PRIVACY, NOTICE, AND DESIGN

Ari Ezra Waldman*

CITE AS: 21 STAN. TECH. L. REV. 129 (2018)

ABSTRACT

Design configures our relationship with a space, whether offline or online. In particular, the design of built online environments can constrain our ability to understand and respond to websites' data use practices or it can enhance agency by giving us control over information. This Article is the first comprehensive theoretical and empirical approach to the design of privacy policies.

Privacy policies today do not convey information in a way understandable to most internet users. This is because they are created without the needs of real people in mind. They are written by lawyers and for lawyers, and they ignore the way most of us make disclosure decisions online. They also ignore the effects of design, aesthetics, and presentation on our decision-making. This Article argues that in addition to focusing on content, privacy regulators must also consider the ways that privacy policy design—the artistic and structural choices that frame and present a company's privacy terms to the public—can manipulate or coerce users into making risky privacy choices. I present empirical evidence of the designs currently employed by privacy policies and the effect of different designs on user choices. This research shows that supposedly "user-friendly" designs are not always boons to consumers; design strategies can manipulate users into making bad choices just as easily as they can enhance transparency. This suggests that recommending "user-friendly" design is not enough. Rather, privacy regulators, including the Federal Trade Commission and state attorneys general and legislators, must ensure that privacy policies, and the websites that display them, are designed in ways that enhance transparency.

* Associate Professor of Law; Director, Innovation Center for Law and Technology, New York Law School; Affiliate Scholar, Princeton University Center for Information Technology Policy. Ph.D., Columbia University; J.D., Harvard Law School. Versions of this paper were workshopped or presented at the Sixth Annual Internet Law Works-in-Progress Conference on March 5, 2016, as part of Whittier Law School's Distinguished Speaker on Privacy Law lecture on March 17, 2016, at the New York Law School Faculty Colloquium on April 12, 2016, and at the Ninth Annual Privacy Law Scholars Conference on June 2, 2016. Special thanks go to Alessandro Acquisti, Danielle Citron, Julie Cohen, Joshua Fairfield, Woodrow Hartzog, Chris Hoofnagle, Bill McGeveren, and Dan Solove. I would also like to thank all conference and symposia participants for their helpful comments, particularly David Ardia, Tamara Belinfanti, Jody Blanke, Robert Blecker, Jill Bronfman, Ignacio Cofone, Mary Culnan, Stacey-Ann Elvy, Matt Hintze, Bill LaPiana, Art Leonard, Rebecca Lipman, Howard Meyers, Joel Reidenberg, Betsy Rosenblatt, Ira Rubinstein, Ross Sandler, Jacob Sherkow, Heather Shoenberger, David Spatt, Berin Szoka, Ann Thomas, Debra Waldman, and Andrew Woods. The New York Law School students participating in the Data Privacy Project contributed greatly to this project: Yusef Abutouq, Ashley Babrisky, Catherine Ball, Emily Holt, Jerry Jakubovic, Ashley Malisa, April Pryatt, Ke Wei, Karyn Wilson, and Anna Zabotina.

TABLE OF CONTENTS

I. INTRODUCTION 131
II. NOTICE AND CHOICE TODAY 134
A. Privacy Policies On the Ground 136
B. Privacy Policies on the Books 139
1. Privacy Principles 139
2. The FTC Focuses on Substance 140
3. Federal and State Laws and Privacy Policy Content 144
a. Federal Laws 145
b. State Laws 146
4. Moving Beyond Content 148
C. Myths About Users and Design 150
III. CONSTRAINED BY DESIGN 152
A. Configuring and Constraining the User 153
1. Fine Art 155
2. Architecture 158
3. *Interior Design* 160
4. Urban Design 161
B. The Design of Privacy Policies 163
1. Research Questions 164
2. Research Methodology 164
3. Results 169
4. Discussion 172
IV. EFFECTIVE NOTICE DESIGN 174
A. Considering Design in Privacy Law on the Books 175
B. Considering Design on the Ground 178
C. Responses to Objections 181
V. CONCLUSION 183

I. INTRODUCTION

Privacy policies are confusing,[1] inconspicuous,[2] and inscrutable.[3] A crucial aspect of the ability of internet users to understand those notices has received less attention—namely, their design. This article helps to fill that void with a theoretical and empirical approach to notice design, aesthetics, and presentation.

Privacy policies are essential to the notice-and-choice approach to online privacy in the United States.[4] They are supposed to tell us what information platforms collect, how and for what purpose they collect it, and with whom they share it (notice). We then have the opportunity to opt out (choice).[5] In practice, they are ineffective: no one reads privacy policies[6] in part because they are long[7] and difficult to understand.[8].

---

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

2. Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 254, 266-67 (2011).

3. Lorrie Cranor's Platform for Privacy Preferences used machine-readable privacy policies to allow consumers to easily compare data use practices before making disclosure decisions. *See* Lorrie Faith Cranor & Joseph Reagle, *Designing a Social Protocol: Lessons Learned From the Platform for Privacy Preferences Project*, *in* TELEPHONY, THE INTERNET, AND THE MEDIA 215 (Jeffrey K. MacKie-Mason & David Waterman eds., 1998); Mark S. Ackerman, Lorrie Faith Cranor & Joseph Reagle, *Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences*, ACM CONFERENCE ON ELECTRONIC COMMERCE 1 (1999).

4. I leave to one side the related discussion of whether a notice and choice approach is the best way to protect online privacy. This Article presumes the existence of a notice and choice regime and challenges our ability to provide adequate notice and choice while ignoring design. That said, the critiques of notice and choice are too voluminous to list here. For a good summary of some of the major critiques, please see Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 485, 490-696 (2015) [hereinafter *Privacy Harms*].

5. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 592 (2014).

6. *See, e.g.*, George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15, 15 (2004); Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services* (forthcoming), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465 [https://perma.cc/D7M2-JWSW].

7. 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 TELECOMM. & 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).

8. *See* Mark A. Graber, Donna M. D'Alessandro & Jill Johnson-West, *Reading Level*

Even privacy experts find them misleading.[9]

These are failures of communication and conceptualization. Privacy policies today do not convey information in a way that reflects the embodied experience of internet users because they are designed without the needs of real people in mind. They are written by lawyers and for lawyers. Privacy law, for the most part, has exacerbated the problem. It primarily mandates the content of notice and ignores how that content is conveyed: statutes insist that policies include a what-when-how of data use, and regulatory action is often triggered when companies violate the substantive terms of their policies.[10] Law has generally ignored privacy policy design.

But most users are not lawyers. Nor are any of us capable of making perfectly rational disclosure decisions based on a 9,000-word privacy policy.[11] Rather, we are embodied, situated users who make choices in the moment based on context.[12] Proposals that are limited to making terms clearer[13] or locating policies in more noticeable places[14] are fine starts: they recognize that, at a minimum, content is not king. Still, these reforms matter little if we are manipulated into breezing by privacy policies in the first place. Our failure to stop and read, let alone understand and choose, suggests that forces exogenous to the substance and language of the policies themselves are constraining our behavior. One of those forces is design. Like with any built environment, we are constrained by the design of the digital spaces that frame platforms' privacy notices.

This paper argues that privacy policy design—the artistic and structural choices that frame and present a company's data use disclosures to the public on a website—constrains our ability to interact with, understand, and translate that policy into action. As scholars have argued, design configures users, limiting our freedom in ways predetermined by

---

of Privacy Policies on Internet Health Web Sites, 51 J. FAM. PRAC. 642, 642 (2002).

9. Reidenberg et al., *supra* note 1, at 87-88.

10. *See* Solove & Hartzog, *supra* note 5, at 627-38. Granted, regulators and state laws often require or recommend that policies be understandable and conspicuously posted. *See, e.g.*, Cal. Bus. & Prof. Code § 22575(b) (requiring clear and conspicuous hyperlink in the privacy policy to online description of operator's protocol); Decision and Order at 2, Sony BMG Music Entm't, F.T.C. File No. 062 3019, No. C-4195 (June 29, 2007), https://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019do070629.pdf [https://perma.cc/BKR7-LSEX]. However, neither the FTC nor a single state attorney general has moved against a company purely for using legal jargon or hiding a policy under several sub-navigation pages. The lion's share of enforcement focuses on content.

11. Leslie K. John, Alessandro Acquisti & George Loewenstein, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. CONSUMER RES. 858, 864 (2011) (arguing online disclosure decisions are not rational).

12. *See* Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUMB. L. REV. 210, 225-27 (2007) [hereinafter Cohen, *Cyberspace*].

13. Reidenberg et al., *supra* note 1, at 87-88.

14. Tsai et al., *supra* note 2.

the designer.[15] It achieves this by leveraging the same principles of art, design, and urban planning long used by painters, interior designers, and politicians to manipulate people's eyes and movements, shuttle individuals through a space, and evoke emotional or behavioral responses.[16] Furthermore, design is not neutral. Design carries with it normative choices that reflect whether a space is welcoming or hostile. In much the same way that the design of public spaces can influence behavior,[17] website design can discourage us from reading privacy notices, make them transparent, or coerce us into mismanaging our privacy contrary to our true intentions.

As reported herein, a canvas of the privacy notices of 191 popular websites shows that privacy policies today are not designed for ordinary users. I would like to go a step further: policies today are paradigmatic examples of "unpleasant design," or design that deters certain behaviors by exercising a form of social control against actors.[18] By designing policies so no reasonable user could ever read, process, and understand them,[19] drafters fail to provide adequate notice. This tactic alone is manipulative and unfair, arguably warranting regulation. But even seemingly user-friendly design can be manipulative: a survey of 564 internet users reveals that privacy policy design, perhaps more than content, has a significant impact on a user's willingness to trust or do business with a website; this is true even when user-friendly designs present highly invasive data use practices.

The extent to which the layout, design, and structure of a privacy policy can manipulate us into sharing personal data is largely undocumented. This Article attempts to fill that gap, proceeding as follows: Part II discusses notice and choice today. It reports on the results of an informal canvas of current policies and argues that these notices are

---

15. *See, e.g.*, LUCY A. SUCHMAN, HUMAN-MACHINE RECONFIGURATIONS 186-92, 257-84, 187-93 (2d ed. 2007); 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). *See also* Cohen, *Cyberspace*, *supra* note 12, at 210, 221, 225, 233-36.

16. *See infra* Part II.A; *see also* Neal 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").

17. *See generally* GORDAN SAVICIC & SELENA SAVIC, UNPLEASANT DESIGN (2013) (collecting and analyzing myriad common examples of how the design of mostly public spaces can deter antisocial behavior, from uncomfortable benches and window sill spikes that discourage people from sitting or lying down to unflattering light that deters everything from congregation to intravenous drug use).

18. This is not my phrase. *See id.*; *see also* Roman Mars, *Unpleasant Design & Hostile Urban Architecture*, 99 PERCENT INVISIBLE (July 5, 2016), http://99percentinvisible.org/episode/unpleasant-design-hostile-urban-architecture/ [https://perma.cc/FN39-E4ZV].

19. Lorrie Cranor found that a user would need an average of 244 hours per year to read the privacy policy of every website she visited. *See* Cranor, *supra* note 7. That is about 54 billion hours per year. *See* McDonald & Cranor, *supra* note 7.

drafted by either ignoring or conceptualizing users as radically disembodied, perfectly rational actors. This Part also shows how privacy laws and litigation have generally overlooked notice design and focused primarily on policy content. I argue that this oversight is based on the fundamental misconception that users make perfectly rational disclosure decisions online.

Part III relies on socio-legal scholarship on configuring the user and the social construction of technology to challenge that conception of the user. From this social science foundation, this section argues that like works of art, the underlying design structure of privacy policies can constrain user choices. This Part concludes by discussing and analyzing the results of an empirical study on the impact of privacy policy design on user disclosure decisions.

Part IV outlines the proposals based on this research. With respect to privacy law, design's role in constraining users suggests that privacy regulators should consider the effects of privacy policy design on user choices when assessing adequate notice and choice and deceptive business practices. Because policy design can manipulate users into handing over personal information, policy design requirements, including mandating a notice designed specifically to convey information to ordinary users, should be included in state and federal statutes that mandate privacy policies. The FTC should also investigate internet companies that design their privacy policies to deceive users. With respect to the practical implementation of notice and choice, this research recommends several strategies for online platforms, including increasing collaboration between privacy counsel and technologists and committing to embedding privacy protection into the corporate ethos. After addressing several anticipated objections, the Article concludes with avenues for future research.

II. NOTICE AND CHOICE TODAY

Privacy policies have been around since the 1990s. It was then that widespread internet use created popular concerns about privacy and led to several privacy-related litigations. At the time, however, online data was collected in a regulatory void: there were no generally applicable laws that limited what websites could do with our data and no recourse for those who felt their data had been misused. Plaintiffs tried privacy torts to no avail.[20] Frustrated users even turned to statutes originally

20. There are four so-called "privacy torts," as defined by William Prosser: intrusion upon seclusion, public disclosure of private facts, false light, and appropriation of name or likeness. *See* William Prosser, *Privacy*, 48 CAL. L. REV. 383, 388-389 (1960). At the time, Prosser served as the Reporter for the Second Restatement of Torts. His review of the case law and his decision to include these (and only these) torts helped shape privacy tort law ever since. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of*

intended to regulate wiretapping.[21] Again, they failed.

