable for failure to keep our information secure.[155] Sarah Ludington proposed a new strict liability tort, the tort of misuse of stored personal data, that would explicitly enforces the FIPPs.[156] And Citron's "reservoirs" metaphor argued for applying the strict liability model of *Rylands v. Fletcher* to data breaches.[157]

### *B. Products Liability and Design*

Though insightful, each of these proposals aim to create liability for privacy harms through strict tort liability litigation. Sachs refers specifically to corporate data breaches, identity theft, and discrimination.[158] Ludington's new tort is situated as a solution to data leaks.[159] And Citron applies *Rylands* to database operators because they are the ones aware of the "vulnerabilities in their computer networks" that could lead to harm ex post.[160] My goal is to put meat on the bones of a privacy by design statute, not create a new tort. Moreover, these proposals focus on the role

150. *See* HARTZOG, *supra* note 4, at 62–67; *see also* NOR. CONSUMER COUNCIL, DECEIVED BY DESIGN: HOW TECH COMPANIES USE DARK PATTERNS TO DISCOURAGE US FROM EXERCISING OUR RIGHTS TO PRIVACY (June 27, 2018), *available at* https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [https://perma.cc/C58N-3BRD].

151. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960) (reviewing privacy case law from 1890 and identifying four privacy torts).

152. *See* William L. Prosser, *The Assault Upon the Citadel (Strict Liability to the Consumer*), 69 YALE L.J. 1099 (1960) (discussing the rise of strict liability over the previous years).

153. *See, e.g.*, Greenman v. Yuba Power Products Inc., 377 P.2d 897, 901 (citing Prosser's *Strict Liability* when adopting a rule of strict liability for defective products that cause injury to consumers); *see also* Daniel J. Solove & Neil M. Richards, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 148–56 (2007) (discussing the impact of Prosser, as well as Warren and Brandeis, on the current state of civil privacy law).

154. *See* RESTATEMENT (SECOND) OF TORTS §§ 652A–652I (1977) (privacy torts); *id.* at §§ 388–408 (products liability).

155. *See* Sachs, *supra* note 25, at 240.

156. *See* Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 171–72 (2006).

157. *See* Citron, *supra* note 25, at 244.

158. *See* Sachs, *supra* note 25, at 219–23.

159. *See* Ludington, *supra* note 156, at 141.

160. Citron, *supra* note 25, at 284.

of strict liability; products liability today has a far more diverse toolkit. This literature, then, only fights half the battle.

Products liability influences design along two axes: directness and specificity (Table 1). Real or threatened litigation affects design indirectly and generally: it raises the ultimate costs of unsafe products to incentivize the development of safer ones.[161] Incentive realignment is at least one of the justifications behind products liability generally[162] and the proposal to apply strict liability in data breach and privacy cases.[163] But because the deterrence factor only increases costs of bad design, it cannot help courts, regulators, or designers interpret what design law actually requires.

**Table 1**

**How Products Liability Can Influence Design**

| | **Specifically** | **Generally** |
|---|---|---|
| **Directly** | Court Decisions (Intra-Industry) | Doctrinal Analogies |
| **Indirectly** | Court Decisions (Inter-Industry) | Increased Costs |

Decisions in products liability cases can influence design directly and specifically by defining precisely what designs are safe and unsafe in given circumstances for given products. For example, after Chrysler was held liable for

161. *See, e.g.*, Lewis v. Timco, Inc., 716 F.2d 1425, 1429 (5th Cir. 1983) (finding manufacturer liability encourages the production of safe products); Beshada v. Johns-Manville Prods. Corp., 447 A.2d 539, 548 (N.J. 1982) (noting that "[b]y imposing on manufacturers the costs of failure to discover hazards, we create an incentive for them to invest more actively in safety research"); Daly v. Gen. Motors Corp., 575 P.2d 1162, 1169 (Cal. 1978) (reasoning that strict liability gives manufacturers an "incentive to produce safe products, . . . to avoid and correct product defects . . . [, and an] incentive toward safety both in design and production"); *see also* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 166 (3d ed. 1986) (arguing that costs of products liability litigation encourage companies to design safer products to bring prices in line with competitors); WILLIAM L. PROSSER & W. PAGE KEETON, THE LAW OF TORTS § 4, at 25–26 (5th ed. 1984) (stating that a "manufacturer who is made liable to the consumer for defects in a product will do what can be done to see that there are no such defects").

162. *See, e.g.*, LaRosa v. Superior Court, 176 Cal. Rptr. 224, 233 (App. Dep't Super. Ct. 1981) (acknowledging that a company "will pass the costs of injuries along to the consumer in the form of increased prices for more dangerous products and that the consumer will be more likely to buy safer goods because they will be relatively less expensive"); *see also* Gregory C. Keating, *The Theory of Enterprise Liability and Common Law Strict Liability*, 54 VAND. L. REV. 1285, 1320 (2001); Robert L. Rabin, *Some Thoughts on the Ideology of Enterprise Liability*, 55 MD. L. REV. 1190, 1194 n. 22 (1996).

163. *See, e.g.*, Citron, *supra* note 25, at 265–67.

injuries to a policeman from an impact to the side of his car, automobile manufacturers knew that they had to design cars to withstand side impact collisions.[164] And after *Garrett v. Ford*,[165] which involved injuries from a lap seat belt, the auto industry started including three-point rear seatbelts in their designs.[166] In this way, court decisions concluding that particular designs were unsafe helped automakers redesign their cars in specific ways to comply.[167] This aspect of products liability law, however, has its limits. Identifying precise safe or unsafe designs may provide certainty to designers in particular industries or in given circumstances. But it is impractical to expect courts to make all design decisions; judges and juries are neither institutionally competent nor close enough to the factors that go into design to do more than make specific decisions on the margins.

Relatedly, products liability law can influence design specifically, but indirectly. For example, products liability decisions that hold companies liable for insufficiently testing potentially dangerous substances, like the silicone in breast implants,[168] could influence any chemical company or drug manufacturer that must test products before putting them on the market. However, this indirect pathway for influencing the design process remains hypothetical and too disconnected from design to answer specific questions about privacy's design law.

This Article is focused on the fourth way products liability can influence design ex ante—namely, directly, yet generally. Over time, products liability litigation has developed a series of requirements and corporate behavioral norms that define what manufacturers have to do even before they get hooked into a tort lawsuit. By analogy, those norms and requirements offer us a new paradigm for what a privacy by design statute should require. This includes how companies can weigh the privacy risks against consumer benefits of new products and how to interpret the meaning of vague terms in the law long before either the threat of litigation or court-mandated designs. To be clear, I am not proposing a products liability tort for privacy by design. Rather, I am taking a snapshot of products liability norms and rules and suggesting that this snapshot can flesh out what a privacy by design statute

164. Dawson v. Chrysler, 630 F.2d 950, 958–59 (3d Cir. 1980).

165. Garrett v. Ford, 684 F. Supp. 407 (D. Md. 1987)

166. *Id.* at 411 (holding that compliance with federal regulations regarding seat belts does not pre-empt a different standard from being established through civil litigation); *see also* AM. ASS'N. FOR JUSTICE, DRIVEN TO SAFETY: HOW LITIGATION SPURRED AUTO SAFETY INNOVATIONS 5 (2010).

167. 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). This direct and specific effect of litigation is similar to how FTC consent decrees help technology companies determine what strategies, designs, and data use practices are "unfair or deceptive" under the FTC Act. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (arguing that the body of law created by FTC consent decrees amounts to a common law body of jurisprudence). "Those involved with helping businesses comply with privacy law . . . parse and analyze the FTC's settlement agreements, reports, and activities . . . ." *Id.* at 585–6.

168. *See, e.g.*, Dow Chemical v. Mahlum, 970 P.2d 98, 118–19 (Nev. 1998) (discussing, among other things, the fact that insufficient testing the safety of silicone in breast implants can be used as evidence in a products liability suit).

should require in practice. After all, doctrinal analogies are common throughout the law and particularly in privacy,[169] where vague case law and statutes are constantly being referenced to answer new questions posed by new technologies. In the manufacturing context, products liability helped redesign dangerous products before. It can do so again for today's data-hungry technologies.

### *C. Applying the Products Liability Analogy*

Products liability for design defects can answer privacy by design's open questions—Who is responsible for design? When does design take place? What does design law require? What are its goals and purposes? And how can users pursue their rights under the law?—and, thereby, transform privacy by design into privacy's design law.

#### *1. Who?*

Privacy by design asks data collectors and upstream technology developers to include privacy considerations during the course of the design process.[170] Though doing so makes some intuitive sense, this allocation of responsibility is subject to an epistemic attack based on STS and sociology scholarship that reminds us that design is not limited to heroic engineers or the corporations that hire them.[171] Products liability had to respond to this same problem. It, too, had to allocate responsibility to someone. But it also acknowledged that users influence design when they modify products after purchase and when they use them in ways designers did not expect. Rather than giving up entirely, the common law adapted to the fact that design is a multifaceted social process by retaining manufacturer liability where consumer modifications and uses were reasonably foreseeable. Privacy's design law can learn from these doctrines to place the onus of privacy design on technology companies.

In the products liability context, manufacturers must do more than design reasonably safe products. They must design them so they can withstand both intended uses and those uses that, though unintended or unimagined by the designer, are reasonably foreseeable.[172] In *Barker v. Lull Engineering*,[173] for example,

---

169. There are really too many to list. *See, e.g.*, United States v. Johnson, 380 F.3d 1013 (7th Cir. 2004) (analogizing the inevitable discovery doctrine in Fourth Amendment law to the concurrent causation doctrine to answer a Fourth Amendment question about whether a second illegal search could cure the defects of a first illegal search); *see also* Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 670 (2006) (suggesting an analogy from privacy to trade secret law to address the problem of "relative privacy"); Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1241–45 (2000) (analogizing privacy to intellectual property, generally, as both doctrines concerned with control over information).