Privacy policies have since become ubiquitous, developing first as industry's way to stave off regulation[22] and spreading further under state and federal mandates.[23] At the core of this regime, even in its earliest iterations, was the notion that websites that collect data should tell us what they do with our information so we can make informed disclosure choices. That sounds reasonable. For some time, however, privacy policies have been under attack. Critics argue that it is impractical for ordinary users to read long and complex privacy notices littered with legal terms,[24] and that we should instead rely on visceral forms of notice[25] or a website's user-controlled privacy settings to set platform privacy obligations.[26] These critiques and proposals have considerable merit. But ever since the earliest iterations of privacy norms, providing some form of notice has been standard. It is safe to assume that any reform of notice and choice would not eliminate the privacy policy any time soon. It is, therefore, worth analyzing how internet platforms convey notice to their users.

There is voluminous scholarship on privacy notices and their faults. Less work has been done on their design. In this section, I describe what notice and choice looks like today, both in practice and theory. Using a canvas of privacy policies from 191 popular websites as a guide, I show that most privacy notices are essentially legal documents written for lawyers; design is either ignored or not geared toward user comprehension. I then demonstrate how privacy law on the books has contributed to this design neglect by focusing the majority of its attention on policy content. This focus plays out at all levels of privacy law: norms, statutes,

---

Confidentiality, 96 GEO. L. J. 123, 148-56 (2007); *see also* Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995) (selling cardholders' names and other data to merchants did not violate any privacy tort); Solove & Hartzog, *supra* note 5, at 590-92.

21. *In re* DoubleClick, Inc. Privacy Litigation, 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001) (holding that use of cookies was not a violation of the Electronic Communication Privacy Act). ECPA was designed to regulate wiretapping, protect against the interception of electronic communications, and preventing spying. *See, e.g.*, Patricia Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 310 (2011); 131 CONG. REC. 24, 365-66 (1985) (statement of Sen. Leahy); *id*. at 24, 396 (1985) (statement of Rep. Kastenmeier).

22. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 593 (2007) ("Online privacy policies have appeared . . . as voluntary measures by websites"); *see also* Solove & Hartzog, *supra* note 5, at 593-94; Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046-47 (2000) (noting that an FTC threat for greater regulation resulted in a substantial increase in the number of websites offering privacy policies).

23. *See discussion infra* Parts II.B.3, II.B.4.

24. *See* Cranor, *supra* note 7; McDonald & Cranor, *supra* note 7.

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

26. Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 TEMP. L. REV. 891, 893-96 (2009).

and regulatory enforcement. Finally, I argue that this focus on content comes from an erroneous conceptualization of users as purely rational decision-makers.

A. Privacy Policies On the Ground

Intentionally or not, privacy policies are imbued with an underlying structure that affects a user's ability to understand the substantive disclosures within. Most of those effects are negative: their designs make their policies difficult to read. This was apparent from an informal canvas we conducted of 191 online privacy policies.[27] We identified several design-related characteristics, including aesthetics (text color, use of different colors, number of paragraphs, number of pages when printed out, number of words, number of sections, length of each section in paragraphs and words, font size, headings color, headings size, contrast between text color and background, use of charts or icons), notification timing, the existence of privacy "centers" and Frequently Asked Questions, and the use of layered notices with a short, simple summary on top, and coded each policy for each characteristic. Each researcher also described and justified his or her impressions on policy design, generally, reflecting on the policy as a whole beyond the particular metrics above.

Although most privacy policies were displayed in black text on white backgrounds, 35% were written in grey on white. Half of those greys were light-to-medium (40%-60% opaque). The median font size was 11; nearly 20% were written in the median size (n=37), which is roughly the same number of policies that were written in size 7 or 8. All the policies reviewed included headings and subheadings for its sections, but nearly half of those headings were written in the same font size and color. Active links are frequently, though not always, differentiated from the text of the policy with a different color (usually a blue).

---

27. The raw data is available online at the Data Privacy Project, New York Law School, at http://www.nyls.edu/innovation-center-for-law-and-technology/institutes-and-programs/data-privacy-project/ [https://perma.cc/LAK7-X8CX]. The sample is not meant to be representative of all privacy policies. Rather, the goal was to get a taste of the privacy policies of some of the most frequently visited websites and to provide a background or control state for the privacy policy design study discussed *infra* Part III.B. I recruited ten outstanding researchers from my Spring, 2016, Information Privacy Law class at New York Law School: Yusef Abutouq, Ashley Babrisky, Catherine Ball, Emily Holt, Jerry Jakubovic, Ashley Malisa, April Pryatt, Ke Wei, Karyn Wilson, and Anna Zabotina. I asked each researcher to select 20 websites that they visit frequently, regularly, or somewhat regularly. I imposed two limitations. First, no more than two websites could be of the same type—namely, no more than two news sites, two social networking sites, two e-commerce sites, two television networks, and so on. Second, researchers could not repeat websites. The remaining columns asked researchers a series of content- and design-related questions about the policies, the analysis of the answers to which are discussed here. Nine websites were excluded from the final analysis because they were incompletely coded.

The longest policy, from Caesar's Entertainment, was 9,965 words and took 20 seconds of continuous scrolling to reach the end.[28] The online technology magazine, "How to Geek," had the shortest privacy policy, at 248 words.[29] The mean policy length was 2,716 words. Approximately 82% of policies' text was single spaced, with the remaining 18% written with larger line spacing up to 1.5. The vast majority (91%) of privacy policies reviewed were written in a single column. Most, however, had ample white space on each side.

Only 9 out of 191 policies had readily noticeable opt-out buttons, where "readily noticeable" is easy to see at first glance.[30] After some additional research, it was clear that of all the opt-out procedures, more than half of them only allowed users to opt out of receiving marketing emails rather than general data tracking. Twenty-three policies required users to send an email or some form of communication to the company in order to opt out of certain data gathering practices; five policies required postal mail. Only four policies included charts providing clear, easy to understand information. One hundred fifty-seven policies, or 82%, did not include a single graphic or icon. Of the remaining 34 policies, the only icons used on 32 of them were either the company's logo at the top or the TRUSTe certification icon. Just two policies used images, icons, and other graphics as part of the privacy policy.[31]

Fewer than 20% of the websites reviewed included pop-up notifications about cookie collection. About 43% used bulleted lists at least once within the policy, but 87% of those used a smaller font size, smaller line spacing, and smaller kerning for the text. Only one website in the sample — Facebook — had anything akin to a "privacy center" where users could manipulate and make changes to their privacy settings.[32] Even these settings were designed to mislead users into thinking they had

28. Try it. Twenty seconds is a long time. *See Privacy*, CAESAR'S CORPORATE (June 29, 2016), http://caesarscorporate.com/privacy/?_ga=1.200037294.1872875718.1467234380 [https://perma.cc/SM3T-9BLB].

29. It was also the funniest privacy policy we saw. *See* HOW TO GEEK, (June 29, 2016), http://www.howtogeek.com/privacy-policy/ [https://perma.cc/H4S6-HLG3] ("We will never sell your email address to any third parties, ever. If we ever sell your email address to anybody, we agree that you can beat us with a large metal object. The object must be at least 4 feet long and weigh more than 20lbs.").

30. The definition of the word "noticeable" already encompasses ease. *Noticeable*, MERRIAM-WEBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/noticeable [https://perma.cc/XG9G-LE63].

31. FitBit, the wearable activity tracker, is one of them. FitBit has designed a user-friendly icon-rich explanation of its data use practices specifically geared toward average users. The company also provides a link to its complete privacy policy, the substance of which conforms to the graphical version. *See Let's Talk About Privacy*, *Publicly*, FITBIT, https://www.fitbit.com/legal/privacy [https://perma.cc/UR3E-KPUS].

32. *See Privacy Settings and Tools*, FACEBOOK, https://www.facebook.com/settings/?%20tab=privacy [https://perma.cc/4A5P-QJG3].

control over their data on the platform.[33]

From this review, it seems that today's privacy policies are not designed with readability, comprehension, and access in mind. Long documents written in difficult language are even harder to understand when presented in small font sizes with letters and lines smashed together. Headings and subheadings, many of which are in the same font, size, and color as the remaining text, are ineffectual. As a result, it is possible that the design of privacy notices today encourages users to give up before they even start to read.[34]

This review of privacy policies on the ground raises three questions. First, what effect, if any, does the design of privacy policies today have on users' decisions to trust or do business with a website?[35] That question is part of the privacy policy survey discussed in Part III. As we shall see, the evidence suggests that it has a significant effect: discouraging and confusing users.

Second, if user trust is so important to data-driven businesses, why would platforms design their privacy policies like this? There are two possible responses to this question. First, platforms may not be designing privacy policies at all; design is not the chief concern of the lawyers involved in a policy's development. Those I have spoken to either disclaim any significant involvement in policy design[36] or stop at recommending that policies be clear and readable.[37] Though regrettable, this

33. Complaint at 4-7, In the Matter of Facebook, Inc., FTC File No. 0923184, No. C-4365 (July 27, 2012), http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf [http://perma.cc/AJQ7-JX34] [hereinafter Facebook Complaint].

34. The privacy policy design survey, the results of which are discussed *infra* Part III.B, tests that hypothesis.

35. Trust is an essential part of a user's willingness to disclose information or do business with a website. *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) (noting that protecting privacy can build trust between online platforms and consumers); Ari Ezra Waldman, *Privacy, Sharing, and Trust*: *The Facebook Study*, 67 CASE W. RES. L. REV. 193 (2016) (describing how users' decisions to share personal information on social networks or with third parties advertising on social networks depend on the decisions of others on the network who they trust); *see also* Timothy Morey, Theodore Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust [https://perma.cc/B3RX-RJ7D].

36. Presented only briefly herein, the results of an ethnographic study of technologists and privacy attorneys on the design of privacy policies are discussed in forthcoming scholarship. *See* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUSTON L. REV. __ (forthcoming 2018). Of the attorneys interviewed, most stated that they are not involved at all in what the policy looks like on a client's website. Others stated that they have, at times, made recommendations. At least fourteen attorneys stated that they and their clients prioritized readability and clarity. All attorneys noted that they considered privacy policies to be "legal documents."

37. *See, e.g.*, Telephone Interview with Attorney at Technology Law Firm (Mar. 26, 2016) (notes on file with author).

explanation speaks to an oversight, not deception. A second, darker explanation is that privacy policies today are purposely unpleasant to look at, discouraging us from actually learning about what websites do with our data.[38] Further research is needed to determine which, if either, explanation is correct.

Either way, we are left with a third question: How did notice get like this? Privacy law is one significant factor. In the following section, I show how laws on the books have generally ignored the impact of design on disclosure decisions, focusing instead on privacy policy content. Therefore, it has failed to generate and embed notice design as an important norm among privacy professionals.

B. Privacy Policies on the Books

Today's privacy policies are based on federal and state data privacy laws that focus almost exclusively on a what-when-how of user data: websites must disclose *what* data is collected, *when* it is collected, and *how* it is used. In other words, the law of notice and choice is about the substance of privacy policies, not their design. This is as true today as it was forty years ago, when data privacy principles were first articulated.

1. Privacy Principles

From the very beginning, the notice-and-choice approach to online privacy was primarily concerned with urging websites to inform users about data practices. It rarely concerned itself with the manner in which they were informed. A series of Fair Information Practices Principles (FIPPs), which developed out of a 1973 report from the federal Department of Housing, Education, and Welfare (HEW),[39] recommended that users be told of data use practices, that they have the opportunity to correct their data, and that they have to consent to any secondary uses of their information.[40] Several years later, the Organization for Economic Cooperation and Development (OECD) issued similar guidelines, requiring, for example, that data gatherers disclose the purpose and scope

38. *See generally* SAVICIC & SAVIC, *supra* note 17 (collecting examples of designs of public spaces that discourage antisocial behavior).

39. *See* U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973), http://www.epic.org/privacy/hew1973report [https://perma.cc/5PZ2-LU6P] [hereinafter HEW REPORT]. The Report was "the first portrait of information gathering and its impact on personal privacy ever provided by the U.S. government." ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 327 (2004).

40. HEW REPORT, *supra* note 39, at 41-42.

of data collection, any security protocols, and all user rights.[41] The FTC got in on the act in 2000, urging Congress to require commercial websites to provide

> notice of their information practices, including what information they collect, how they collect it (e.g., directly or through nonobvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.[42]

The FTC then identified "notice" as the most important FIPP. But the Commission's concept of notice, as illustrated by its specific recommendations, was limited to the words inside the policy.

This limited series of recommendations set the tone for determining what websites could be trusted to protect user privacy. As Daniel Solove and Woodrow Hartzog point out, TRUSTe would award one of its coveted privacy seals if a website notified users about "what information is gathered/tracked; [h]ow the information is used; [and] [w]ho information is shared with"[43] — namely, the what-when-how of user data. Therefore, being a trusted website depended on the substance of its disclosures. How the website made those disclosures — where it placed the privacy policy, what the policy looked like, when it notified users, and whether it was readable, accessible, and informative to a layperson — was less important.

2. The FTC Focuses on Substance

FTC enforcement actions have translated FIPPs into privacy law. The FTC stepped into the role of de facto privacy regulator in the late 1990s pursuant to its authority in Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[44]

---

41. ORG. FOR ECON. COOPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2001) http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/EFG7-A5KC].

42. PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON "PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE", BEFORE THE S. COMM. ON COMMERCE, SCI., AND TRANSP. § III(1) (May 25, 2000), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-online/testimonyprivacy.pdf [https://perma.cc/KSX4-SE4A].

43. Solove & Hartzog, *supra* note 5, at 593.

44. 15 U.S.C. § 45(a)(1) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful"). The FTC was given the authority to prevent such practices in subsection (a)(2). *See* 15 U.S.C. § 45(a)(2) (2012).