170. *See supra* Part I.A.1.

171. *See supra* Part I.A.2.

172. *See, e.g.*, Micallef v. Miehle Co., 348 N.E.2d 571, 577 (N.Y. 1975).

173. Barker v. Lull Engineering, 573 P.2d 443 (Cal. 1978).

a high-lift loader that was designed without outriggers overturned while working on a slope, injuring the lift's operator.[174] One of the manufacturer's responses to the plaintiff's products liability claim was that the lift was never meant to operate on a slope.[175] The trial judge took this to heart, instructing the jury that they could only find the manufacturer liable if its product was being used in the intended manner.[176] The California Supreme Court rejected this, noting that the proper instruction had to include uses in "reasonably foreseeable manner[s]."[177] It was reasonably foreseeable that a lift would sometimes be used on ground that was not perfectly flat. Similarly, in *Katz v. Swift & Company*,[178] a butcher was injured when a rubber band securing lamb shanks snapped off.[179] The court found that it was reasonably foreseeable that the bands would cause injury if not properly secured.[180]

In both these cases, it was immaterial that the defendants claimed they did not anticipate the particular use or misuse of their products. It "was sufficient that it was foreseeable that injury might result" from uses that were reasonable, even if unintended.[181] Otherwise, if designer intent delimited liability, then car manufacturers would be immune from lawsuits when their cars crashed and chair manufacturers would not have to design chairs strong enough for people to stand on; cars are meant to be driven, not crashed, and chairs are meant for sitting, not standing. Foreseeability became the linchpin of manufacturer liability, thus reflecting the reality of user involvement in the design process and the social construction of cultural artifacts.

In most jurisdictions,[182] moreover, manufacturer liability withstands not just unintended uses but subsequent modifications. *Thompson v. Package Machine Company*[183] and *Soler v. Castmaster*[184] are prime examples. In *Thompson*, the plaintiff lost her arm while reaching inside a plastic molding machine to remove a finished piece. She alleged several design defects, particularly to the safety mechanisms that were supposed to keep the machine open so a completed segment of plastic could

174. *Id.* at 447.
175. *Id.* at 448.
176. *Id.* at 449.
177. *Id.* at 452, 455–56.
178. Katz v. Swift & Co., 276 F.2d 905 (1960).
179. *Id.* at 905.
180. *Id.* at 906 (the "defendant knew or should have known that if the rubber band were not securely attached it might slip off and cause injury").
181. *Id.*
182. New York, among a few others, is an exception. In *Robinson v. Reed-Prentice Division*, 403 N.E.2d 440 (N.Y. 1980), the New York Court of Appeals, the state's highest court, held that a manufacturer of a product will not be held liable for a user's injuries where "after the product leaves the possession and control of the manufacturer, there is a subsequent modification which substantially alters the product and is the proximate cause of plaintiff's injuries." Robinson v. Reed-Prentice Division, 403 N.E.2d 440, 441 (N.Y. 1980). The majority of jurisdictions follow California's and New Jersey's rule on manufacturer liability even with subsequent consumer modifications. *See infra* nn. 184–90 and accompanying text.
183. Thompson v. Package Machine Co., 99 Cal. Rptr. 281 (1971).
184. Soler v. Castmaster, 484 A.2d 1225 (N.J. 1984).

be removed and replaced.[185] The company argued that only a modification to the machine after it had left the factory could have caused the safety latches to malfunction.[186] The court declined to hold that a manufacturer could be immune from liability as a matter of law simply because of a "reasonably foreseeable" modification.[187]

The New Jersey Supreme Court came to a similar holding in *Soler*. There, the safety gate on a die-casting machine malfunctioned, injuring the plaintiff's hands when he tried to remove a finished product from the mold.[188] Notably, though, the machine was not originally designed with a safety mechanism; the plaintiff's employer had added one that would automatically shut off the machine's power when the gate was open, thus allowing workers to reach in.[189] The court declined to exonerate the machine's manufacturer, despite the modification.[190] Adding safety elements was foreseeable, the court said, especially since safety mechanisms were available on the market when the defendant built the machine.[191]

Though they may not have recognized it at the time, the *Barker*, *Katz*, *Thompson*, and *Soler* courts were wrestling with the social aspects of design and technology. Each case shows that users do not just use; they also influence design. By deploying machines in ways their designers did not expect—much like when farmers used the first cars as stationary power sources[192] or how rural women used their first telephones as agents of social connection[193]—the plaintiffs in *Barker* and *Katz* changed the design. In *Thompson* and *Soler*, consumers made physical modifications to machines, much like women had for years made a variety of adjustments to household and cooking appliances, all of which were created by men, when the designs did not suit their needs.[194] Against this backdrop, most jurisdictions retained manufacturer liability despite user influence over design where uses and modifications were foreseeable. This puts the onus on manufacturers not just to design reasonably safe products (chairs that can be sat on), but also to consider the myriad ways in which their products can be used and how those products and uses fit into the broader ecosystem of social practice (chairs on which one can stand to reach a high shelf).

This provides a convenient analogy to define the *who* of privacy's law of design. Most jurisdictions retain manufacturer liability for defective products despite user impact on design. Not doing so would let manufacturers escape responsibility too often and, therefore, undermine the goals of products liability

185. *Thompson*, 99 Cal. Rptr. at 283.
186. *Id.*
187. *Id.* at 286.
188. *Soler*, 484 A.2d. at 1227.
189. *Id.* at 1228.
190. *Id.* at 1233.
191. *Id.*
192. *See* Kline & Pinch, *supra* note 61, at 768–94.
193. *See* MARTIN, *supra* note 61.
194. *See* Cowan, *supra* note 70.

generally.[195] But in a nod to the social nature of design, courts limit that responsibility to designing for foreseeable uses. An analogous rule can be applied to a privacy by design statute: technology companies are responsible for privacy by design, and their duties to consider privacy from the ground up extends to the privacy implications of all the foreseeable uses of their products. In Part II.C.3, I discuss what that means in detail.

*2. When?*

But before detailing the *what* of design law, we have to determine the *when* of design. Given that design is an ongoing process that can continue well after product release, during what time span do corporate design law responsibilities exist? Products liability law generally requires manufacturers to design products that are reasonably safe from the moment of sale or distribution.[196] This is mostly because harm to consumers starts at sale.[197] But manufacturer duties extend well beyond that. Indeed, the products liability analogy suggests that privacy by design duties should exist throughout the lifecycle of data collection tools, from conception through use.[198]

Products liability scholars have long debated the point in time at which courts should judge the safety of products.[199] John Wade listed six possibilities: at the time of manufacture, distribution, purchase, injury, trial, or at no time in particular.[200] Both Restatements seemed to have settled on the time of distribution or sale. The

---

195. *See, e.g.*, John Jay Fossett, *The Development of Negligence in Computer Law*, 14 N. KY. L. REV. 289, 306 (1987) ("Four policies are generally recognized as supporting the imposition of strict products liability. First, the party in the best position to detect and eliminate defects should be responsible for damages inflicted by defective products. Second, liability should be placed upon the party best able to absorb and spread the risk or cost of injuries through insurance. Third, a remedy should not be prevented by burdensome requirements of proof, since an injured person is not normally in a position to identify the cause of the defect. Fourth, due to modern marketing methods, consumers today rely on the reputation of a manufacturer and no longer accept the doctrine of caveat emptor.").

196. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 402A(1)(b) (1977); RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (1998); *see* Chown v. USM Corp., 297 N.W.2d 218, 221 (Iowa 1980) (holding that a plaintiff has to show that the design was unsafe as of time product manufactured).

197. One of the goals of products liability is to reduce and ameliorate the harm faced by consumers. *See, e.g.*, Virginia E. Nolan & Edmund Ursin, *Enterprise Liability and the Economic Analysis of Tort Law*, 57 OHIO ST. L.J. 835, 847 (1996); *see also* CALABRESI, *supra* note 42, at 24–94; Donald G. Gifford, *The Peculiar Challenges Posed by Latent Diseases Resulting from Mass Products*, 64 MD. L. REV. 613, 627 (2005) (discussing Calabresi's view that tort law can protect consumers from harm).

198. Notably, this is how Article 25 conceptualizes the *when* of privacy by design. Article 25(1) states, in relevant part, that "the controller shall, *both at the time of the determination of the means for processing and at the time of the processing itself*, implement appropriate technical and organisational measures . . . ." Regulation 2016/679, *supra* note 1, art. 25, at 48 (emphasis added).

199. John W. Wade, *On the Effect in Product Liability of Knowledge Unavailable Prior to Marketing*, 58 N.Y.U. L. REV. 734, 739 (1983) (a defect "is not defined relative to a particular point in time").

200. *Id.* at 753–54.

Second Restatement focuses liability on a product that is "expected to and does reach the user or consumer without substantial change in the condition in which it is sold,"[201] implying that manufacturers are responsible for ensuring safety before their products leave the warehouse. The Third Restatement limits defects to those found "at the time of sale or distribution."[202] This suggests that designer and manufacturer responsibilities end at product release.[203]

But these Restatement provisions do not tell the whole story. It is axiomatic that manufacturers retain certain duties to consumers after sale.[204] Manufacturers have a duty to warn consumers of latent defects when the manufacturer discovers them.[205] The rationale for this ongoing duty is that products with latent defects already on the market pose significant risks to consumers, and products liability law is meant, in part, to reduce danger to unsuspecting users.[206] At the same time, however, manufacturers are rarely required to update their old products and retrofit those on the market to accommodate the latest and best safety technologies.[207] Doing so would be too onerous, administratively difficult, and prohibitively

---

201. RESTATEMENT (SECOND) OF TORTS § 402A(1)(b) (1977).

202. *See* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 (1998).