Its role, however, was limited. It started by enforcing the promises that companies made in their privacy policy disclosures.[45] Although the FTC has since developed a more expansive privacy jurisprudence,[46] many of its enforcement actions focus on privacy policies' substantive disclosures. This is evident in both the FTC's complaints and its settlements. At both ends, the lion's share of the Commission's focus on privacy policies has been on the substance of notice provided to consumers.[47]

Broken promises litigation is entirely based on the substantive disclosures in a privacy policy. The FTC brings these actions when a company says one thing — "[p]ersonal information voluntarily submitted by visitors to our site . . . is never shared with a third party"[48] — and does the opposite. In *In re Eli Lilly & Co.*, for example, the FTC alleged that the company violated its privacy policy when it sent out an email to nearly 700 people that disclosed personal information from customers who used the website Prozac.com.[49] The company's privacy policy had promised "security measures" that would protect consumers' confidential information.[50] Since no such security measures had been in place, the company had broken its promise. *In re Toysmart.com*[51] concerned another broken promise. During bankruptcy, Toysmart wanted to auction off a trove of customer data to pay its creditors even though the company had promised never to do so.[52] The FTC sued Toysmart in

45. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2114 (2004) ("[T]he agency is powerless—absent a specific statutory grant of authority—to regulate the collection of personal data by companies that either make no promises about their privacy practices or tell individuals that they will engage in unrestricted use and transfer of their personal data.").

46. *See* Solove & Hartzog, *supra* note 5. As the authors point out, the FTC has developed a broader view of unfair or deceptive practices, including, for example, "deception by omission," *id.* at 631, "inducement" to share personal information, *id.* at 632-33, and "pretexting," *id.* at 633, to name just a few. Their persuasive argument is that "through a common law-like process, the FTC's actions have developed into a rich jurisprudence that is effectively the law of the land for businesses that deal in personal information." *Id.* at 589. I argue that even though the FTC's jurisprudence is more than just enforcing privacy policy promises, when it has acted on unfair or deceptive privacy practices, it has limited itself to enforcing the content of privacy policies and generally ignored privacy policy design.

47. This Article does not purport to provide a comprehensive summary and analysis of all FTC privacy jurisprudence. For that complete review, *see generally* CHRIS JAY HOOFNAGLE, FED. TRADE COMM'N PRIVACY LAW AND POLICY 135-305 (2016); Solove & Hartzog, *supra* note 5, at 627-66.

48. First Amended Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. July 21, 2000) [hereinafter, Toysmart.com Complaint], http:// www.ftc.gov/sites/default/files/documents/cases/toysmart-complaint.htm [https://perma.cc/2GGQ-MDV6].

49. *In re* Eli Lilly & Co., 133 F.T.C. 763, 767 (2002) (complaint).

50. *Id.* at 765-66.

51. Toysmart Complaint, *supra* note 48.

52. *See id.* ¶ 11.

federal court to prevent the sale, arguing that it violated the express terms of the Toysmart privacy policy and would be constitute user deception if it went through.[53]

The FTC has also moved against companies that have promised, yet failed, to protect the confidentiality of their users' data,[54] to collect only certain types of data,[55] to put in place adequate security safeguards,[56] and to maintain user anonymity,[57] to name just a few examples. Broken promise litigation, which, by its very nature, is key to the substantive disclosures in privacy policies, remains a significant share of the FTC's overall privacy enforcement actions.[58]

The second way the FTC focuses on the substance of privacy policies is by requiring companies to include specific content in those policies as part of its settlement orders, while saying very little about what proper notice looks like. In its first privacy enforcement action, the FTC alleged that GeoCities sold its customers' personal information in express violation of its privacy policy.[59] As part of a settlement, the FTC ordered the company to disclose the what-when-how of data use: what information it collected, why it did so, to whom the information would be sold, and how customers could access their information and opt out.[60] The FTC has continued this laser focus on privacy policy content in its more recent privacy enforcement actions, as well. In *In re Frostwire, LLC*, for example, the FTC alleged that the company, which developed peer-to-peer file-sharing software, misled customers into thinking that certain files would not be publicly accessible on the peer-to-peer network. Frostwire also failed to adequately disclose how the software actually worked.[61] In *In re Sony BMG Music Entertainment*, the FTC alleged

53. *See id.* ¶¶ 16-18.

54. *In re* Eli Lilly, *supra* note 49.

55. *In re* Microsoft Corp., 134 F.T.C. 709, 715 (2002) (complaint).

56. *See, e.g.*, *id.* at 712; Complaint for Permanent Injunction and Other Equitable Relief ¶ 43, FTC v. Rennert, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000), http://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm [https://perma.cc/7C9T-V8QP].

57. Complaint, *In re* Compete, Inc., FTC File No. 102 3155, No. C-4384 ¶ 23 (F.T.C. Feb. 20, 2013), http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf [https://perma.cc/X5DX-BJK2] (alleging that the company had allegedly failed to anonymize data prior to transmission).

58. *See* Hoofnagle, *supra* note 47, at 159-66; Solove & Hartzog, *supra* note 5, at 628-38 (collecting cases).

59. Complaint ¶¶ 13-14, *In re* GeoCities, F.T.C. File No. 982 3015, No. C-3850 (Aug. 13, 1998), https://www.ftc.gov/sites/default/files/documents/cases/1998/08/geocmpl.htm [https://perma.cc/4BCQ-WLJY].

60. Decision and Order, *In re* GeoCities, F.T.C. File No. 982 3015, No. C-3850 (Feb. 12, 1999), https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do_.htm [https://perma.cc/D4PD-BUFR].

61. Complaint for Permanent Injunction and Other Equitable Relief at 19, FTC v. Frostwire, LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 12, 2011) [hereinafter Frostwire Complaint],

that Sony failed to inform customers that the software it installed on certain CDs would transmit music listening data back to Sony.[62] The FTC settled both cases. In each settlement, the FTC ordered Frostwire and Sony, respectively, to make specific what-when-how disclosures to its customers.[63] Each time, when it came time to think about how to use privacy policies to improve consumer notice and choice, the FTC focused on regulating their content.

Even when faced with manipulation via design, the FTC focused its remedial demands on the content of privacy disclosures. *In re Facebook* and *In re Sears Holdings Management* are prime examples because both companies used interface and design tactics to mislead or misinform users. In the *Facebook* Complaint, the FTC alleged that after Facebook changed its privacy settings to make certain information publicly available, it deceived its members via a seemingly user-friendly Privacy Wizard.[64] The Wizard consisted of several graphical dialog boxes with readable statements like, "We're making some changes to give you more control of your information and help you stay connected."[65] Users could click through and select privacy settings for different categories of information, from photos to birthdays to family.[66] Facebook thus used an appealing interface to suggest to its members that they had control over the privacy of their profile information. But the Wizard never disclosed that access to newly public information could not be restricted.[67] In *In re Sears Holdings Management Corp.*, the FTC charged Sears with misleading consumers about software that, when installed, acted like a vast fishing net, sweeping in extraordinary amounts of data.[68] Although the software "monitor[ed] nearly all of the internet behavior that occurs on consumers' computers," Sears only disclosed that the software would track users' "online browsing" and only in a click-through licensing agreement.[69] That license agreement was inscrutable:

---

http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf [https://perma.cc/54YR-D2SE].

62. Complaint at 4, *In re* Sony BMG Music Entm't, F.T.C. File No. 062 3019, No. C-4195 (June 29, 2007) [hereinafter Sony Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2007/01/070130cmp0623019.pdf [https://perma.cc/L2AH-WWH8].

63. *See* Frostwire Complaint, *supra* note 61, at 6; Sony Complaint, *supra* note 62, at 4.

64. Complaint at 4-7, *In the Matter of* Facebook, Inc., F.T.C. File No. 092 3184, No. C-4365 (July 27, 2012) http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf [https://perma.cc/7YBU-3SJK] [hereinafter Facebook Complaint].

65. *Id.* at 7.

66. *Id.* at 8.

67. *Id.*

68. Complaint at 1, *In re* Sears Holdings Mgmt. Corp., F.T.C. File No. 082 3099, No. C-4264 (Aug. 31, 2009) [hereinafter Sears Complaint], http://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf [https://perma.cc/BRZ9-56YG].

69. *Id.* at 5.

it was 19 pages long of small print, with only a handful of subheadings.[70] And yet, both the Sears complaint and settlement order virtually ignored the design of Sears's policy when it came time to allege counts of unfair and deceptive practices. Other than stating that the companies had to "clearly and prominently" inform consumers, the order listed particular substantive disclosures to include in a policy.[71] Sears's policy design tactic was relegated to an afterthought.[72]

As Solove and Hartzog found, almost all FTC enforcement actions settle.[73] And they settle with some common recurring elements, including, in relevant part, requirements that the company notify its customers of its wrongdoing, make substantive changes or additions to privacy policies, and establish a comprehensive privacy and data security program and inform users about it.[74] Missing from these settlement orders is any requirement as to the design of notice or, more specifically, what the notice would have to look like to adequately inform users.

3. Federal and State Laws and Privacy Policy Content

Unlike in the European Union, there is no comprehensive nationwide privacy protection law in the United States.[75] Instead, there are dozens of "sectoral" federal and countless state laws that purport to

---

70. Exhibit E, Sears Complaint, https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscomplaintaf.pdf [https://perma.cc/3U2K-YCF7].

71. Decision and Order, *In re* Sears Holdings Mgmt. Corp., F.T.C. File No. 082 3099, No. C-4264 (Aug. 31, 2009) [hereinafter Sears Order], https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searsdo.pdf [https://perma.cc/3G57-6Q7A]; Decision and Order, *In re* Facebook, Inc., F.T.C. File No. 092 3184, No. C-4365 (July 27, 2012) https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf [https://perma.cc/NX28-XV84] [hereinafter Facebook Order].

72. It is true that many of these orders and settlements included a requirement that any notice be displayed "clearly and prominently." According to the Facebook Order, which included common boilerplate language defining the phrase, "clear and prominent" notices are those "of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear" and "of understandable language and syntax." Facebook Order, *supra* note 71, at 2-3. Although noting the importance of clear and conspicuous display is an important step toward recognizing the manipulative tools beyond policy content, it says nothing about policy design. Even if it did, the FTC has never initiated an action against a company for deceptive privacy policy design. For a more complete discussion of how "clear and conspicuous" posting is an afterthought in privacy law, see *infra* Part II.B.4.

73. Solove & Hartzog, *supra* note 5, at 610-11.

74. *See id*. at 614-19.

75. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L281) 31, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046 [https://perma.cc/27NG-SL95]. Notably, the Directive is being replaced by the General Data Protection Regulation, with an effective date of the middle of 2018. *See* Reform of EU Data Protection Rules, http://ec.europa.eu/justice/data-protection/reform/index_en.htm [https://perma.cc/M66X-PXKR].

protect information privacy.[76] For example, the Health Information Portability and Accountability Act (HIPAA) helps protect the privacy of medical information[77] and the Gramm-Leach-Bliley Act gives individuals notice and control over information held by certain financial institutions.[78] HIPAA and Gramm-Leach-Bliley, along with the Children's Online Privacy Protection Act (COPPA)[79] and the E-Government Act,[80] are among the few federal laws that envision or mandate privacy policies. In most cases, like the Fair Information Practices on which they are based,[81] the statutes pay most of their attention to privacy policy content. A similar pattern is playing out in the states, where laws that envision privacy policies—like California's Online Privacy Protection Act[82] and New York's Internet Security and Privacy Act[83]—spend most of their time mandating particular substantive disclosures.

a. Federal Laws

Four federal privacy laws touch on or require privacy policies. In all four cases, Congress opted to try to achieve adequate notice and choice by focusing on privacy policy content. For the most part, it ignored design. COPPA, for example, which guards against unauthorized use, collection, and dissemination of information of children 13-years-old and younger,[84] requires certain child-oriented websites to post privacy policies. As with FTC settlement orders that demand privacy policies, COPPA also focuses on a what-when-how of data use. Websites must

76. State privacy laws are too numerous to list. Federal privacy laws, in addition to the ones discussed here, include, but are not limited to, the Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681 (2012) (credit histories), the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §§ 1221, 1232g (2012) (school records), the Privacy Act of 1974, 5 U.S.C. § 552a (2012) (personal information maintain by government), the Right to Financial Privacy Act of 1978, U.S.C. §§ 3401-3422 (2012) (bank records), the Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2012) (television viewing habits), the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2709 (2012) (protection against federal surveillance and electronic searches), and the Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (2012) (video rentals), among others. For a more comprehensive list, please see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 37-39 (4th ed. 2011).

77. 42 U.S.C. § 300gg (2012), 29 U.S.C. § 1181 (2012), and 42 U.S.C. § 1320d (2012).

78. 15 U.S.C. §§ 6801-6809 (2012).

79. 15 U.S.C. §§ 6501-6506 (2012) (protecting information websites gather from children under 13 years old).

80. E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (regulating federal agencies that gather and store personal data).

81. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 44 (2001) (noting how many federal privacy laws incorporated the HEW Report's Fair Information Practices).