203. *See* Michael B. Gallub, *Limiting the Manufacturer's Duty for Subsequent Product Alteration: Toward a Rational Approach*, 16 HOFSTRA L. REV. 361, 363 (1988).

204. *See, e.g.*, John S. Allee, *Post-Sale Obligations of Product Manufacturers*, 12 FORDHAM URB. L.J. 625 (1984) (discussing and collecting cases on post-sale duty-to-warn contexts); Victor Schwartz, *The Post Sale Duty to Warn: Two Unfortunate Forks in the Road to a Reasonable Doctrine*, 58 N.Y.U. L. REV. 892 (1983) (similar).

205. *See* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY, *supra* note 202 at § 10; *see also* Bly v. Otis Elevator, 713 F.2d 1040, 1046 (4th Cir. 1983) ("the duty to warn is continuous and is not interrupted by manufacture or sale of the product."); Comstock v. Gen. Motors Corp., 99 N.W.2d 627, 634 (Mich. 1959) (there exists "duty to give prompt warning exists when a latent defect which makes the product hazardous to life becomes known to the manufacturer shortly after the product has been put into the market").

206. *See, e.g.*, Alden D. Holford, *The Limits of Strict Liability for Product Design and Manufacture*, 52 TEX. L. REV. 81, 81–82 (1973) (explaining that one of the goals of products liability law is to protect consumers from dangerous materials on the market).

207. *See, e.g.*, Habecker v. Copperloy Corp., 893 F.2d 49, 54 (3d Cir. 1990) (no Pennsylvania case has ever required a duty to retrofit); Noel v. United Aircraft Corp., 342 F.2d 232 (3d Cir. 1964) (a manufacturer is under a continuing duty to improve the safety of its products, even those already on the market); Gregory v. Cincinnati, Inc., 538 N.W.2d 325, 336–37 n. 42 (Mich. 1995) (rejecting the idea that manufacturers had a duty to update and retrofit products based on newly available safety technology because of the burden that would entail); Patton v. Hutchinson Wil-Rich Mfg. Co., 861 P.2d 1299, 1308–09 (Kan. 1993) (post-sale retrofitting duties would create perverse incentives for manufacturers). When feasible in and certain limited circumstances, however, manufacturers have been required to remedy the danger. *See, e.g.*, Braniff Airways, Inc. v. Curtis-Wright Corp., 411 F.2d 451, 453 (2d Cir. 1969) ("It is clear that after such a product has been sold and dangerous defects in design have come to the manufacturer's attention, the manufacturer has a duty to either remedy these or, if complete remedy is not feasible, at least to give users adequate warnings and instructions concerning methods for minimizing the danger."); Bell Helicopter v. Bradshaw, 594 S.W.2d 519, 532 (Tex. Civ. App. 1979) (manufacturer post-sale duties required the company to "mandate replacement" of dangerous helicopter blade system, or to strongly suggest replacement in a notice "reasonably calculated to impress upon users the gravity of the risk, that such replacement be made.").

expensive.[208] And most jurisdictions hold that manufacturers are immune from post-sale liability when they sell so-called "naked" products, or dangerous machinery that will not work upon sale unless the consumer installs whatever safety equipment she chooses, on the theory that the original manufacturer is selling an inoperative and, thus, not dangerous, product.[209]

These rules yield several lessons for the *when* of privacy by design. Manufacturer duties do not end at product release. Just like latent defects in manufactured products justify ongoing duties, privacy gaps in data collection code that pose continual risks to user data should give rise to ongoing duties as well.[210] In fact, this principle is already embodied in privacy law: data breach notification statutes require notifying consumers without unreasonable delay if personal data has been compromised[211] and the FTC requires user notifications when privacy policies change.[212] Moreover, whereas products liability generally declines to impose significant retrofitting duties on manufacturers because of cost and administrability, those barriers do not exist in the data collection context because most technology products are "tethered."[213] Tethered products, as defined by Chris Hoofnagle, Aniket Kesari, and Aaron Perzanowski, are those that are persistently linked to the seller, in this case, over wifi.[214] Regular updates to code over an internet connection are relatively inexpensive and easy to administer compared to the cost of rebuilding heavy machinery that is physically beyond the control of the manufacturer. Therefore, the products liability analogy would both obligate technology companies to design for privacy through the moment of sale and beyond, and include ongoing duties to update platforms to better protect privacy going forward.

*3. What?*

Privacy by design requires technology companies to consider privacy from the ground up, making it endemic to their corporate culture and the products they create. But commentators have never been clear about what that means in practice.[215] The products liability paradigm can help to specify the requirement. Since the California Supreme Court unanimously adopted a strict liability standard

208. *See* Schwartz, *supra* note 204, at 898 (arguing that courts do not impose a post-sale duty to retrofit, in part, because of the expense); *see also, e.g.*, *Cincinnati Inc.*, 538 N.W.2d at 336–37 n. 42 (declining to impose a duty to retrofit products with latest technology because of the burden on manufacturers).

209. *See, e.g.*, Bautista v. Verson Allsteel Press Co., 504 N.E.2d 772, 774 (Ill. App. Ct. 1987).

210. *See infra* Part II.C.3 (discussing standards for governing those notices).

211. *See, e.g.*, Cal. Civ. Code § 1798.82 (West 2017).

212. *See* Solove & Hartzog, *supra* note 167, at 616 (discussing how the FTC requires companies to notify consumers of wrongdoing and about updates to data use practices).

213. Chris Hoofnagle, Aniket Kesari & Aaron Perzanowski, *The Tethered Economy*, 87 GEO. WASH. L. REV. __ (forthcoming 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3318712 [https://perma.cc/5SY9-2QY6].

214. *Id.* at 1.

215. *See supra* Part I.B.1.

in products liability cases in *Greenman v. Yuba Power Products*,[216] design defects law has evolved to include a panoply of specific tests and doctrines that tease out manufacturer responsibilities. Products liability today is not the same as it was in *Greenman*. But four elements—the risk/utility doctrine, foreseeable unintended uses, the reasonable alternative design (RAD) test, and the duty to warn—can, when taken together, describe the specific elements that go into manufacturers' proactive obligations to design safe products. I argue that the same rules can clarify technology companies' duties under privacy's design law as well.

*a. Balancing Test During Design*

The California Supreme Court introduced the risk/utility test in *Barker v. Lull Engineering*[217] as one of two ways consumers could prove a manufacturer had designed a defective or unsafe product. *Barker* involved a high lift loader that overturned when it was used on a slope instead of flat ground.[218] The court said either a plaintiff could demonstrate that a product failed to perform "as an ordinary consumer would expect"[219]—the consumer expectations test—or a jury could determine that "the risk of danger inherent in the challenged design outweigh[ed] the benefits of such design"[220]—the risk/utility test. Later, the court clarified when to use each test.[221] A consumer expectations test is appropriate when common "everyday experience" is enough to understand how a product is supposed to work,[222] as when farmers are injured by defective tractors,[223] or when hospital workers get sick from unsafe latex gloves,[224] or when weightlifters are hurt by leg press machines they use regularly.[225] For more "complex" products like cars, a risk-utility test, informed by expert testimony, makes more sense.[226]

These tests normally operate inside adversarial litigation to determine ex post if a manufacturer violated its duty to consumers. But they can also have a direct effect on the design process.[227] Where applicable, a consumer expectations test encourages manufacturers to conform the design of everyday products to ordinary

216. Greenman v. Yuba Power Products Inc., 377 P.2d 897 (Cal. 1963).

217. Barker v. Lull Eng'g, 573 P.2d 443 (Cal. 1978).

218. *Id.* at 443.

219. *Id.* at 454.

220. *Id.* at 455.

221. *See* Soule v. Gen. Motors Corp., 882 P.2d 298 (Cal. 1994). Notably, the Restatement (Third) of Torts: Products Liability does not include the consumer expectations test for design defect cases. Scholars disagree about whether this accurately reflects the state of the law or merely models the conservative policy preferences of the Reporters. For scholarly debate on the merits of changes brought on by the Third Restatement, see the literature cited in nn. 238, 253.

222. *Soule*, 882 P.2d at 308, 310.

223. *See* Delaney v. Deere & Co., 999 P.2d 930, 945–46 (Kan. 2000).

224. *See* Green v. Smith & Nephew AHP, Inc., 629 N.W.2d 727, 751 (Wis. 2001). The plaintiff used forty latex gloves per shift. *Id.* at 732.

225. *See* Vautour v. Body Masters Sports Indus., Inc., 784 A.2d 1178, 1182 (N.H. 2001).

226. *Soule*, 882 P.2d at 309; *see also, e.g.*, Potter v. Chi. Pneumatic Tool Co., 694 A.2d 1319, 1333 (Conn. 1997).

227. *See infra* notes 5–169 and accompanying text; *see also* Tbl. 1.

uses and user expectations. The complexity of data collection tools, however, makes that impossible in the privacy context.[228] A risk-utility test, however, encourages companies to weigh safety dangers against the benefits of the product during the design phase before product release. Notably, this is precisely the goal of privacy by design.

Indeed, as scholars have noted, the problem identified by privacy by design is that privacy is getting short shrift before technology products are released,[229] forcing privacy law to focus, rather ineffectively,[230] on punishments after the fact.[231] If privacy could be considered during design, it could compete against pernicious motives[232] and the contrary incentives of corporate actors.[233] This may require a heavy lift at some companies, including creating an active privacy team integrated into the design process[234] and sufficiently powerful to make its voice heard within the corporate dynamic.[235] It would require a group of privacy lawyers inside the design process to spot privacy issues as they come up.[236] And it would require documenting the ways in which privacy is considered during design and how the product that emerges does not put privacy at unnecessary risk relative to its benefits. Understood through the analogy of the risk-utility test, then, privacy by design's expectation that companies will consider privacy from the ground up can be

228. *See, e.g.*, PASQUALE, *supra* note 44, at 3, 28–31; Pauline Kim, *Data Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 889 (2017) ("[T]he quality or characteristic the model seeks to maximize (the target variable) may be clearly specified, but the algorithm is so complex that it is not possible to explain which factors drive the model's predictions."); W. Nicholson Price II, *Big Data, Patents, and the Future of Medicine*, 37 CARDOZO L. REV. 1401, 1404 (2016) (describing black box algorithms as "'black-box' precisely because the relationships at [their] heart are opaque—not because their developers deliberately hide them, but because . . . they are too complex to understand"); Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 886 (2016) (noting that algorithms can be so complex that the programmers do not even understand how they work).

229. *See* HARTZOG, *supra* note 4, at 5 (noting the extraordinary incentives to design technologies to enhance data collection rather than restrict it); Waldman, *Designing Without Privacy*, *supra* note 91, at 685–89 (discussing how some engineers at technology companies simply fail to consider privacy during design because of other pressing demands, the ambiguous nature of privacy, and a lack of corporate attention).

230. *See, e.g.*, Solove & Citron, *supra* note 15, at 747–56 (discussing how courts have generally declined to recognized data breach harms); Strahilevitz, *supra* note 169, 939–46 (discussing the lack of clear rationales in decisions "limited privacy" cases, with many results failing to protect privacy).

231. *See* Richards & Hartzog, *supra* note 104, at 436.

232. *See, e.g.*, 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/ [ https://perma.cc/T9YC-A4E5].

233. *See, e.g.*, Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014) (arguing that technology companies have primary incentives to collect more information about consumers in order to compete with their competitors); Rubinstein, *supra* note 88, at 1431–44 (discussing the role of market incentives in corporate decisions to adopt privacy-enhancing technologies).

234. *See* Waldman, *Designing Without Privacy*, *supra* note 91, at 711–25 (arguing for corporate organizational changes to better integrate privacy into the design process).

235. *See* BAMBERGER & MULLIGAN, *supra* note 90.

236. *See* Waldman, *Designing Without Privacy*, *supra* note 91, at 714–15.

translated into design law as a requirement to perform a balancing of privacy harms against consumer benefit during the design phase of new products.[237]

*b. Foreseeable Uses*

Although there is considerable scholarly disagreement on whether it should be part of the law of products liability,[238] foreseeability was included in the Third Restatement. It defines a defective product as one where the "foreseeable risks of harm" could have been avoided by a safer design.[239] Foreseeability is also part of the doctrine of unintended uses, as discussed above.[240] The foreseeability doctrine offers another helpful analogy for privacy's law of design. When conducting risk-utility balancing, technology companies should consider the privacy implications of all foreseeable uses of a product.[241]

Data-based technologies have been used in many ways their designers might not have intended. For example, Facebook claims it was designed to bring people together,[242] not to spread fake news[243] or manipulate user behavior.[244] Live-streaming technology may have been designed to help reach a vast audience at low cost, but it has also been used to broadcast sexual assault[245] and mass shooting.[246] And location-based tracking may facilitate a host of modern conveniences, but it

---

237. *See* HARTZOG, *supra* note 4, at 127–28.

238. Although I use foreseeability here, I am not arguing that liability for defective products *should* be based on a foreseeability standard. Rather, the goal of this Article is to describe ex ante obligations for privacy by design. Liability is not an issue. For arguments against including foreseeability in products liability, please see, e.g., John B. Attanasio, *The Principle of Aggregate Autonomy and the Calabresian Approach to Products Liability*, 74 VA. L. REV. 677 (1988); Stephen P. Croley & Jon D. Hanson, *Rescuing the Revolution: The Revived Case for Enterprise Liability*, 91 MICH. L. REV. 683 (1993); Mark Geistfeld, *Reconciling Cost-Benefit Analysis with the Principle That Safety Matters More Than Money*, 76 N.Y.U. L. REV. 114 (2001); Jon D. Hanson & Kyle D. Logue, *The First Party Insurance Externality: An Economic Justification for Enterprise Liability*, 76 CORNELL L. REV. 129 (1990); Keating, *supra* note 162; Kysar, *supra* note 127, at 1790; Stephen F. Williams, *Second Best: The Soft Underbelly of Deterrence Theory in Tort*, 106 HARV. L. REV. 932 (1993).

239. *See* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2(b) (1998).

240. *See supra* Part II.C.1.

241. *See, e.g.*, Gallub, *supra* note 203, at 404 n. 2424 (noting that "foreseeability of product's uses establishes the parameters of its manufacturer's responsibility").

242. *See, e.g.*, Josh Constine, *Facebook Changes Its Mission Statement to 'Bring the World Closer Together,'* TECHCRUNCH (June 22, 2017), https://techcrunch.com/2017/06/22/bring-the-world-closer-together/ [https://perma.cc/7KD8-XYC8].

243. *See, e.g.*, Siobhan Hughes, *Mark Zuckerberg: Facebook Made Mistakes on 'Fake News,' Privacy*, WALL STREET J. (Apr. 9, 2018 2:45 PM), https://www.wsj.com/articles/mark-zuckerberg-facebook-made-mistakes-on-fake-news-privacy-1523289089 [https://perma.cc/92P8-BMDG].

244. *See, e.g.*, Kashmir Hill, *Facebook Manipulated 689,003 Users' Emotions for Science*, FORBES (June 28, 2014 2:00 PM), https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/#3df42df7197c [https://perma.cc/KV8T-TA3Y].

245. *See, e.g.*, Brittney McNamara, *Girl Who Live Streamed Rape on Periscope Sentenced to Prison*, TEEN VOGUE (Feb 15, 2017 6:40 PM), https://www.teenvogue.com/story/girl-live-streamed-rape-on-periscope-sentenced-prison [https://perma.cc/X9RT-S8D2].

246. *See* Kate Klonick, *Inside the Team at Facebook That Dealt with the Christchurch Shooting*, NEW YORKER (Apr. 25, 2019 12:16 PM), https://www.newyorker.com/news/news-desk/inside-the-team-at-facebook-that-dealt-with-the-christchurch-shooting [https://perma.cc/JD7V-MM4S].

has also been a tool of intimate partner harassment and invasions of privacy.[247] Admittedly, only some of these uses are arguably foreseeable. And reasonable people can disagree; foreseeability in tort law is usually a question of fact for a jury anyway.[248] But in the ex-ante design context, foreseeability would be a fact-based conversation among technology product designers, privacy professionals, users, professional associations, journalists, and independent and academic experts, each of whom may bring unique perspectives on foreseeable uses. At a minimum, using the design phase to consider at least the foreseeable potential dangers of privacy-compromising technologies can make technology products safer.

For example, the genetic testing company 23andMe recently formed a partnership with the pharmaceutical giant, GlaxoSmithKline, to use 23andMe's storehouse of DNA data to develop new drugs.[249] This eventuality was arguably foreseeable from the moment 23andMe's saliva-based home DNA tests were designed. The company included the possibility in its privacy policy.[250] But the partnership with Glaxo raises several privacy concerns, including the risks in transferring personal data, the potential dangers for blood relatives who never consented to use of their DNA, and the likelihood that 23andMe customers may not have understood the implications of their consent. Considering these questions before product release could have led to several design modifications to the product that could pre-empt problems after the fact. Granted, consent to participate in research was designed as an opt-in, rather than opt-out. But the company could have gone further by making the opt-in far clearer, including explaining exactly how the consumer's DNA data will be used,[251] and more noticeable, whether through an on-screen pop-up during registration or a brightly-colored insert in the package itself. Designers could have also created anonymization and security tools with future partnerships in mind. Executives could have also minimized the amount of

247. *See, e.g.*, DIANA FREED ET AL., "A STALKER'S PARADISE": HOW INTIMATE PARTNER ABUSERS EXPLOIT TECHNOLOGY (Apr. 2018), http://www.nixdell.com/papers/stalkers-paradise-intimate.pdf [perma.cc/RW9L-MJMW].

248. *See, e.g.*, Merriweather v. E.W. Bliss Co., 636 F.2d 42, 45 (3d Cir. 1980) (same); Wingett v. Teledyne Indus., 479 N.E.2d 51, 56 (Ind. 1985) (holding that the question of foreseeability is properly for a jury); Thibault v. Sears, Roebuck & Co., 395 A.2d 843, 847–48 (N.H. 1978) (same).

249. *See* Maggie Fox, *Drug Giant Glaxo Teams up with DNA Testing Company 23andMe*, NBC NEWS (July 25, 2018 2:00 PM), https://www.nbcnews.com/health/health-news/drug-giant-glaxo-teams-dna-testing-company-23andme-n894531 [https://perma.cc/LC2Z-2TZ9].

250. *See Privacy Highlights*, 23ANDME, https://www.23andme.com/about/privacy/ [https://perma.cc/KL5W-ES95] (last visited June 16, 2019) ("If you choose to consent to participate in 23andMe Research, 23andMe researchers can include your de-identified Genetic Information and Self-Reported Information in a large pool of customer data for analyses aimed at making scientific discoveries.").