82. CAL. BUS. & PROF. CODE §§ 22575-22579.

83. N.Y. STATE TECH. LAW § 203 (McKinney 2002).

84. 15 U.S.C. §§ 6501-6506.

disclose what data they collect, whether it is obtained actively or passively, how it will be used, whether it will be shared with others, and how to delete data or opt out of collection.[85] The E-Government Act mandates similar disclosures from federal government agencies and contractors.[86]

The Gramm-Leach-Bliley Act requires certain financial institutions to explain their data collection and use practices to their customers. The policy must state what information is collected, the names of affiliated and outside third parties with whom information is shared, which data is shared with them, and how to opt out.[87] HIPAA is even more specific in its content requirements: all HIPAA notices must have the same introductory sentence, informing readers of the purposes of the policy, and disclose what information is collected and how it will be used. It also must detail patients' rights with respect to their data, how the health care company will protect their data, and whom to contact for further information.[88] As with COPPA, the E-Government Act, and Gramm-Leach-Blilely, the statute's primary regulatory focus with respect to notice of data use practices is on the substance of disclosures.

b. State Laws

State laws have stepped in where the federal government feared to tread, regulating online intermediaries, protecting personal information, and requiring companies to inform users of their data use practices. State attorneys general have issued guidance documents, pressured internet companies, and initiated privacy enforcement litigation to enhance user notice and choice, as well.[89] The states and their chief legal enforcers are, in fact, the only ones to even nod to the manipulative capacity of privacy policy design. And yet, although some state statutes and best practice guides address extra-content issues like readability, accessibility, and design, the majority of laws, enforcement actions, and attorney-general opinions focus on the substance of privacy policy disclosure.

85. 15 U.S.C. § 6502(b)(1)(A)(i).

86. 44 U.S.C § 3501 (2015) (requiring the privacy policies of federal agencies to state, among other things, what information the agency collects, why it does so, how it will be used, with whom it will be shared, and how it will be secured).

87. 15 U.S.C. §§ 6803(a)(1)-(2); 16 C.F.R. §§ 313.6(a)(3), (6). Notably, regulations promulgated under Gramm-Leach-Bliley offer a model privacy form designed to simplify privacy notice. *See* Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62890-62994 (West 2016).

88. 45 C.F.R. § 164.520(b)(1) (West 2017).

89. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 758-63 (2016).

California's Online Privacy Protection Act (CalOPPA) is a groundbreaking law that requires commercial websites and other online service operators that collect information about California residents to post a data use policy and comply with its disclosures.[90] Like the policies envisioned by COPPA, the E-Government Act, Gramm-Leach-Bliley, and HIPAA, CalOPPA-compliant policies must contain specific substantive disclosures: what information is collected, with whom it may be shared, how the data will be used, and how individuals will be notified about policy changes.[91] A similar focus on disclosure content can be found in the state's "Shine the Light" law. This law, passed shortly after CalOPPA, requires businesses that have disclosed personal information about California residents to third parties for marketing purposes within the last year to disclose their data use and information sharing practices.[92]

Other states are following California's lead. In New York, the Internet Security and Privacy Act requires state agencies to create, adopt, and display a privacy policy on their websites.[93] Once again, the statute requires a what-when-how of data use practices: the policy must disclose what information is being collected, under what circumstances, whether the information will be retained by the state, how the data is gathered (actively or passively), the voluntariness of collection, how users can go about gaining access to their information, and what steps the state is taking to secure the data.[94] Connecticut and Michigan have laws requiring similar disclosures of any person or entity that collects Social Security numbers in the course of business.[95] Utah's Government Internet Information Privacy Act mandates adoption of a privacy policy before any government agency can collect citizens' data. The law makes only content-related requirements for the policy: the policy must disclose what information is collected, how it will be used, when and how it may be shared, how citizens can view and correct their information, and what security measures are in place.[96] Delaware's Online Privacy and Protection Act requires the operator of any online service that collects data on Delawareans to post a privacy policy. The law requires the

90. *See* CAL. BUS. & PROF. CODE §§ 22575-22579 (West 2016). The law sets a de facto national standard because companies have an incentive to comply with the strictest law rather than navigating fifty different requirements. *See* Citron, *supra* note 89, at 762.

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

92. CAL. CIV. CODE § 1789.83 . https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV.

93. N.Y. STATE TECH. LAW § 203 (McKinney 2002).

94. *Id*. § 203(1)(a)-(g).

95. CONN. GEN. STAT. ANN. § 42-471(b) (West 2009); MICH. COMP. LAWS § 445.84(1) (2005).

96. UTAH CODE ANN. § 63D-2-103(2) (West 2017).

same what-when-how content as CalOPPA does.[97]

As Danielle Keats Citron shows, state attorneys general (AGs) have used these and other laws to regulate privacy more aggressively than the FTC.[98] This is true for various legal, historical, and practical reasons that need not be repeated here.[99] Suffice it to say, however, that with few exceptions, when state AGs turned their considerable power to notice and choice, they focused primarily on privacy policy content. After ten states sued DoubleClick for tracking its users' online behavior without sufficient notice, for example, the company settled the matter by agreeing to post a privacy policy. The settlement required a notice of the what-when-how of data use: data collection practices, a promise to comply, and an opt-out option.[100] Policy design was not a factor.

In the mobile space, however, where the California Attorney General's Office has been particularly successful, regulatory efforts included at least one significant policy design feature: timing. Former Attorney General Kamala Harris's working group on mobile privacy secured commitments from Amazon, Apple, Google, Microsoft, Facebook, and others not only to display privacy policies on mobile apps but also to show them *before* users download the app.[101] This is an important step toward the consideration of privacy policy design, but it is still too rare among privacy regulators today.

4. *Moving Beyond Content*

Privacy regulators are not wrong to focus at least some of their energy on content. For a notice and choice regime to be possible, regulators must require some specific substantive disclosures. Those requirements also help establish data governance norms by forcing companies to commit to certain data use practices. And although the FTC and state AGs engage in more than just broken promises litigation, having a statement of specific disclosures facilitates privacy enforcement. On a more practical level, privacy policies, and the laws that require or enforce them focus on policy content because the key players in drafting privacy

97. DEL. CODE ANN. § 1201 (2000).

98. *See* Citron, *supra* note 89, at 750.

99. *Id*. at 3-4, 6-10.

100. *Id*. at 764 (citing Stephanie Miles, *DoubleClick Reaches Deal with State Attorneys General*, WALL STREET J. (Aug. 26, 2003, 5:37 PM), http://www.wsj.com/articles/SB1030381164280449795. [https://perma.cc/B7J9-DCEW]).

101. *Id*. at 756. *See* Press Release, State of Cal. Office of the Attorney Gen., Attorney Gen. Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy [https://perma.cc/3V5T-JEBA].

policies and their related laws are all lawyers. Trained and well-practiced in drafting contracts, lawyers possess knowledge and skill in the substantive terms of privacy policies, not in their design and presentation. As one prominent privacy attorney who also leads her firm's privacy group told me, privacy policies "are seen as legal documents, and they are regulated like ones. So we write them as if they are."[102]

But the substance of a company's data use disclosures cannot be the only part of a notice and choice approach to information privacy. The FTC and state privacy regulators are starting to recognize this. Many of the content requirements described above also mandate that the policies be readable[103] and clearly and conspicuously posted,[104] which means, at a minimum, requiring a link that is of a font, size, and color designed to call attention to itself.[105] An understandable policy available via a prominent link is an important step toward achieving adequate notice and choice. However, even with these requirements, the FTC has focused most of its attention on privacy policy content.

That should come as no surprise. There has been only occasional recognition that privacy policy design is an important factor for determining if a company is being transparent or deceptive about its data use practices. In 2001, former FTC Commissioner Sheila Anthony called for a "standard format" for privacy policies, along the lines of the Nutrition Labeling and Education Act's standard format for food labels.[106] Anthony recognized that inconsistent and confusing policy design was preventing consumers from becoming aware of their data privacy

102. Telephone Interview with "Private Practice Attorney" (name redacted per wishes of interviewee) (Mar. 16, 2016).

103. *See, e.g.*, 16 C.F.R. § 312.4(a) (LEXIS through 2016 Sess.) (listing COPPA's requirement that a covered website's privacy policy must be clear and understandable). The FTC's Financial Privacy Rule, promulgated under the Gramm-Leach-Bliley Act, requires that privacy policy language be "reasonably understandable," which means (1) using "clear, concise sentences, paragraphs, and sections; (2) us[ing] short explanatory sentences or bullet lists whenever possible; (3) us[ing] definite, concrete, everyday words and active voice whenever possible; (4) avoid[ing] multiple negatives; (5) avoid[ing] legal and highly technical business terminology whenever possible; and (6) avoid[ing] explanations that are imprecise and readily subject to different interpretations." 16 C.F.R. § 313.3(b)(2)(i)(A)-(F) (LEXIS through 2016 Sess.). As Joel Reidenberg and others have shown, however, privacy policies are generally not "reasonably understandable." *See* Reidenberg et al., *supra* note 1, at 87.

104. *See, e.g.*, Facebook Order, *supra* note 71, at 2; Sears Order, *supra* note 71, at 3; Decision and Order at 2, *In re Sony BMG Music Entm't*, FTC File No. 062 3019, No. C-4195 (F.T.C. June 28, 2007), https://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019do070629.pdf [https://perma.cc/2HS8-8M7K]; CAL. BUS. & PROF. CODE § 22575(b)(1), (3) (CalOPPA's clear and conspicuous link requirement); CAL. CIV. CODE § 1789.83(b)(1)(B) (California's "Shine the Light" law's conspicuous link requirement).

105. 16 C.F.R. § 313.3(b)(2)(ii)(A)-(E).

106. Sheila F. Anthony, *The Case for Standardization of Privacy Policy Formats*, FED. TRADE COMMISSION (July 1, 2001), https://www.ftc.gov/public-statements/2001/07/case-standardization-privacy-policy-formats [https://perma.cc/7XEA-MVL9].

rights.[107] In a report on how to comply with CalOPPA, the California Attorney General's Office recommended that policies be drafted in "a format that makes the policy readable, such as a layered format."[108] In reaction, the International Association of Privacy Professionals (IAPP) suggested "us[ing] graphics and icons in . . . privacy policies to help users more easily recognize privacy practices and settings."[109] California has also gone so far as to recommend that companies publish two different policies, one that is easy to read and geared toward ordinary consumers and another one for lawyers, regulators, and the FTC.[110] These infrequent nods toward the importance of privacy policy design in informing the public of its data privacy rights suggest an underlying recognition of the problem, but we need to bring privacy policy design out of the closet.

C. Myths About Users and Design

At the heart of these laws, norms, and lawsuits are two related misconceptions about users and design. First, by focusing almost exclusively on the content of privacy policies, notice and choice embeds an autonomy-based vision of privacy into the law. Second, and relatedly, notice and choice leads us to make disclosure decisions in a vacuum, divorced from embodied experience.[111] Both assumptions are dangerous to maintaining privacy online.

---

107. *Id.* ("If the goal of the industry's self-regulatory efforts is to provide informed consent for consumers, it has failed . . . . As a general rule, privacy policies are confusing, perhaps deliberately so, and industry has no incentive to make information sharing practices transparent. If privacy policies were presented in a standard format, a consumer could more readily ascertain whether an entity's information sharing practices sufficiently safeguard private information and consequently whether the consumer wishes to do business with the company."). *But see* Gill Cowburn & Lynn Stockley, *Consumer Understanding and Use of Nutrition Labeling: A Systematic Review*, 8 PUB. HEALTH NUTRITION 21, 22 (2005) (arguing that standardized labeling does not alleviate all comprehension problems).

108. CAL. DEP'T OF JUST., MAKING YOUR PRIVACY PRACTICES PUBLIC: RECOMMENDATIONS ON DEVELOPING A MEANINGFUL PRIVACY POLICY [hereinafter PRIVACY PRACTICES] (May 2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf [https://perma.cc/788Q-9NZF].

109. Lei Shen, *Unpacking the California AG's Guide on CalOPPA*, THE PRIVACY ADVISOR (May 27, 2014), https://iapp.org/news/a/unpacking-the-california-ags-guide-on-caloppa [https://perma.cc/G7FC-9ESW].

110. *See* CAL. DEP'T OF JUST., PRIVACY PRACTICES, *supra* note 108, at 4-5.

111. "Embodied" experience refers to the phenomenological and pragmatic idea that things like comprehension, understanding, and truth are only possible through lived experience as mediated by the social structures around us. *See, e.g.*, *Preface* to MAURICE MERLEAU-PONTY, PHENOMENOLOGY OF PERCEPTION xi (Ted Honderich ed., Colin Smith trans. 1962) ("The world is not an object such that I have in my possession the law of its making; it is the natural setting of, and field for, all my thoughts and all my explicit perceptions."). It was applied to the context of cyberspace by Julie Cohen. *See, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 34-41 (2012) [hereinafter, "NETWORKED SELF"]; Cohen, *Cyberspace*, *supra* note 12, at 226-35.

As a doctrine of informed consent,[112] notice and choice ostensibly allows us to exercise control over our information by making rational disclosure decisions based on all the evidence. Such notions of autonomy and choice animated the FIPPs and the Clinton Administration's "Framework for Global Electronic Commerce."[113] And the FTC has explained that notice is "essential to ensuring that consumers are properly informed before divulging personal information."[114] In other words, notice and choice was meant to give us the tools needed for perfectly rational decision-making.[115]

Basing a data privacy regime on this conception of the self is problematic. A perfectly rational self does not exist. Even if it did, it can be anathematic to privacy. If privacy is the liberty to decide for ourselves what others know about us, then any act of revelation is transformed into a conscious volitional act of disclosure for which we assume the risk that whatever we share could be further disseminated, publicized, or used against us. Courts have run with the idea,[116] narrowing privacy to mere secrecy, or what Daniel Solove has called the "secrecy paradigm."[117]

---

112. *See* IMMANUEL KANT, GROUNDWORK OF THE METAPHYSICS OF MORALS (Lara Denis ed., Thomas Kingsmill Abbott trans., 2005) (ebook). A complete retelling of Kant's metaphysics is beyond the scope of this paper. For the best summary of Kant's philosophy and his connection to modern liberalism, see MICHAEL SANDEL, LIBERALISM AND THE LIMITS OF JUSTICE (2d ed. 1998).