251. *Compare id.* (referring only to "use of your data for scientific research purposes"), *Frequently Asked Questions*, "*Privacy*," ALL US RES. PROGRAM https://www.joinallofus.org/en/faq [https://perma.cc/EL5V-UMHA] (last visited June 16, 2019) (explaining precisely when, how, and why personal information may be used).

data they would share with pharmaceutical companies.[252] These steps cannot guarantee safety from privacy or data breaches, but they can pinpoint inflexion points and ameliorate the risk.

*c. A Reasonable Alternative Privacy-Protective Design*

That said, merely requiring companies to engage in a balancing test of foreseeable benefits and harms is still rather vague. A third products liability analogy—the reasonably alternative design, or RAD, test—can specify what technology companies should be balancing. The rich literature on RAD is voluminous, including whether it reflects the state of the common law[253] or undermines the entire project of strict liability for defective products.[254] Those debates are for another time. For our purposes, a RAD is, on its face, easy to understand: if a safer way of designing a product with available technology[255] would have reduced the foreseeable risk of harm[256] without undue cost, the manufacturer should have chosen that design instead of the more dangerous one. Or, put another way, a safer design's costs (including manufacturing costs and reduced product functionality, among others) must be less than the costs of foreseeable injuries prevented by incurring the costs of the safer design.[257]

Wherever one stands on the role of RAD in design defect litigation, the concept can serve as a convenient analogy for privacy's design law. Like RAD, where a manufacturer has to weigh the costs of safer designs against the foreseeable injuries, privacy by design requires a technology company to weigh the costs of more privacy-protective design—including privacy defaults, opting in to data collection, just-in-time notifications, enhanced consents, data minimization,

252. This principle is embodied in the GDPR. *See* Regulation 2016/679, *supra* note 1, art. 5(1)(c), at 35 (data minimization).

253. *See, e.g.*, James A. Henderson, Jr. & Aaron D. Twerski, *Achieving Consensus on Defective Product Design*, 83 CORNELL L. REV. 867 (1998) (justifying the conclusion that RAD had been adopted by many jurisdiction through analysis of case law); Frank J. Vandall, *The Restatement (Third) of Torts: Products Liability Section 2(B): The Reasonable Alternative Design Requirement*, 61 TENN. L. REV. 1407, 1408–13 (1994) (reviewing cases challenging the conclusion that RAD was supported by the majority of jurisdictions at the time). This debate is beyond the scope of this Article. This Article takes no position on whether demonstrating a RAD *should* be part of a products liability claim. Rather, it is based on the presumption that RAD is at least part of the law of products liability for design defects today, something even critics have come to accept. *See* Vandall, *supra* 1413–20 (noting that some jurisdictions include RAD as either one factor to consider in risk-utility balancing and that other jurisdictions require defendants to prove that there was no RAD).

254. *See, e.g.*, Ellen Wertheimer, *The Biter Bit: Unknowable Dangers, the Third Restatement, and the Reinstatement of Liability Without Fault*, 70 BROOK. L. REV. 891 (2005) (seeing RAD as reneging on the promise of strict liability in products liability).

255. *See* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 reps. n. cmt. d(IV)(B) (1998). The Restatement uses the phrase "state of the art" and notes that the phrase "has been variously defined by a multitude of courts. For some it refers to industry custom or industry practice; for others it means the safest existing technology that has been adopted for use; for others it means cutting-edge technology."

256. *Id.* at § 2 cmt. f.

257. *See id.* at cmts. d, f.

restrictions on processing, limitations on collections and storage, and so forth—against foreseeable privacy risks and any loss in program utility or function. If a safer, more privacy-enhancing option exists without undue sacrifices in function, privacy's design law would require companies to choose the safer option.[258]

The Third Restatement places the burden of proving a RAD on a plaintiff during litigation.[259] But that is a minority view; only a few states have abandoned the Second Restatement for the Third in this regard.[260] In *Barker v. Lull Engineering*,[261] for example, the California Supreme Court concluded that when consumers had everyday experience with the products at issue, design defects should be determined on a consumer expectations test. But when the product was too complex for ordinary comprehension, risk-utility balancing made more sense.[262] As several courts have already concluded,[263] the burden of demonstrating that no other RAD exists is the manufacturer's responsibility.[264] In the context of privacy's law of design, the very complexity of algorithmic platforms[265] and technology companies' continued insistence on maintaining the secrecy of their data collection tools also suggests that they should shoulder the burden of demonstrating that a RAD did not exist when they built and sold their products.

To support this more directed balancing test, companies can learn from privacy impact assessments (PIAs) at government administrative agencies. PIAs are analyses of how personal information is collected, used, shared, and maintained.[266] Their purpose is to ensure that designers, executives, privacy professionals, and other relevant employees have consciously incorporated privacy protections throughout the lifecycle of a product. More specifically, PIAs identify and evaluate privacy risks, consider alternatives, identify strategies to mitigate risks, and help

---

258. *See also* HARTZOG, *supra* note 4, at 128.

259. *See also* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2(b) (1998).

260. *See* Vandall, *supra* note 253, at 1408–13.

261. Barker v. Lull Eng'g Co., 573 P.2d 443 (Cal. 1978).

262. *See, e.g.*, *id.* at 455–56 (the risk-utility test "places the burden on the manufacturer, rather than the plaintiff, to establish that because of the complexity of, and trade-offs implicit in, the design process, an injury-producing product should nevertheless not be found defective."); *see supra* notes 218–27 and accompanying text.

263. *See, e.g.*, Onati v. Straub Clinic & Hosp., Inc., 659 P.2d 734 (Haw. 1983) (applying *Barker*); Caterpillar Tractor Co. v. Beck, 593 P.2d 871 (Alaska 1979) ("We hold that the plaintiff need only show that he was injured and that the injury was proximately caused by the product's design. The defendant may then avoid liability for a defectively designed product by proving by a preponderance of the evidence that 'on balance, the benefits of the challenged design outweigh the risk of danger inherent in such design.'").

264. *See* Vandall, *supra* note 253, at 1408–13.

265. *See* PASQUALE, *supra* note 45, at 140–42; *see also* Frank Pasquale, *Bittersweet Mysteries of Machine Learning (A Provocation)*, LONDON SCH. ECON. & POL. SCI.: MEDIA POL'Y PROJECT BLOG (Feb. 5, 2016), http://blogs.lse.ac.uk/mediapolicyproject/2016/02/05/bittersweet-mysteries-of-machine-learning-a-provocation/ [https://perma.cc/849V-Q8BS] (calling complex algorithms the "sweet mystery of machine learning").

266. FED. TRADE COMM'N, PRIVACY IMPACT ASSESSMENTS, https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments [https://perma.cc/LB7H-YAC4] (last visited June 16, 2019).

articulate the rationale for the final product.[267] Therefore, PIAs help technology products designers conduct their own version of a RAD analysis, ensuring that privacy-protective options get a fair shot during design. Although simply adopting a version of a PIA would be insufficient—a commitment to privacy has to be instantiated into the culture, as well[268] and not merely a symbol of compliance[269]—the protocol would force companies to make a record of their privacy considerations and foster transparency and accountability.[270]

*d. Privacy Notices and Design*

Alongside conducting a risk-benefit analysis and determining if a RAD exists, manufacturers also have duties to warn consumers of foreseeable dangers.[271] Technology companies that collect our data have similar duties to warn; indeed, informing users of a company's data use practices is at the heart of the notice-and-choice regime that governs much of consumer privacy law today.[272] But, as I have argued elsewhere, neither data collectors nor regulators have paid much attention to the manner in which privacy notices are presented to users, despite the fact that design and aesthetics can be manipulative.[273] An analogy to the duty to warn in products liability would establish notice as a design obligation and bring much needed corporate and regulatory attention to the design of privacy policies.

There are two types of warnings in products liability law. At the point of sale, manufacturers are required to warn customers of dangers associated with foreseeable uses of the product.[274] If sometime after sale, manufacturers learn or should have learned that their products are dangerous, they have a duty to make a reasonable effort to issue a post-sale warning to consumers.[275] And the general rule is that point-of-sale and post-sale warnings have to be "adequate," or reasonable under the circumstances.[276] Post-sale duties to warn are more limited than those at the time of sale. Warning customers at the time of sale is relatively easy: a manufacturer can place labels on products before they leave the warehouse.[277] After

267. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 76 (2008).

268. *Id.* at 78.

269. *See* EDELMAN, *supra* note 18 (discussing how merely symbolic structures have replaced substantive progress as evidence of compliance with civil rights laws).

270. *See* A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1752 (2015) (recommending the adopting of Privacy Impact Notices (PINs), combining transparency and accountability in good privacy design).

271. *See, e.g.*, Richter v. Limax Int'l, Inc., 45 F.3d 1464, 1471 (10th Cir. 1995) (manufacturers have a duty to warn of dangers "reasonably foreseeable to the manufacturer of the product").

272. *See* Solove & Hartzog, *supra* note 167, at 592 (noting how privacy policies are used to fulfill the "notice" part of "notice and choice").

273. *See* Waldman, *Privacy, Notice, and Design*, *supra* note 23.

274. *See, e.g.*, Melancon v. W. Auto Supply Co., 628 F.2d 395, 399 (5th Cir. 1980).

275. *See, e.g.*, Bertrand v. Johns-Manville Sales Corp., 529 F. Supp. 539, 542 n.2 (D. Minn. 1982).

276. *See, e.g.*, Brochu v. Ortho Pharm. Corp., 642 F.2d 652, 657 (1st Cir. 1981); Levin v. Walter Kidde & Co., 248 A.2d 151 (Md. 1968).

277. *See* Lovick v. Wil-Rich, 588 N.W.2d 688, 693 (Iowa 1999).

sale, after a product leaves the control of the manufacturer, practical barriers make post-sale warnings far more expensive and difficult.[278]

In certain cases, courts have gone further, describing what adequate notices should look like. Warnings need to be "clear and specific," and clear and unequivocal warnings on the product itself or in the owner's manual have sufficed.[279] Notices that are too long can undermine their effectiveness. As the Fourth Circuit has stated, "Well-meaning attempts to warn of every possible accident lead over time to voluminous yet impenetrable labels—too prolix to read and too technical to understand."[280] Several courts have also held that warnings cannot be simple lists of risks; rather, they must convey information in a format and using language that gets a consumer's attention and conveys the seriousness of the risks involved.[281] Notice adequacy in products liability law is, therefore, a matter of "display, syntax and emphasis."[282] Warnings must also be attuned to a consumer's level of knowledge, or reflect a foreseeable consumer's lack of experience or skill operating the product.[283]

Privacy notices can learn from this jurisprudence. The two types of notices in privacy map neatly on manufacturers' warnings. First, privacy policies, which developed first as industry's way to stave off regulation[284] and spread further under state and federal mandates,[285] are akin to point-of-sale warnings. Privacy policies

278. *See id.* at 694; *see also* Schwartz, *supra* note 204, at 895–96.

279. *See* Hood v. Ryobi Am. Corp., 181 F.3d 608, 611 (4th Cir. 1999).

280. *Id.*

281. *See Brochu*, 643 F.2d at 657. A product warning "may be inadequate in factual content, in expression of the facts, or in the method by which it is conveyed." Graham v. Wyeth Labs., 666 F. Supp. 1483, 1498 (D. Kan. 1987).

282. *See* D'Arienzo v. Clairol, Inc., 310 A.2d 106, 112 (N.J. Sup. Ct. 1973) (adequacy "depends upon the language used and the impression that it is calculated to make upon the mind of an average user of the product" and involves "[q]uestions of display, syntax and emphasis").

283. *See* Todalen v. U.S. Chem. Co., 424 N.W.2d 73, 80 (Minn. Ct. App. 1988) (when developing product warnings, manufacturers have to consider inexperience or lack of skill of a foreseeable class of consumers). It is worth noting that many, but certainly not all, of the cases to describe this more detailed standard for adequacy involve drugs or chemicals. *See, e.g.*, *Brochu*, 643 F.2d at 653 (oral contraceptives); *Wyeth Labs.*, 666 F. Supp. at 1498 (vaccines); *D'Arienzo*, 310 A.2d at 226 (hair dye). The Restatement (Third) of Torts immunizes prescription drug manufacturers from design defect liability, see James A. Henderson, Jr. & Aaron D. Twerski, *Drug Designs Are Different*, 111 YALE L.J. 151 (2001), suggesting there may be a trend to treat drug manufacturers differently than other manufacturers. *But see* George W. Conk, *Is There a Design Defect in the Restatement (Third) of Torts: Products Liability*?, 109 YALE L.J. 1087 (2000). But, the standard is also used in other types of product liability cases. *See, e.g.,* Dalton v. Toyota Motor Sales, Inc., 703 F.2d 137 (5th Cir. 1983) (car); Stapleton v. Kawasaki Heavy Indus., Ltd., 608 F.2d 571, 572 (5th Cir. 1979), *opinion amended on denial of reh'g*, 612 F.2d 905 (5th Cir. 1980) (motorcycle).

284. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN. ST. L. REV. 587, 593 (2007) ("Online privacy policies have appeared . . . as voluntary measures by websites . . . ."); *see also* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2047 (2000) (noting that an FTC threat for greater regulation resulted in a substantial increase in the number of websites offering privacy policies); Solove & Hartzog, *supra* note 167, at 593–94.

285. *See* Waldman, *Privacy, Notice, and Design*, *supra* note 23, at 90–95 (showing how state and federal statutes require privacy policies).

warn us of all the ways in which our data will be collected, used, and shared. They are, however, confusing.[286] No one reads them.[287] They are long[288] and difficult to understand.[289] And they are designed and presented to us in ways that make them manipulative of our behavior.[290] Second, so-called "just-in-time" notices, roughly like post-sale warnings, are presented to us not when we first buy a Google Phone or visit a website, but at the moment just before data collection occurs while using a platform, product, or app, allowing us to navigate our disclosure behavior more effectively.[291] Just-in-time notices have been endorsed by the FTC and recommended as a best practice in the mobile privacy ecosystem.[292] But just-in-time notifications today are often take-it-or-leave-it and far more about encouraging users to just click "yes" and move on than consider their disclosure behavior.[293]

Privacy policies and just-in-time notifications today are ineffective because they are inadequately designed. In products liability, the design of warnings matters because courts recognize that presentation influences comprehension and only comprehensible notices can adequately protect consumers.[294] The same should be true of privacy notices. Under this analogy, "a clear, concise warning of potential" privacy concerns would be required.[295] It could be supplemented by a longer privacy policy intended for regulators, but technology companies and regulators should design and present privacy notices with an eye toward ordinary user comprehension,

---

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

287. *See, e.g.*, George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15, 24 (2004).

288. George R. Milne, Mary J. Culnan & Henry Greene, *A Longitudinal Assessment of Online Privacy Notice Readability*, 25 J. PUB. POL'Y & MARKETING 238, 243 (2006). Lorrie Cranor estimates that it would take a user an average of 244 hours per year to read the privacy policy of every website she visited. *See* Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOM. & HIGH TECH. L. 273, 274 (2012). This translates to about 54 billion hours per year for every U.S. consumer to read all the privacy policies she encountered. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y. 540, 563 (2008).

289. *See* Mark A. Graber, *Donna M. D'Alessandro & Jill Johnson-West, Reading Level of Privacy Policies on Internet Health Web Sites*, 51 J. FAM. PRAC. 642, 642 (2002).

290. *See* Waldman, *Privacy, Notice, and Design*, *supra* note 23.

291. FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 15 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [https://perma.cc/ZSJ6-AGPV].

292. *See id.* at 1.

293. *See* HARTZOG, *supra* note 4, at 23–67; *see also* Norwegian Consumer Council, *supra* note 141. Consider, for example, the take-it-or-leave-it approach of cookie notifications, which are often presented as acknowledgements with "ok" or "dismiss" buttons rather than with options to "accept" or "decline" cookies.

294. *See* D'Arienzo v. Clairol, Inc., 310 A.2d 106, 112 (N.J. Sup. Ct. 1973); Brochu v. Ortho Pharm. Corp., 642 F.2d 652, 657 (1st Cir. 1981).

295. *D'Arienzo*, 310 A.2d at 112.

using simple statements, user-friendly aesthetics, and colors and tables,[296] while making them accessible to users through pop-ups and even more "visceral" forms of notice that ensure understanding.[297] Moreover, because technology companies face none of the practical burdens manufacturers used to face when trying to reach consumers post-sale, just-in-time notifications should follow the same rules.

*4. Why?*

The next building block of privacy's design law is identifying its underlying values. This is an important task, as it helps make sense of confusing statutory language[298] and helps regulated entities craft effective compliance strategies. But, as discussed above, the various definitions of privacy by design reflect a variety of different values, including control, trust, and obscurity, among others.[299] Indeed, it is hard to imagine privacy values not embraced by some definition of privacy by design. A products liability paradigm offers a different perspective: fairness.

Fairness was at the heart of Justice Traynor's concurrence in *Escola v. Coca Cola Bottling*,[300] where he laid out the policy arguments justifying strict liability for defective products. Whereas manufacturers can anticipate some of the dangers in their own products, consumers of mass produced goods cannot.[301] Whereas manufacturers are well situated to bear the costs of preventing injury through new designs, consumers are generally unprepared to handle the overwhelming cost of injury to life and limb.[302] And whereas manufacturers are the ones placing dangerous goods on the markets, consumers are the ones getting injured.[303] As the torts scholar Gregory Keating put it, as between the party benefiting from production and the party that "happen[s] to be victims," those that cause harm as a result of their profit-making activities should be responsible, and not only because they can more easily absorb and distribute the loss.[304] It is, rather, a matter of simple fairness.[305] As a weapon of fairness, products liability law aims to reset the imbalance between producers and consumers, holding manufacturers' responsible for the harm they cause.

---

296. *See* Waldman, *Privacy, Notice, and Design*, *supra* note 23, at 117–24.

297. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1034–44 (2012).

298. *See, e.g.*, KARL LLWELLYN, THE COMMON LAW TRADITION: DECIDING APPEALS 268–77 (1960); Lon Fuller, *Positivism and Fidelity to Law: A Reply to Professor Hart*, 71 HARV. L. REV. 630, 667 (1958) (arguing that rather than trying to discern the meaning of specific words, the task of interpretation is to look at the statute and make it a "coherent, workable whole").

299. *See supra* Part I.B.2.

300. Escola v. Coca Cola Bottling, 150 P.2d 436 (Cal. 1944).

301. *Id.* at 440–41 (Traynor, J., concurring).

302. *Id.*

303. *Id.*

304. Gregory C. Keating, *Pressing Precaution Beyond the Point of Cost-Justification*, 56 VAND. L. REV. 653, 667 (2003) (calling this rationale "enterprise liability").

305. Gregory C. Keating, *Rawlsian Fairness and Regime Choice in the Law of Accidents*, 72 FORDHAM L. REV. 1857 (2004).

The wide social, informational, and resource asymmetry between technology companies and their users mirrors the power imbalance between manufacturers and consumers described by Justice Traynor in *Escola*, thus requiring a similar rebalance through a fairness lens. Technology companies know (or should know) about the privacy risks their products create, but because those data collection tools are "black box" proprietary algorithms, ordinary consumers are ill-equipped to protect themselves.[306] Technology companies are some of the most dynamic, nimble, and richest businesses operating today,[307] which makes them far more capable than ordinary consumers to address privacy dangers. Users can only try to deal with the enormous costs after something goes wrong. Fairness dictates that technology companies should shoulder the responsibility of designing products that better protect users from privacy dangers that users cannot protect against themselves.