113. HEW Report, *supra* note 39, at 41-42. *See also* President William Jefferson Clinton, *A Framework for Global Electronic Commerce*, THE WHITE HOUSE (July 1, 1997), http://clinton4.nara.gov/WH/New/Commerce/read.html [https://perma.cc/Q6PM-EDDL] ("[d]isclosure by data-gatherers is designed to simulate market resolution of privacy concerns by empowering individuals to obtain relevant knowledge" about data collection and practices. "Such disclosure will enable consumers to make better judgments about the levels of privacy available and their willingness to participate.").

114. FED. TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf [https://perma.cc/F56B-TG43]. Notably, these same Kantian principles animate the doctrine of informed consent in the medical and research contexts.

115. *See* Calo, *supra* note 25, at 1049.

116. A telephone user, for example, "voluntarily convey[s] numerical information to the telephone company . . . [and] assume[s] the risk" that the telephone company would subsequently reveal that information. Smith v. Maryland, 442 U.S 735, 744 (1979). A bank depositor has no legitimate expectation of privacy in the financial information freely given to banks because "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." United States v. Miller, 425 U.S. 435, 443 (1976). And this doctrine has been extended to the internet. Some federal courts have held that because any information conveyed to an online service provider in order to access the internet is "knowingly revealed," there can be no invasion of privacy when an internet service provider ("ISP") gives that information to someone else. United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); United States v. Hambrick, 55 F. Supp. 2d 504, 508–09 (W.D. Va. 1999).

117. DANIEL J. SOLOVE, THE DIGITAL PERSON 42-43, 143 (2004).

Nor is it clear that conceptualizing the self as radically disembodied from experience, identity, and social life is actually a good idea.[118] And, in fact, scholars have shown that we do not make perfectly rational disclosure decisions.[119] Rather, we make them in context, influenced by those around us and the design of online built environments.[120] The law of notice and choice today ignores such contextual factors.[121] Therefore, it does not correspond to how we make decisions in the real world, it is inconsistent with what we know about the propensity to disclose, and it satisfies no one.[122]

III. CONSTRAINED BY DESIGN

Notice and choice today is focused primarily on the content of privacy policies and is manifested in long and impractical notices. It is also built on the foundation of the perfectly rational user. But, as Julie Cohen notes, "cyberspace is not, and never could be, the kingdom of the mind; minds are attached to bodies and bodies exist in the space of the world."[123] Laws and norms regulating internet social life, therefore,

---

118. *See, e.g.*, COHEN, NETWORKED SELF, *supra* note 111, at 16-21 (describing the governing principles of cyberspace); MICHAEL SANDEL, DEMOCRACY'S DISCONTENT 3-28 (1996) (describing the foundations of political philosophy).

119. *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363-64 (Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis & Sabrina di Vimercati eds., 2007); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SEC. & PRIVACY Jan.-Feb. 2005, https://www.dtc.umn.edu/weis2004/acquisti.pdf [https://perma.cc/BSU7-Y7WD].

120. For example, Alessandro Acquisti, Leslie John, and George Loewenstein have found that disclosure behavior is based on comparative judgments: if we perceive that others are willing to disclose, we are more likely to disclose; if we perceive that the information asked of us is particularly intrusive, we are less likely to disclose. *See* Alessandro Acquisti et al., *The Impact of Relative Standards on the Propensity to Disclose*, 49 J. MARKETING RES. 160, 160, 165, 171, 172 (2012), https://www.cmu.edu/dietrich/sds/docs/loewenstein/ImpactRelStandards.pdf [https://perma.cc/QP7C-L4W8]. Leslie John found that individuals are, perhaps counter-intuitively, more willing to admit to bad behavior on unprofessional-looking websites. These platforms were perceived to be more casual, relaxed, and informal, rather than less secure. *See* John, Acquisti & Loewenstein, *supra* note 11. Moreover, other scholars have found that disclosure can be emotionally manipulated: positive emotions about a website, inspired by website design, the type of information requested, and the presence of a privacy policy, correlate with a higher willingness to disclose. *See* Han Li et al., *The Role of Affect and Cognition on Online Consumers' Decisions to Disclose Personal Information to Unfamiliar Online Vendors*, 51 DECISION SUPPORT SYS. 434, 435 (2011).

121. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, PRIVACY, AND THE INTEGRITY OF SOCIAL LIFE (2009).

122. These are the requirements of "pragmatic" truth, based on the work of John Dewey. *See* James T. Kloppenberg, *Pragmatism: An Old Name for Some New Ways of Thinking?*, 82 J. AM. HIST. 100, 103 (1996).

123. Cohen, *Cyberspace*, *supra* note 12, at 218.

cannot ignore our embodied experiences.[124] And those embodied experiences are constrained by the design of the built environments around us, both offline and online. In other words, the law of privacy notices must both recognize that we can be constrained and manipulated by policy design and, therefore, protect us from design's potentially coercive effects.

The notion that the design or frame of online space can configure and constrain embodied users is nothing new. Larry Lessig wrote about it,[125] as has Julie Cohen,[126] Ryan Calo,[127] and Woodrow Hartzog.[128] The general notion is well accepted among social scientists, artists and architects, interior designers, and urban planners as well. I would like to argue that the same principle holds true for privacy policies. In this section, I briefly construct an embodied conception of the user that is configured by technology and design. I then provide examples from the world of art and design to show that the constraints imposed by design are all around us. Throughout, I suggest ways that privacy policy design similarly limits our free choice. Finally, I discuss the results of an empirical study that shows that privacy policy design has a significant impact on user decisions to trust or do business with a website.

A. Configuring and Constraining the User

For many social scientists, there are structural elements of society beyond our control that constrain our freedom of will.[129] The sociologist Anthony Giddens argued that the social world is "made to happen" within the rules and available resources of a society.[130] These rules, manifest in everyday life, coerce us with and without our knowledge. They are everything from subtle tactics like Cass Sunstein's "nudges"[131] to the blunt axe of New York City's subway tracks, which make it difficult to get from Chelsea to the Upper East Side.

---

124. That real people are on the other end of online data flows is, after all, why we care about data flows in the first place. *Id.* at 221.

125. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 24-29 (1999) (noting that the design of the digital technologies that make up "cyberspace" make it impossible for it to be a completely free space).

126. *See generally* Cohen, *Cyberspace*, *supra* note 12.

127. *See generally* Calo, *supra* note 25.

128. *See generally* Hartzog, *supra* note 26.

129. EMILE DURKHEIM, THE RULES OF SOCIOLOGICAL METHOD 50–51 (Steven Lukes ed., W.D. Halls trans., The Free Press 1982) (1895), http://comparsociology.com/wp-content/uploads/2013/02/Emile-Durkheim-Rules-of-Sociological-Method-1982.pdf [https://perma.cc/9DLB-WSK2].

130. KIM DOVEY, FRAMING PLACES: MEDIATING POWER IN BUILT FORM 19-20 (2d ed. 2008).

131. *See* RICHARD THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

These structures constrain or, to borrow Steve Woolgar's term, configure us.[132] When Woolgar coined that phrase, he was talking about how the process of designing new technologies involves identifying some conception of the user and engineering a device that puts limits on users' actions.[133] For just two examples, think of how our computer ports are designed for specific inputs (a USB cable, for example, will not fit in a Parallel Port) or the restrictions imposed by Digital Rights Management. As the user figures into the design process, the technology undergoes a process of social construction: it obtains meaning and changes through the embodied experience of those involved, from the engineers to the users.[134] For example, Susan Douglas has shown that amateur radio operators helped make the technology a medium for broadcasting rather than just one-to-one communication.[135] Ronald Kline and Trevor Pinch have demonstrated how rural America helped change the design and use of the car.[136] They are not alone.[137]

This social narrative of technology envisions users differently than notice and choice today. We interact with technology not as ideal disembodied, purely rational actors, but as real people, doing real things with technology, situated in times and places where needs are contingent and decisions are contextual.[138] We may have an impact on the design of new technologies if our needs trickle down to the engineers,[139] but we are always configured, or affected and constrained, by the designs of the technologies we use and the spaces we inhabit.

Art and design are parts of this story[140] because they frame and limit our agency in a space.[141] Indeed, as Henri Lefebvre argued, the nature

---

132. Woolgar, *supra* note 15, at 61.

133. *Id.* at 59, 61, 89.

134. SUCHMAN, *supra* note 15, at 187.

135. SUSAN DOUGLAS, INVENTING AMERICAN BROADCASTING, 1899-1922 (1987).

136. *See generally* 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).

137. *See, e.g.*, CLAUDE FISHER, AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940 (1992); MICHELE MARTIN, HELLO CENTRAL?: GENDER, TECHNOLOGY AND CULTURE IN THE FORMATION OF TELEPHONE SYSTEMS (1991); DAVID E. NYE, ELECTRIFYING AMERICA: SOCIAL MEANINGS OF A NEW TECHNOLOGY, 1880-1940 (1990) (electricity and electric appliances, streetlights, and trolleys).

138. SUCHMAN, *supra* note 15, at 191; *see* Nissenbaum, *supra* note 121.

139. Woolgar's ethnographic study of a company developing one of the first microcomputers showed that structural forces at play prevented users from truly being considered in design. *See* Woolgar, *supra* note 15, at 70-71, 73-4.

140. Michel Foucault, *On Power*, *in* MICHEL FOUCAULT: POLITICS, PHILOSOPHY, AND CULTURE: INTERVIEWS AND OTHER WRITINGS, 1977-84 (Lawrence Kritzman ed., 1988) (arguing that architecture is complicit in a "long elaboration of various techniques that made it possible to locate people, to fix them in precise places, to constrict them to a certain number of gestures and habits").

141. DOVEY, *supra* note 130, at 1.

of a space is determined by what designers want to happen or not to happen in it.[142] Movers in that space, then, are part of and subject to the environment, not in control of it. Such constraint is part of our embodied experience. The same can be said of internet users, generally: when we log on to Facebook or shop on Amazon, our freedom is constrained by the design of the interface, the capacities of the server, and the platform's data use practices. And when we try to understand a website's privacy policy, we are similarly constrained by the way it is framed, presented, and designed. It makes sense, then, that privacy notices, and the laws that govern them, should reflect this reality.

1. Fine Art

Artists are particularly adept at using the principles of design and structure to lead their audiences on a journey through a work. They deploy line, color, contrast, perspective, and positioning, among other tools, not only to tell a story, but also to bring their viewers along with them through that story. Leonardo da Vinci's *The Last Supper*[143] (Image 1) uses one-point perspective to focus our attention on Jesus Christ at the center of the table. The lines implied by the upper and lower edges of the walls and windows and the sides of the table and ceiling coffers create the illusion of perspective by directing the eye toward a single vanishing point behind Christ's head. In fact, all lines—and, therefore, viewers' eyes—are directed to that single focal point. Even the faces and hands of Jesus's disciples, seated on either side, take the viewer on a step-by-step and directed journey from the ends of the table, from one disciple to another, toward Jesus at the center.[144] By making the artistic choice to situate his subjects in the foreground of a long hallway, Leonardo promoted visual movement, taking his audience on a visual journey he prescribed.

142. HENRI LEFEBVRE, THE PRODUCTION OF SPACE 224 (Donald Nicholson-Smith trans., 1991) (1984).

143. MARTIN KEMP, LEONARDO DA VINCI: THE MARVELLOUS WORKS OF NATURE AND MAN 177 (2007) (displaying "The Last Supper").

144. *Id.* at 176-87.

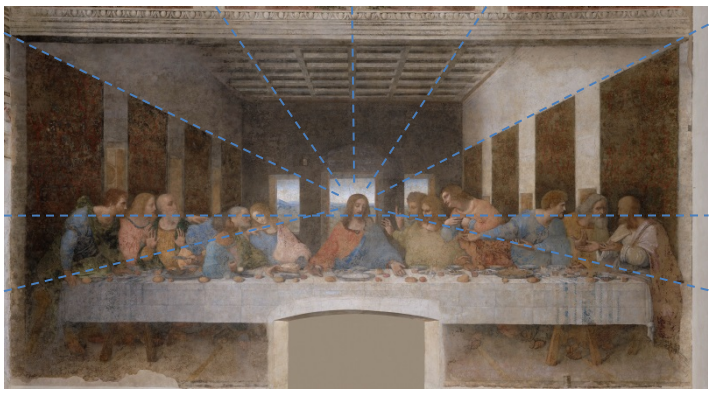


Image 1

Line was one among several tools Leonardo used to draw the viewer's attention toward his image of Christ. He used light as well: the white tablecloth and the light at the center of the horizon in the background supplement the one-point perspective in *The Last Supper*. Francisco de Goya uses line, color, and contrast to tell an emotional story about Napoleonic aggression in Spain in *The Third of May, 1808* (Image 2).[145] Goya wanted to depict the horrors of the French invasion of 1808, in which Napoleon overthrew the Spanish monarchy.[146] Aggressive yet faceless French troops are lined up on the right, with their heads pointed down. But the viewers' eyes are drawn from the darkness engulfing the French, along the line of the rifles, toward a bright Christ-like figure, dressed in white, with his arms in the air. The lantern in the middle of the painting allows Goya to use light to focus our eyes on the Spanish victim. But it was his artistic choice to highlight the tops of the rifles rather than the bottoms, off which the light from the lantern would have been reflected in reality, that allowed him to encourage visual movement from right to left, where he wants our visual focus to rest.

145. *See* ENRIQUE LEFUENTE FERRARI, GOYA: THE COMPLETE ETCHINGS AND LITHOGRAPHS (Raymond Rudorff trans., 1995).

146. *See generally* CHARLES J. ESDAILE, THE PENINSULAR WAR: A NEW HISTORY (2002); IAN FLETCHER ED., THE PENINSULAR WAR: ASPECTS OF THE STRUGGLE FOR THE IBERIAN PENINSULA (1998).

Image 2

These examples suggest that constitutive elements of the underlying structure of a work of art—line, contrast, perspective, color, and light, for example—can be used to help the artist tell her story and push the audience to focus on particular points of interest.[147] The same is true with privacy policies. They, too, tell a story: they offer a narrative of a company's data use practices and provide users with options to change their privacy settings or opt out entirely. If internet services are truly interested in providing their users with adequate notice and choice, they too could use principles of design to focus the reader on important information. Any policy could use bold typeface, large fonts, and subheadings. They could also contrast white and dark spaces to highlight particularly important user rights. Charts with shaded boxes separated from the background may be particularly helpful. As would contrasting colored text and arrows and lines that direct users to explanations about data use practices. Of course, as discussed in more detail below, line and structure can be used to manipulate and misdirect. Design is not neutral,[148] though adequate regulatory enforcement and monitoring can guard against the nefarious use of design.

147. Ryan Calo's argument about "visceral notice" reflects this point as well—namely, that effective notice must draw attention to itself through design. *See* Calo, *supra* note 25.

148. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (forthcoming 2018).

2. Architecture

Architects design built environments that influence human behavior within them.[149] Sometimes, they do so explicitly, as with designs based on Jeremy Bentham's *Panopticon*.[150] Indeed, as Julie Cohen has pointed out, spaces can be designed to achieve the regulatory and passivity goals of surveillance even if no one is watching on the other end. Even though we cannot see ourselves being watched, we recognize that watching is possible, and we alter our behavior accordingly.[151] Elsewhere, structure is deployed in more subtle ways to influence human behavior. For example, the Design Against Crime Research Centre at the University of the Arts London has redesigned environments that had seen high rates of bicycle and bag theft. The program's central thesis is that built environments can "influence offender decisions *before* criminal acts occur."[152] They moved barriers, added lights, created social spaces, and eliminated hidden corners. And they succeeded at reducing levels of petty crime.[153]

We see the symbiotic relationship between the design of built online environments and users' behavior within them every day. The specter of online surveillance affects how we interact with each other and with the websites we visit.[154] Danielle Citron has argued that we can design digital spaces to tamp down on antisocial and harassing behavior by "imbu[ing] online interactions with a sense of human connectedness," i.e., through rich digital avatars, gender- and sexually-inclusive imagery, and strategies that evoke physical social spaces and the norms that come with them.[155] Digital Rights Management (DRM) technology is a form of internal structure that restrains the freedom of consumers of copyrighted works by building in limits to potentially unlawful behavior.[156]

149. *See, e.g.*, Maurice Broady, *Social Theory in Architectural Design*, *in* PEOPLE AND BUILDINGS 170, 171-85 (Robert Gutman ed., 2009).

150. The panopticon uses architecture, or the arrangement and structure of a built environment, to achieve particular coercive behavioral goals: specifically, it is designed so everyone inside can be seen and surveilled from a central point. *See* JEREMY BENTHAM, PANOPTICON; OR, THE INSPECTION HOUSE (1787). *See also* LISA FINDLEY, BUILDING CHANGE: ARCHITECTURE, POLITICS AND CULTURAL AGENCY 3 (2005).

151. Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 193-94 (2008).

152. Lorraine Gamman & Adam Thorpe, Design Against Crime as Socially Responsive Design for Public Space, Presentation at the UK/Brazil Workshop on Innovation and Investment in Research and the Creative Economy (December 2007).

153. *Id.*

154. Cohen, *supra* note 151, at 196.

155. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 239-41 (2015).

156. James Grimmelmann, Note, *Regulation By Software*, 114 YALE L.J. 1719 (2005). Some free software advocates even call DRM "Digital *Restrictions* Management." *See, e.g.*, *What is DRM?*, DEFECTIVEBYDESIGN.ORG (Feb. 22, 2016), http://www.defectivebydesign.org/what_is_drm [https://perma.cc/JLT5-4RBG].

The fact that Twitter posts must be under 280 characters also constrains behavior: the restriction has spawned an entire language of abbreviations[157] and forces users to replace standard grammar with symbols and shorthand,[158] or to give up on comprehensibility altogether.[159] Drop-down menus limit our response options to certain questions.[160] Facebook is designed to nudge us to disclose personal information with our friends and online advertisers.[161] Design does indeed configure users.

Online environments can constrain or foster behavior, restrict or inspire autonomy, and erode or protect privacy.[162] That an online environment can be designed from the ground up to protect data privacy is at the heart of one vision of privacy by design, or, as Ann Cavoukian, the Information & Privacy Commissioner of Ontario, defined it: "the philosophy and approach of embedding privacy into the design specifications of various technologies."[163] Instead of relying purely on a post-breach regulatory and litigation regime that merely reacts to privacy losses, Cavoukian wanted technologies to embody privacy protection as a matter of course.[164] This could include building databases with internal cybersecurity measures, incorporating privacy into everyday corporate practice, placing limits on data collection, and everything in between.[165]

Creating and presenting privacy policies in a way users can understand is an important part of making privacy by design a reality. The policies, often placed at the bottom or in a corner of a page, are hidden

---

157. *See, e.g.*, Tia Fisher, *Top Twitter Abbreviations You Need to Know*, SOCIAL MEDIA TODAY (May 22, 2012), http://www.socialmediatoday.com/content/top-twitter-abbreviations-you-need-know [https://perma.cc/D4E8-DGVF].

158. *See, e.g.*, Carrie Fisher (@carrieffisher), TWITTER (Dec. 14, 2016), https://twitter.com/carrieffisher [https://perma.cc/V3NY-H3FN].

159. *See* Sam Biddle, *Senator Chuck Grassley Is the Worst Twitter User in the United States of America*, GIZMODO (Apr. 28, 2011), http://gizmodo.com/5796338/senator-chuck-grassley-is-the-worst-twitter-user-in-the-united-states-of-america [https://perma.cc/LN7E-XLM7].

160. *See, e.g.*, Jason Kessler, *Facebook Adds Civil Union, Domestic Partnership to Relationship Status*, CNN (Feb. 18, 2011, 6:53 AM), http://www.cnn.com/2011/TECH/social.media/02/18/facebook.relationship.status [https://perma.cc/DZ4Z-HQA5].

161. *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1151 (2009); *see also* Ari Ezra Waldman, *Privacy, Sharing, and Trust*, 67 CASE W. RES. L. REV. 193 (2016).

162. *See* Cohen, *Cyberspace*, *supra* note 12, at 222-24.

163. ANN CAVOUKIAN, PRIVACY BY DESIGN 3 (2009). *See also* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE SEVEN FOUNDATIONAL PRINCIPLES (2009); Hartzog, *supra* note 148.

164. *See also* Paul Dourish & Ken Anderson, *Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena*, 21 HUMAN-COMPUTER INTERACTION 319, 321 (2006).

165. *But see* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH L.J. 1409 (2011); Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents* (N.Y.U., Working Paper No. 12-43, 2012).

from view.[166] This sends two messages, both of which encourage users to ignore the policies. First, many websites make them difficult to find, so most users give up trying; this operationalizes resignation as a business tool. Second, by placing the privacy policy link at the bottom of a page in a small font, the website's design diminishes the policy's importance, suggesting to users that their privacy is an afterthought, and that the act of reading the privacy policy is not worth their time. Retailers are familiar with this tactic: the price tag on a shirt at H&M, a discount apparel store, is usually obvious to consumers; indeed, the price is often posted above an entire rack of clothes. At the high-end department store Barney's, by contrast, not only is the price tag frequently hidden in a pocket on the inside of a garment, but the price itself is often written in a small font. A privacy policy from a company that imbues consumer privacy throughout its corporate ethos, practice, and routine would not only be prominent, but would make its privacy-protective practices key elements of a company's marketing strategy. A website designer can also program privacy notifications to pop up when a user is about to share personal information, enhancing user notice and creating opportunities for affirmative consent.[167]

3. *Interior Design*

A room is not just a space, just like a privacy policy is not just legalistic argle-bargle.[168] Rooms are social spaces, and the placement of the fixtures and pieces of furniture within them influences the social interactions that take place inside.[169] Designers create "circulation plans" for spaces, showing how a space and its constituent elements will encourage movement or discourage other behavior.[170] Interior design thus has a direct coercive effect on behavior: because spaces require that we walk through them, our movement is manipulated and constrained by a

166. *See, e.g.*, METLIFE, https://www.metlife.com [https://perma.cc/Y8JR-GSEG] ("Privacy Policy" located at the bottom, toward the left of the page, in size-6 font); DISNEY, https://www.disney.com [https://perma.cc/VG2T-LUCW] ("Privacy Policy," located at the very bottom, center-left of the page, in size-6 font).

167. These are called "just-in-time" notifications. The FTC recommends them: "Providing such a disclosure at the point in time when it matters to consumers, just prior to the collection of such information by apps, will allow users to make informed choices about whether to allow the collection of such information." FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013) at 15, 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/4ZZ6-26UX].

168. *See United States v. Windsor*, 133 S. Ct. 2675, 2709 (2013) (Scalia, J., dissenting).

169. LEFEBVRE, *supra* note 142, at 73, 193 (arguing that spaces are designed to create spatial relationships that facilitate or discourage social exchange). *See also* Cohen, *Cyberspace*, *supra* note 12, at 233, 235-6.

170. JOHN F. PILE, INTERIOR DESIGN 84 (1988).

space's design.[171] A predetermined plan can direct movement along a path, like in any Ikea store, for example. Given a massive open space, Ikea's store planners lay out walls that separate their products into different departments in such a way as to create a single path through the stores. Following this prescribed course, a customer has to make her way through "bedrooms" before reaching "bathrooms."[172]

Influencing behavior through the placement of furniture can be subtler, yet no less effective. For example, the environmental psychologist Robert Sommer helped improve the lives of residents at a facility for the elderly when he removed couches from the walls and placed chairs and tables in the center. He and his colleagues noticed a marked increase in conversation and interaction among residents, contributing to greater happiness and health.[173] Where Sommer used furniture placement to encourage social interaction, some fast food restaurants use interior design to encourage turnover. They install uncomfortable or unpleasant chairs and design spaces to be functional, but aesthetically unsatisfying.[174] This discourages conversation and prevents loitering and delays for other customers.

Privacy policies today may be designed like a McDonald's restaurant. Privacy policies may deploy placement strategies that make users uncomfortable and keep them uninformed. They are, then, paradigmatic examples of "unpleasant design."[175] For example, many policies are presented single-spaced, with small letters and small margins, creating no possibility for effective eye movement and reading ease. And although most privacy policies have opt-out links, these tend to be hidden: they are either inside the text, perhaps written in the same color and size as the rest of the policy, or under a series of click-through subnavigation pages. These placement strategies discourage users from even trying to understand their privacy rights in the first place.

4. *Urban Design*

Urban planners are particularly adept at using design to manipulate behavior: they can restrict movement, foreclose or encourage behavior, and evoke powerful emotional responses.[176] There are countless examples of coercive urban plans throughout history,[177] but the most famous

171. *Id*. at 50.

172. *See* JOHAN STENEBO, THE TRUTH ABOUT IKEA: THE SECRET BEHIND THE WORLD'S FIFTH RICHEST MAN AND THE SUCCESS OF THE FLATPACK GIANT (2010).

173. *See* ROBERT SOMMER, PERSONAL SPACE: THE BEHAVIORAL BASIS OF DESIGN (1969).

174. *See* Katyal, *supra* note 16, at 1043 (*citing* WILLIAM H. ITTELSON ET AL., AN INTRODUCTION TO ENVIRONMENTAL PSYCHOLOGY 236 (1974)).

175. *See supra* notes 17-18.

176. LEFEBVRE, *supra* note 142, at 101.

177. *See* DIANE FAVRO, THE URBAN IMAGE OF AUGUSTAN ROME 3, 221, 227-32 (1996)

one is Napoleon III and Georges Haussmann's radical redesign of Paris after 1850.[178] Napoleon III became President of the Second French Republic and then Emperor of France in 1848 and 1852, respectively.[179] At that point, Paris was a "confused,"[180] overcrowded, and poorly designed city:[181] it had narrow, oddly shaped streets, some of which randomly reached dead-ends and many of which were difficult to traverse because of their shape, poor construction, and filth.[182] Its design allowed disease to fester and spread.[183] It was so difficult to get around that people gave up: Parisians tended to avoid walking long distances, keeping to the 4-block radius around their homes.[184] Unpleasant design constrained their behavior.

In the two decades before Napoleon III came to power, Paris was plagued by several peasant uprisings, all of which used the design of the city to their advantage. As depicted by Victor Hugo in *Les Misérables* (1862), Paris's narrow, winding streets were easily barricaded; troops were cut off from their regiments by peasants using household furniture to block several choke points.[185] Napoleon III wanted to change the city's layout to prevent this from happening again. Along with Haussmann, his Prefect of the Seine, he set out to redesign Paris in ways that would have indelible effects on the behavior of the city's residents. He replaced narrow streets with broad thoroughfares that were impossible to barricade.[186] He arranged his new boulevards to facilitate the movement of traffic (and troops, if necessary) through the city.[187] And he designed these new open spaces to amplify France's imperial prestige.[188]

(Rome under Emperor Augustus); LEFEBVRE, *supra* note 142, at 151-52 (Spanish colonial towns in South America).