Fairness also recognizes the undeniable connection between privacy and equality.[308] Traditionally marginalized social groups require data privacy in ways entrenched majorities often fail to recognize. As Mary Anne Franks has explained, "[a]ttentiveness to race, class, and gender is vital to understanding the true scope of the surveillance threat. Marginalized populations, especially those who experience the intersection of multiple forms of subordination, also often find themselves at the intersection of multiple forms of surveillance: high-tech and low-tech, virtual and physical."[309] And those forms of surveillance can be designed into new technologies. For example, surveillance apps, geosocial tracking, and other tools are becoming common weapons in intimate partner violence.[310] A fairness-in-design approach puts the onus on the designing company to consider how design will not just affect the ordinary consumer, but also marginalized consumers, many of whom have even less of an opportunity to protect themselves from privacy harms.[311]

---

306. *See* PASQUALE, *supra* note 44, at 3, 28–31, 34–36, 78–79.

307. Apple recently became the first American company worth $1 trillion. *See* Mark Gurman, *Apple Becomes First U.S. Company to Hit $1 Trillion Value*, BLOOMBERG (Aug. 2, 2018 11:57 AM), https://www.bloomberg.com/news/articles/2018-08-02/apple-becomes-first-u-s-company-to-hit-1-trillion-market-value [http://web.archive.org/web/20190330222838/https://www.bloomberg.com/news/articles/2018-08-02/apple-becomes-first-u-s-company-to-hit-1-trillion-market-value]. Moreover, on July 26, 2017, Facebook reported $9.3 billion in revenue for the second quarter of that year, up 45 percent from the same period in 2016. Profits rose to $3.9 billion, up 91 percent from the previous year. *See* Mike Isaac, *Facebook's Profit and Revenue Surge, Despite Company Predictions of a Slowdown*, N.Y. TIMES (July 26, 2017), https://www.nytimes.com/2017/07/26/technology/facebook-users-profit.html [https://perma.cc/62LT-RW7J].

308. *See, e.g.,* JUDITH W. DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY (1997) ("Protection of privacy enhances and ensures the freedom from such scrutiny, pressure to conform, and exploitation.").

309. Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 464 (2017).

310. *See, e.g.,* Rahul Chatterjee et al., *The Spyware Used in Intimate Partner Violence*, IPV TECH RES. (2018), https://www.ipvtechresearch.org/pubs/spyware.pdf [http://web.archive.org/web/20190510222447/https://www.ipvtechresearch.org/pubs/spyware.pdf] (presented at the 2018 IEEE Symposium on Security and Privacy).

311. This is especially true when predictive algorithms reflect data and human biases. *See, e.g.*, Julia Angwin et al., *supra* note 139.

*5. How?*

Privacy's law of design must also provide sufficient notice to users, allowing them to both distinguish compliance from malfeasance and practically enforce their right to a design process that considers their privacy from Day 1. Unfortunately, pathways to vindicating design rights have rarely been part of the privacy by design literature. Scholars either ignore it and focus on corporate ex ante obligations[312] or deputize regulators like the FTC, European DPAs, and state attorneys general as privacy enforcers.[313] Undoubtedly, regulators should be (and are) empowered to force technology companies to follow privacy's law of design. And, as Woodrow Hartzog has argued, the FTC is well-situated to consider manipulative and abusive design as part of its mandate to police "unfair and deceptive" business practices.[314] But saddling consumer safety regulators with the entire burden of enforcing privacy's law of design is risky. Both the FTC and European DPAs are overworked and lack the budgets and institutional capacities to address bad corporate behavior on their own.[315] Users must be able to validate their own design rights through a private right of action built into a privacy by design statute. Products liability offers several insightful lessons to make that a reality.

Privacy plaintiffs have struggled to prove particularized harm because courts have routinely found their claims of injury—risk of future harm, preventative measures to guard against identity theft, and anxiety about data security[316]—too speculative.[317] In so doing, judges are requiring plaintiffs to demonstrate harms as

312. Ann Cavoukian's PbD, for example, makes no mention of privacy by design as a consumer right capable of validation through the courts. *See* CAVOUKIAN, *supra* note 9.

313. *See, e.g.*, HARTZOG, *supra* note 4, at 138–42 (describing how the FTC has already litigated cases involving deceptive design tactics).

314. *Id.*; *see also* Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785 (2015) (arguing that the FTC has the capacity to regulate the deceptive designs of robots).

315. *See* Solove & Hartzog, *supra* note 169, at 600 (stating that the FTC averages 10 enforcement actions per year); *see also* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, DATA PROTECTION IN THE EUROPEAN UNION: THE ROLE OF NATIONAL DATA PROTECTION AUTHORITIES 42 (2010), *available at* http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf [https://perma.cc/JS52-NE4R] ("In many Member States, DPAs are not in a position to carry out the entirety of their tasks because of the limited economic and human resources available to them. This is the case in Austria, Bulgaria, Romania, Cyprus, France, Greece, Italy, Latvia, Netherlands, Portugal and Slovakia."); Julia Powles & Enrique Chaparro, *How Google Determined Our Right to Be Forgotten*, GUARDIAN (Feb. 18, 2015, 2:30 EST), http://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search [https://perma.cc/NU7B-UADQ] ("Most of Europe's 31 national data protection authorities are cumbersome, under-resourced bureaucracies issuing occasional, random fines and reacting when a court occasionally clarifies the law.").

316. For a taxonomy of alleged data breach harms and an insightful discussion of how courts have conceptualized those harms, see Solove & Citron, *supra* note 5, at 749–54. "The overarching concern is that risk and anxiety are speculative, subjective and, worse, susceptible to manipulation by attorneys who desire to manufacture injuries out of a data breach." *Id.* at 774.

317. *See, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (plaintiffs failed to show that ongoing government surveillance affected their work in any way); Reilly v. Ceridian Corp., 664 F.3d 38, 40, 43 (3d Cir. 2011) (increased risk of identity theft is too speculative); *In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 326–27 (E.D.N.Y. 2005) (stating that "loss of privacy" is not a

if an invasion of privacy is no different than getting hit by a car, a fist, or falling debris. But the two injuries are quite different and in ways that the law has long understood. Privacy plaintiffs should not be crammed into a physical harm box; other types of harms are recognized at common law. The tort of assault, where the shibboleth of liability is fear, not physical or pecuniary harm, is more than 600 years old.[318] Intentional infliction of emotional distress (IIED) compensates for emotional harm as well.[319] Daniel Solove and Danielle Citron have argued that an objectively reasonable person standard can determine the reasonable cost of ensuring against the intangible, though no less real, risks associated with data breaches, thus creating a cognizable injury.[320] Failing to consider privacy during design creates technology products that put our privacy at risk.[321] As Ryan Calo has argued, this kind of harm is analytically distinct from the category of harm cognizable in torts like assault and IIED.[322] It also resembles the intangible harms Solove and Citron discussed in the data breach context.[323] Therefore, assessing the reasonable costs of injury prevention could operate in design litigation as well.

As a statute, privacy's design law can impose statutory damages that obviate the need for any user to identify specific harm, much like the GDPR. Products liability justifies this. Products liability recognizes that in addition to a specific injury caused by a faulty product, defective designs on the market carry social costs: they can cause harm to many people at the same time, burden ordinary individuals with outrageous recovery costs,[324] and allow predatory manufacturers to gain a competitive advantage by shortcutting safety.[325] These social costs are one of the

---

sufficiently concrete injury to survive a motion to dismiss). *But see* Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388 (6th Cir. 2016) (recognizing that increased risk of identity theft and reasonably incurred mitigation costs to avoid future harm were sufficient for standing because hackers allegedly had stolen plaintiffs' information and the defendant offered free credit monitoring services to help consumers mitigate danger). Recently, in *Spokeo v. Robbins*, 136 S. Ct. 1540, 1549 (2016), the Supreme Court held that a plaintiff had to show "concrete" injury for Article III standing, but that "intangible harm" and "risk" could suffice if it bore a "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit."

318. I de S et Ux. v. W de S, Y.B. 22 Edw. 3, fol. 99, pl. 60 (1348).

319. *See* Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 140–58 (1992) (discussing various examples included IIED).

320. *See* Solove & Citron, *supra* note 15, at 774.

321. HARTZOG, *supra* note 4, at 1–21 (discussing the pervasive role of design and its manipulative potential to take away our data).

322. Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 363 (2014).

323. *See generally* Solove & Citron, *supra* note 15 (discussing how data breaches cause increased feelings of risk, anxiety, and emotional harm).

324. *See* Ellen Wertheimer, *Punitive Damages and Strict Products Liability: An Essay in Oxymoron*, 39 VILL. L. REV. 505, 506 n.4 (1994) ("Design defects thus threaten equally all those who come into contact with the particular product, and therefore bring with them the potential for widespread injury and liability."); *see also* CALABRESI, *supra* note 43, at 24, 70, 72 (arguing for shifting social costs of accidents from individual victims to those more capable of handling them).

325. *See* Michael Rustad, *In Defense of Punitive Damages in Products Liability: Testing Tort Anecdotes with Empirical Data*, 78 IOWA L. REV. 1, 86 (1992).

reasons why products liability permits punitive damages in some circumstances.[326] Therefore, significant statutory damages can be imposed to deter technology companies from evading their design responsibilities to society.