178. DAVID H. PINKNEY, NAPOLEON III AND THE REBUILDING OF PARIS 7-8 (1958). This was, in fact, the second major redesign of Paris. The Bourbon kings, Henri IV, Louis XIII, and Louis XIV, all helped redesign Paris from a medieval enclave to a modern city. *See* JOAN ELIZABETH DEJEAN, HOW PARIS BECAME PARIS 21-44 (2014).

179. TED W. MARGADANT, FRENCH PEASANTS IN REVOLT: THE INSURRECTION OF 1851, xvii (1980).

180. PINKNEY, *supra* note 178, at 16.

181. *Id.* at 7, 9.

182. *Id.* at 14.

183. *Id.* at 8.

184. *Id.* at 18.

185. *See generally* JILL HARSIN, BARRICADES: THE WAR OF THE STREETS IN REVOLUTIONARY PARIS, 1830-1848 (2002); MARK TRAUGOTT, THE INSURGENT BARRICADE (2010). The 1848 uprising in Paris, which ended the Orléans Monarchy and paved the way for Louis-Napoléon's election to the presidency in the Second Republic, was just one in a long series of worker and peasant revolts in Paris. One such insurgency, the June Rebellion in 1832, inspired Victor Hugo to write *Les Misérables* (1862), a historical novel telling the story of downtrodden peasants fighting against income inequality.

186. PINKNEY, *supra* note 178, at 35-36.

187. *Id.* at 39.

188. *Id.* at 38.

This way, the design of the city became an ally in his plan to pacify the Parisian peasant class.

In such ways, urban planners, using some of the same tools employed by painters, architects, and interior designers, help determine how a city's inhabitants and visitors interact with the space around them. Privacy policy designers can use similar methods to analogous effect. Where Napoleon III's broad thoroughfares directed traffic through the city and toward its center, a web designer's wide margins, large headings, and sizeable charts could direct readers' eyes to important data use practices. As it stands, websites and their privacy policies are much more like the France of 1850: there are few clear paths through the policy and few clear paths to find the policy in the first place.

B. The Design of Privacy Policies

Design, as we have seen, can be a constraining tool. Artists, architects, interior designers, and urban planners create their works with their audiences in mind, configuring and affecting our embodied experience. Even unseen structure can tell a story, guide someone's eye, or make city traffic flow smoothly. It can also obfuscate, discourage dissident behavior, and empower entrenched interests. When it does so, it erodes freedom and limits choice. The same is true of the structure of online space.[189]

To what extent do designs of privacy notices influence users' decisions to share personal information? In this section, I present the results of a study on the effect of policy design on user privacy and disclosure choices. The data suggest that, when given the opportunity, users consider design when making privacy choices, not just the substance of a website's data use practices: holding data use practices constant, users prefer to do business with websites that post privacy policies designed with real people in mind. Of greater concern, however, is evidence that design can be used to manipulate and harm consumers: users tended to opt for websites with pleasing privacy policy designs even when those websites' data use practices were invasive and unsafe. Furthermore, poorly designed privacy policies, like most privacy policies in use today, discourage users from reading them in the first place. In both cases—where design is used to manipulate and where design is used to obfuscate—users are much more likely to make risky privacy choices. Therefore, privacy regulators who seek to protect consumers from unfair, coercive, and deceptive practices should not only consider how a company's disclosures conform to its actual data practices. They should also investigate how websites use design to transmit those disclosures.

189. *See generally* Cohen, *Cyberspace*, *supra* note 12.

1. Research Questions

Design's coercive potential raises the following questions: Are users more willing to trust or do business with companies whose privacy policies are designed with transparency and user comprehension in mind? Are there specific design strategies that make policies easier to understand? Could a user-friendly design influence users to make poor privacy choices? What effect do poorly designed privacy policies, like those in use today, have on users? Does poor design discourage users from reading policies in the first place? Does poor design make users think that they have no power to protect their privacy regardless of what choices they make or settings they choose?

These questions are the next step in a growing literature on privacy policies, trust, and the propensity to disclose. Several studies have found that a website's data use policies matter: individuals are more willing to share their personal information with websites that have strict data-retention practices and promise to use customer data for very limited purposes.[190] This research also suggests that trust and sharing are linked: when we trust that a website will protect our privacy, we are more willing to share personal information with that platform.[191] But trust is based on more than just the substance of a website's data use disclosures. Individuals make trust and privacy decisions based on a slew of contextual and comparative factors, from the behavior of others to website design. It would be reasonable to conclude, then, that our propensity to share could be influenced by how a company's data use practices are presented.

2. Research Methodology

I designed a survey that asked respondents to choose one website over another based solely on images and descriptions of privacy policies and cookie notifications.[192] Part I collected basic demographic data, key baseline metrics, and their knowledge of privacy policies in general. Respondents selected age categories, gender, and education level, and how much time they spend online per day. They were then asked to select the social networking websites on which they maintain active profiles,

190. *See, e.g.*, Pedro Giovanni Leon et al., *What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers*, PROCEEDINGS OF THE NINTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 7 (2013), https://cups.cs.cmu.edu/soups/2013/proceedings/a7_Leon.pdf [perma.cc/RW35-REFQ].

191. *See, e.g.*, David Gefen & Paul A. Pavlou, *The Boundaries of Trust and Risk: The Quadratic Moderating Role of Institutional Structures*, 23 INFO. SYS. RES. 940 (2012).

192. The survey used Google Forms and was conducted through Amazon Mechanical Turk. A total of 576 unique Turkers took the survey. Twelve subjects were eliminated from consideration for completing the survey improperly. The entire survey had twenty-four substantive questions, including several on demographics.

where "active" referred to any website that respondents viewed or updated regularly. Ten of the most popular social networks were listed; the eleventh option was an "other" category. Respondents were also asked to select the e-commerce websites they regularly use; an "other" category was included, as well. Time online, number of social networking profiles, and number of e-commerce sites used help assess how "networked" an individual is, where higher uses correlated with an increased willingness to disclose personal information.

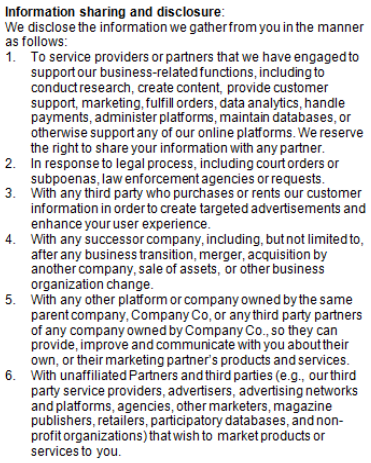
The next question asked respondents about their knowledge of privacy policies, in general. These questions were modeled on the research of Joseph Turow and others, and had correct and incorrect answers.[193] The survey listed seven statements about privacy policies and asked respondents to select which were true. The statements were, as follows: "If a website has a privacy policy, it means that . . . (1) the website cannot, by law, share my data with anyone else; (2) the website will get my permission before sharing my data with a third party; (3) the website gives me control over who sees my data; (4) I am protected if something goes wrong or if my data is hacked or released; (5) the website collected some information from me; (6) I can sue the website for misusing my data; (7) the website is, by law, required to do what it says in its privacy policy; (8) None of these statements are true." Together with sample demographics, the answers to this question can help us describe the kinds of internet users making disclosure choices.

Parts II through V measured how different visual designs of privacy policies affected users' preferences and trust.[194] Part II of the survey included five policy pairs, all of which were presented in traditional, user-unfriendly ways. But their content varied between protective and invasive data use practices. For example, a data use policy that respected consumer privacy would say: "We will never share your personal data with third parties without your express consent" or "We will always ask you before we share your data with someone else." An invasive data

193. *See* JOSEPH TUROW, MICHAEL HENNESSY & NORA DRAPER, THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 4-5 (June 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf [https://perma.cc/3BBK-ZVJC]; Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 723, 740 (2007), http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/FTC_and_privacy.pdf [https://perma.cc/24K8-3Q78]. *See also* Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR. (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is [https://perma.cc/T7JW-9BQ2].

194. Policies are too long to include in their entirety. *See supra* Part II.A. I recognize that length of the policy as a whole is a design technique that makes website data practices incomprehensible to the average internet user. An experimental interface could be designed to test website trust based on a full policy compared to a graphical presentation. This could be accomplished in future research.

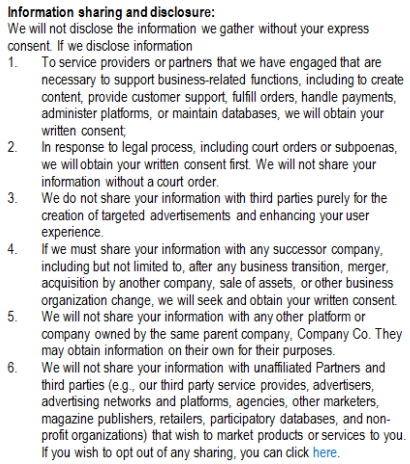
practice was described as follows: "We share information you provide to us and information we gather from your visit with our third-party partners" or "We will share your data with other websites." Figures 1 and 2 show two sample policies from this section of the survey.[195] The policy in Image 3 (with invasive data use practices) allows the company to do more with user data than the policy in Image 4 (with protective data use practices). The questions included images of policies along a range of protective to invasive practices.



Information sharing and disclosure:
We disclose the information we gather from you in the manner as follows:

1. To service providers or partners that we have engaged to support our business-related functions, including to conduct research, create content, provide customer support, marketing, fulfill orders, data analytics, handle payments, administer platforms, maintain databases, or otherwise support any of our online platforms. We reserve the right to share your information with any partner.
2. In response to legal process, including court orders or subpoenas, law enforcement agencies or requests.
3. With any third party who purchases or rents our customer information in order to create targeted advertisements and enhance your user experience.
4. With any successor company, including, but not limited to, after any business transition, merger, acquisition by another company, sale of assets, or other business organization change.
5. With any other platform or company owned by the same parent company, Company Co, or any third party partners of any company owned by Company Co., so they can provide, improve and communicate with you about their own, or their marketing partner's products and services.
6. With unaffiliated Partners and third parties (e.g., our third party service providers, advertisers, advertising networks and platforms, agencies, other marketers, magazine publishers, retailers, participatory databases, and non-profit organizations) that wish to market products or services to you.

Image 3



Information sharing and disclosure:
We will not disclose the information we gather without your express consent. If we disclose information

1. To service providers or partners that we have engaged that are necessary to support business-related functions, including to create content, provide customer support, fulfill orders, handle payments, administer platforms, or maintain databases, we will obtain your written consent;
2. In response to legal process, including court orders or subpoenas, we will obtain your written consent first. We will not share your information without a court order.
3. We do not share your information with third parties purely for the creation of targeted advertisements and enhancing your user experience.
4. If we must share your information with any successor company, including but not limited to, after any business transition, merger, acquisition by another company, sale of assets, or other business organization change, we will seek and obtain your written consent.
5. We will not share your information with any other platform or company owned by the same parent company, Company Co. They may obtain information on their own for their purposes.
6. We will not share your information with unaffiliated Partners and third parties (e.g., our third party service provides, advertisers, advertising networks and platforms, agencies, other marketers, magazine publishers, retailers, participatory databases, and non-profit organizations) that wish to market products or services to you.

If you wish to opt out of any sharing, you can click here.

Image 4

Respondents could choose to trust or do business with either website, select "I don't trust either of them," or select "I trust them both the same."[196] Answers to these questions should help us understand how users, when given the opportunity to choose between invasive or protective practices, respond to privacy policies today.

To test the impact of design, Part III of the survey varied designs, but kept the underlying data use practices constant.[197] Some designs

195. These designs were inspired by the design of most privacy policies today, but particularly by the New York Times's privacy policy. *See* Privacy Policy, N.Y. TIMES (June 10 2015), http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html [https://perma.cc/73GF-XUJD].

196. The survey explained that respondents should only choose "I trust them both the same" if they actually trusted both websites to protect their data.

197. From question to question, the practices changed, but within each question, the substance of the policies was identical.

were similar to those in Part I; others used strategies that elicited positive emotional responses from the privacy policy research team. Examples of pairings are seen in Images 5 and 6 below.[198]

Information we collect:

We collect information provided directly to us, such as personal information you provide when you visit our site, and information that is passively or automatically collected from you, such as information collected from your browser or mobile device and through cookies and web beacons.

- When you register for our services, which are required to do, we collect information from you, including your name, address, email address, telephone number, fax number, credit card information, and other information.
- We also collect information you provide, including name, address, email address, and telephone number, about other persons to whom you designate as recipients of our services.
- We, and our Partners, who include Company Affiliates, third party services providers, advertisers, and distribution or other partners, use automated means to collect various types of information about you, your computer, or other device used to access our Services. A representative, non-exhaustive list of the types of automatically collected information may include: network or internet protocol address and type of browser you are using, the type of operating system you are using, the name of your internet provider, domains used by such providers, mobile network, device identifiers, device settings, the web pages you have visited, our company's services visited before and after you visit this website, the type of handheld or mobile device used to view our website and whether you are viewing a mobile or standard version, geolocation information, and the content and advertisements you have accessed, seen, forwarded and/or clicked on. Please see our Section titled Cookies, and Other User and Ad-Targeted Technologies for more information about how the foregoing information may be collected and used.

Image 5

What information do we collect?

We collect the information you give us and some information automatically. This chart explains it.

	Info we **DO** collect	Info we **DON'T** collect	Notes
You Provide:	Name Address Phone & fax Credit card Other info, including info about other persons (name, email, phone)	We will not collect your passwords.	
Auto Collection:	IP address, browser type, ISP name, domains, mobile network, device type, browser settings, web browser history, our websites visited, geolocation info, & content of ads	We will not collect your passwords.	We use cookies and web beacons to passively collect data. You can view our Cookies, and Other User and Ad-Targeting Technologies section

Image 6

To test how design can positively or negatively affect user preferences, Part IV changed the pairings of designs and data use practices. Sometimes, user-friendly designs were paired with privacy-protective practices; in other questions, the designs displayed highly invasive practices. Images 7 and 8 are two examples of policies with user-friendly designs with very different data use practices.[199] Finally, Part V offered a potpourri of options, stepping out of the pattern of the previous sections, to ensure that respondents were answering honestly and not following a biased pattern.