*6. Privacy's Design Law Summary*

Tying these who, what, when, why, and how strands together gives us a vision of privacy's law of design. Under this model, a privacy by design statute would require anyone who develops and markets products that collect and process user data[327] to, when conceiving, designing, developing, and using those products,[328] balance the products' benefits to consumers against their foreseeable privacy risks and only place in commerce those products that achieve reasonably similar consumer benefit with the least privacy risk.[329] This duty includes the responsibility to inform users, throughout the lifecycle of products, of how the products collect and process data and of all foreseeable privacy risks in a manner that adequately and comprehensibly conveys those risks to an ordinary user.[330]

This approach to privacy's law of design has several advantages. First, it reflects both the social nature of design and the importance of fairly allocating responsibility for protecting personal privacy. Current privacy law, based on the myth of control and extracted consent,[331] forces unprepared users to bear the burden of protecting their information in the face of manipulative design. As Woodrow Hartzog has written, even when platforms give control to users through various options, privacy centers, and click boxes, consent "can act to shift the burden of responsibility for protecting privacy to people who are less equipped to handle it . . . . Control . . . comes [with] a practical *obligation*" to exercise that control.[332] When users do not, as primed by design,[333] technology companies translate our "inaction as acquiescence."[334] This formulation of privacy by design is consciously meant to tip the balance back toward corporate responsibility for privacy.

---

326. *See, e.g.*, Acosta v. Honda Motor Co., 717 F.2d 828, 839 (3d Cir. 1983) (punitive damages may be awarded for "outrageous conduct"); Palmer v. A.H. Robins Co., 684 P.2d 187, 227–28 (Colo. 1984) (punitive damages intrauterine device case); Sturm, Ruger & Co. v. Day, 594 P.2d 38, 46–47 (Alaska 1979) (allowing punitive damages where gun manufacturer knew of defective design yet still put the revolver in commerce), *modified*, 615 P.2d 204 (Alaska 1980), *cert. denied*, 454 U.S. 894 (1981); Rinker v. Ford Motor Co., 567 S.W.2d 655, 668 (Mo. Ct. App. 1978) (stating that "there is no fundamental reason for excluding products liability cases from the cases in which punitive damages may be recovered"); *see id.* at 67–69.

327. *See supra* Part II.C.1.

328. *See supra* Part II.C.2.

329. *See supra* Part II.C.3.

330. *See supra* Part II.C.3.d.

331. *See* HARTZOG, *supra* note 4, at 62–67.

332. *See* Woodrow Hartzog, *Privacy and the Dark Side of Control*, IAI NEWS (Sept. 4, 2017), https://iainews.iai.tv/articles/privacy-the-dark-side-of-control-auid-882 [https://perma.cc/J8DH-F5YQ].

333. *See* NOR. CONSUMER COUNCIL, *supra* note 293, at 12–39.

334. *See* HARTZOG, *supra* note 4, at 66.

Second, this model of privacy's design law is clear, yet flexible. It provides a governing structure and some level of certainty as to what the law requires without mandating specific designs. The only specific limit it places on designers is the requirement to choose a reasonably alternative privacy-protective design when one exists. Otherwise, design law guarantees that privacy will have a fair shake during design. And for judges and regulators seeking to interpret design law's requirement, a products liability model gives them the tools to answer vanguard questions as they come up. It also gives users clear guideposts for pursuing their design rights through regulators like the FTC or directly through the courts.

Third, despite its flexibility, it nevertheless places limits on predatory, opportunistic corporate behavior. Absent a requirement to consider privacy during design and to market only those products that achieve similar goals with privacy-protecting tools, many dangerous technologies are making their way to unsuspecting consumers. For example, there is no reason why a smartphone flashlight app needs to collect terabytes of user data and share it with advertisers.[335] Nor should an app track us after we delete it.[336] Privacy's design law would restrict this kind of deception.

That said, some might object to this formulation of privacy's law of design as arbitrary; that is, ask why products liability? Although it is true that other analogies besides products liability—consumer protection, for example[337]—could bring clarity to privacy by design, products liability for design defects makes the most sense. As I argued above, privacy by design and products liability developed in similar socioeconomic circumstances to address similar problems of design. They both focus on the way new technologies are built and how they affect real people. That other options exist does not detract from the validity of the products liability analogy.

This proposal may also trouble those who feel that judges, juries, and regulators do not belong meddling in the design process. Indeed, if privacy's law of design requires technology companies to demonstrate that products sold to users did not have a reasonable alternative privacy-protective design, the judgment of courts or regulators could supplant the judgment of designers themselves. Such concerns are overblown. Products liability for design defects has been around for decades, and overtime, judges have developed flexible standards for determining what is safe and reasonable. At no time have judges replaced designers. For example, courts decided that building a car with seatbelts capable of inflicting injury during an accident is unreasonably dangerous,[338] but those judges never designed new seatbelts themselves. Rather, they set out boundaries, made value judgments, and

335. *See* Robert McMillan, *The Hidden Privacy Threat Of … Flashlight Apps?*, WIRED (Oct. 20, 2014 2:30 AM), https://www.wired.com/2014/10/iphone-apps/ [https://perma.cc/ASQ9-YHXN].

336. *See, e.g.*, Lily Hay Newman, *supra* note 232.

337. *See* HARTZOG, *supra* note 4, at 123–26.

338. *See, e.g.*, Garrett v. Ford, 684 F. Supp. 407 (D. Md. 1987).

represented society's interests in designing safe cars. That said, if privacy's design law shines some light on the "black box" of technology design, that might be a good thing. Technology companies today reap enormous benefit from zealously guarding their algorithmic secrets. And yet, as Frank Pasquale has shown, opaque data collection tools have the potential to influence and manipulate human behavior.[339] They can discriminate,[340] and cause substantial harm to real people.[341] Technology companies are even using the opacity of their data products market technologies without taking responsibility if something goes wrong.[342] Peering into the black box to ensure social justice concerns like safety and privacy are at least part of the design process is long overdue.[343]

A third related objection is that this formulation of privacy's design law would stifle technological innovation. Again, I disagree. Despite the prevalence of the argument that regulation stunts innovation, there is very little evidence in support.[344] Indeed, creativity and innovative thinking often thrive within constraint.[345] And even if that were not the case, I am unwilling to surrender to the intellectual hegemony of innovation. Sometimes, there are other things that matter more, including fairness and protecting users from predatory, data-hungry design.

## CONCLUSION

Privacy by design today is a lot of hype with very little substance. Although it has enormous potential to reset the power imbalance between data collectors and users, it suffers from too much ambiguity. It has yet to define its who, what, when, why, and how. And without that, it cannot transition from a buzzword to a legal mandate.

---

339. *See* PASQUALE, *supra* note 44, at 18.

340. *See, e.g.*, Julia Angwin et al., *supra* note 139.

341. *See* Sidney Fussell, *AI Professor Details Real-World Dangers of Algorithm Bias*, GIZMODO (Dec. 8, 2017 5:00 PM), https://gizmodo.com/microsoft-researcher-details-real-world-dangers-of-algo-1821129334 [https://perma.cc/JGX9-8JV7] (discussing several harms to users from black box algorithms).

342. *See* Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CAL. L. REV. 721, 729 (2007) (noting that DNA typing "weathered a series of challenges related to the reluctance of private companies to divulge claimed proprietary secrets"); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1356–71 (2018) (discussing several cases in which courts have denied motions to disclose how secret algorithms impacted criminal justice).

343. *See* PASQUALE, *supra* note 44, at 189–220 (calling for an "intelligible society," where we can understand how data inputs generate the effects algorithms have on us).

344. *See* Robert Atkinson & Les Garner, *Regulation as Industrial Policy: A Case Study of the U.S. Auto Industry*, 1 ECON. DEV. Q. 358 (1987) (finding regulation had a positive impact on innovation in the auto industry); Richard Newell, Adam Jaffe & Robert Stavins, *The Induced Innovation Hypothesis and Energy-Saving Technological Change*, 114 Q.J. ECON. 941 (1999) (finding innovation as a result of imposition of energy conservation standards); Katherine J. Strandburg & Yafit Lev-Aretz, *Better Together: Privacy Regulation and Innovation Policy* (forthcoming 2019) (demonstrating that little evidence exists for the argument that privacy regulation will stifle technology innovation).

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

This Article set out to facilitate that transition by answering privacy by design's open legal questions. It began by laying out those questions, and it relied on science and technology and sociology scholarship to identify the built-in complexities and assumptions of each. With this background, and drawing from the law of products liability for design defects, the Article then offered a new vision for what privacy by design should mean in practice. And that analogy makes sense. Both doctrines emerged in similar socioeconomic contexts to answer similar questions. Both share the similar goals of creating safer products and protecting consumers from harm. Both recognize that the best way to do that is to have an impact on ex ante design rather than to wait for something to go wrong. Both want to be sufficiently flexible to balance the need for regulation with breathing room for dynamic technological change.

Privacy by design has been around for over a decade. But as it matures so must its scholarship. Privacy studies on design need to shift from ideas to substance if design law's impact is going to match its potential. Future scholarship must apply this model of privacy's law of design to specific questions as they come up. It must also be tested to determine if this, or any other, vision is being operationalized on the ground, at the technology companies designing the digital products we use every day and among data protection regulators and policymakers. This research can take the form of ethnographic interviews and controlled experimentation. Policymaking about privacy by design should not only consider the paradigm proposed in this Article, but it should focus on the purposes and goals privacy by design is meant to achieve. In this Article, I focused on protecting consumers, alleviating power imbalances, removing manipulative and privacy—invasive technologies from the market, and, above all—fairness. Privacy's law of design, whatever form it takes, can be successful when it embraces these values.