198. The design of the policy in Figure 4 was based on Chase/JPMorgan's privacy policy, which deploys charts and shaded boxes. *See* U.S. Consumer Privacy Notice, CHASE (October 2014), https://www.chase.com/digital/resources/privacy-security/privacy/consumer-privacy-notice [https://perma.cc/2THE-H8SP]. The printed version of the policy, which is sent to all Chase customers per the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6803(a)(1)-(2) (2014), also uses charts. *See* U.S. Consumer Privacy Policy, CHASE (October 2014), https://www.chase.com/content/dam/chase-ux/documents/digital/resources/consumer-privacy-policy.pdf [https://perma.cc/SGP3-Z7P5].

199. Figure 5 comes from FitBit's privacy notice. Figure 6 is of my own design.

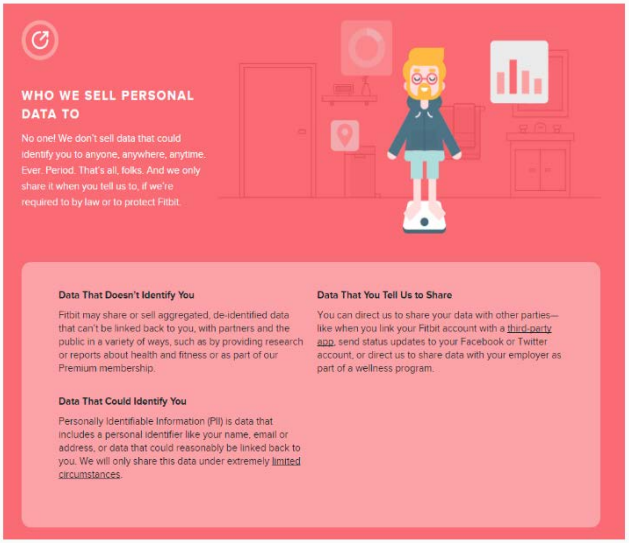


Image 7

Image 8

3. Results

The sample population can be characterized as follows: There were 564 valid responses ($n = 564$), of which 42% (235) were female and 58% (329) were male.[200] Users ages 18-24 constituted 19.5% of the sample; 25-34 year-olds made up just over 41%; 26% of the sample were 35-44 year-olds; 12.8% were 45 and older.[201] More than 81% of the sample reports that they are online more than three hours per day. The sample is highly educated, with 56% of respondents reporting that they at least graduated college. The sample is also relatively networked. Nearly half of the respondents maintain active profiles on three or more social networking sites.[202]

Hypothesis 1: The design of privacy notices has an impact on user trust, with user-friendly designs inspiring trust and a willingness to do business with a website even when the underlying data use policies are not protective of personal privacy.

Design had powerful effects, confirming this paper's hypothesis that notice design, perhaps more than content, influences our decisions to trust or do business with websites. In Part II, where content varied but all policies were designed like today's notices, it was common for respondents to not trust either website. Where designs changed, but content stayed the same, many respondents chose to trust the policy with a more pleasing, modern aesthetic. This was true even when attractive designs framed invasive data use practices.

In Part II, where all policies used traditional, user-unfriendly designs, "I don't trust either of them" was the most popular answer. When the substantive policies differed the most, as with Figures 1 and 2 above, most respondents (68%) could identify that the website represented by Figure 1 had more protective privacy and security practices. This suggests that when given the time and opportunity to read privacy policies, the substance of those policies factor into user determinations of trust.[203]

---

200. This departs somewhat from evidence that suggests Facebook users are more likely to be female. *See* MAEVE DUGGAN, PEW RES. CTR., MOBILE MESSAGING AND SOCIAL MEDIA 2015 10 (Aug. 19, 2015), http://www.pewinternet.org/files/2015/08/Social-Media-Update-2015-FINAL2.pdf [https://perma.cc/Y4KF-Z3MS].

201. The 25-34 year-old age bracket may be overrepresented, according to the best statistics available. *See* MAEVE DUGGAN ET AL., PEW RES. CTR., SOCIAL MEDIA UPDATE 2014 5 (Jan. 9, 2015), http://www.pewinternet.org/files/2015/01/PI_SocialMediaUpdate20144.pdf [https://perma.cc/2MC2-6C33]. *See also* Mark Hoelzel, *Update: A Breakdown of the Demographics For Each of the Different Social Networks*, BUS. INSIDER (June 29, 2015, 5:09 PM), http://www.businessinsider.com/update-a-breakdown-of-the-demographics-for-each-of-the-different-social-networks-2015-6 [https://perma.cc/GMV9-SEPX].

202. This is also in line with Pew findings. *See* Duggan et al., *supra* note 201.

203. *See, e.g.*, Leon et al., *supra* note 190. Kirsten Martin is also doing excellent work in

As the content of the policies started to change, however, respondents had trouble trusting one over the other. That difficulty was particularly acute in this section, where the policies were difficult to read. This remained true even when there were still significant differences. Between a policy that gave users a means of opting out and provided notice before any data sharing outside the company, and a policy that offered no choice, no notice, and substantial data tracking, 60.2% of respondents did not trust either website. Similarly, 57.4% of respondents did not trust either the notice and opt-out policy and the strict privacy policy in Figure 1. Some other factor, exogenous to content, is undercutting user trust.

In Part III, when the survey varied designs but kept the underlying policies identical, pleasing design had an impact on respondents. On average, more than five times as many respondents trusted the policy that used a chart to display information, as in Figure 4, over policies displayed like Figure 3.[204] By a ratio of more than eight to one, respondents also preferred a privacy policy designed with a modern aesthetic—sans serif font, large type, and 1.5x line spacing—over a standard policy.[205] At a minimum, this provides strong initial evidence that when users are given the opportunity to consider privacy policies, their design has a significant impact on the development of user trust in the platform.

Part IV varied designs and data use practices in three different questions. By putting design and substance together, this section tested how users react when competing companies have different data use practices and different designs. Fifty-eight percent of respondents favored a graphical, user-friendly privacy policy that permitted some information sharing across platforms, like Figure 5 above, over a traditionally designed policy that permitted none.[206] Only 21% trusted the platform with the policy that had the toughest privacy protections. The remaining respondents trusted neither or both the same. In the next question, a policy designed entirely with infographics, in varying color tones, and

---

this area. *See* Kirstin Martin, *Formal Versus Informal Privacy Contracts: Comparing the Impact of Privacy Notices and Norms on Consumer Trust Online* (Oct. 5, 2015) (unpublished manuscript), http://www.law.uchicago.edu/files/file/martin_formal_versus_informal_privacy_contracts.pdf [https://perma.cc/8C44-HBM6].

204. There were three questions that compared traditional policy design to charts. The policies designed as charts were preferred by 5.5 times (n_1=301, n_2=54), 5.1 times (m_1=314, m_2=61), and 5.5 times (p_1=270, p_2=49) as many respondents in each question. In each question, a large majority of total respondents preferred the policy that used a chart.

205. Though its design can certainly be improved, Uber deploys some of these design strategies in its privacy policy. *See User Privacy Statement*, UBER (July 15, 2015), https://www.uber.com/legal/privacy/users/en [https://perma.cc/A8VE-X8NS].

206. The graphical policy was an exact copy of FitBit's user-focused privacy policy. *See Let's Talk About Privacy, Publicly*, FITBIT, https://www.fitbit.com/privacy [https://perma.cc/V73E-HKPW].

with fifteen-point lettering that described wildly invasive data use practices (as in Figure 6) was trusted by 43% of respondents. Thirty-nine percent trusted a traditionally designed policy which promised to seek user consent before data sharing. Only 13% trusted neither. Finally, a cookie policy that presented in a pop-up menu was trusted by roughly the same number of respondents as a traditionally designed cookie policy with similar practices.

The final section offered a variety of pairings—same policies, different designs; different policies, same designs—that mixed designs with different practices. Two similar policies with almost identical language promising not to use cookies were designed differently: one used color and different columns, large type, and 1.5x line spacing, whereas the other typified traditional design. The former was preferred by 53% of respondents; the latter, by only 8.5%. The next question compared graphical design with extensive cookie use and data tracking, on the one hand, and traditional, user-unfriendly design with no cookie use and no data tracking. Respondents split: 40% trusted the site with the graphical design and the extensive user tracking; 38.2% trusted the restrictive policy with a traditional design. Between a pop-up notification that the website deployed cookies to track users and a user-unfriendly policy that promised no tracking or data sharing, users split again: 39% trusted the graphically designed pop-up; 40% trusted the strict policy in a traditional design.

Hypothesis 2: Those more educated about the law of privacy policies are less likely to be influenced by notice design.

Unfortunately, the data do not prove this hypothesis. I wanted to know if there is a relationship between certain categories or clusters of respondents as a way of making predictions about who is more or less likely to be influenced by design. For example, if we knew that users that are less educated about the law of privacy policies—namely, those large percentages of respondents who answered questions like Joseph Turow's True/False questions incorrectly—are more likely to let design influence them into making risky privacy choices, then we know that educating the public about what privacy policies can and cannot do could bring real meaning to notice and choice. The survey's introductory questions—covering background demographics and some basic True/False questions about the legal implications of privacy policies—were included for this very purpose.

Discriminant analysis was used to analyze the data. Discriminant analysis is often used to predict whether certain types of people are more or less likely to pass an exam or develop a disease based on a series of variables. More specifically, it helps determine if membership in a given group (older versus younger respondents or those who answered the True/False questions correctly versus incorrectly, for example) makes membership in another group (those influenced by design or

those ignored design and chose to trust policies with privacy protective practices, for example) more likely.[207]

The analysis did not find any statistically significant relationship. For example, I tried to identify if any characteristic—age, education, how many social networking sites one uses, education level achieved, income, and knowledge of privacy policy law—made it more likely that a respondent would choose to trust a website with the privacy policy in Figure 2 (current design, very limited data sharing) versus Figure 6 (colorful, graphic design with invasive data use practices). None of the variables tested explained the result. Nor did these variables explain the other choices in the survey with any statistical significance. This could happen for a number of reasons. First, these might not be the right classifying variables. Second, the impact of design could cut across demographic groups. Third, the sample set might not be large enough: of the 564 valid responses, only sixty-nine users, or 12%, answered the privacy policy True/False questions correctly. That subset may be too small to draw out any statistical relationships.

4. *Discussion*

The choices respondents made based on privacy policy design highlight several areas of concern for regulators, legislators, and online platform providers. That policies with the same underlying data use practices can create such radically different impressions among users casts doubt on the ability of a regime focused on content, readability, and conspicuousness alone to actually provide adequate notice. If websites are not effectively conveying information to the public, and if internet users are unable to process what is given to them, then notice and choice hardly has any meaning at all. Indeed, a significant difference in the levels of trust individuals had for websites with policies that were designed differently suggests, at a minimum, that privacy policy design is an important factor in consumer decisions to conduct online business. At worst, policy designs can also mislead the general public into making risky privacy decisions they would have otherwise opted against. If such deceit is intentional, it should be illegal.

The data suggest that current privacy policy design can lead to confusion, at best, or nihilism, at worst. Respondents chose "either" or "don't know" most often when deciding between two policies with different data use practices but with traditional, user-unfriendly designs, suggesting that traditional design made it harder to choose between two different policies. It may be the case that inscrutable design contributes to the popular view that there is no privacy online and nothing to be

207. Discriminant analysis is similar, though not identical, to logistic regression. Both are used to analyze data with categorical, as opposed to continuous, variables. Discriminant analysis assumes normal distribution of independent variables, which is the case in this data set (excluding gender, which, as a nominal variable, cannot be normally distributed).

done to fix it.[208] As the Pew Research Center has found, exceedingly small numbers of people express any confidence that information they share online will remain private and only a few feel that they have any control over how much information is collected about them and how it is used.[209] It is no wonder, then, that survey respondents expressed the same helplessness when faced with poorly designed policies.

The results of Part III of this survey show that when given the opportunity, respondents did take privacy policy design into account when making privacy choices. This makes sense given current research on the propensity to disclose.[210] That users consider design may be reason enough for regulators to include the design of privacy policies in their orders when enforcing notice and choice. A minority (28%) of the sample set could not choose between the options, suggesting that a small number may have actually read the policies and realized that the practices were the same. But most made a choice regardless of the similarity of the underlying disclosures. There are several possible conclusions to draw from this evidence. It is possible that the appealing designs created a more positive emotional reaction among respondents, and we know that feelings of happiness contribute to a greater willingness to share.[211] It could also be that some user-friendly designs can help inform. If so, there may be a strong market incentive for web platforms to make their privacy policies more user-friendly: increasingly savvy internet users may be more willing to share personal information when faced with a privacy policy designed to inform them, not confuse them.

Although user-friendly designs may sometimes be tools of transparency, they may also be tools of manipulation and coercion. In Parts IV and V of the survey, large percentages of respondents trusted websites with policies that included user-friendly design tools: charts, modern fonts, just-in-time pop-up notifications. Admittedly, respondents may have been primed to select policies with modern or clearer designs. Sometimes, though, users appeared to make risky privacy choices: for example, a large majority trusted the invasive policy with the pop-up cookie notification. This could be one example of users making an informed choice: they might have trusted the website, regardless of its invasive data practices, because it was honest about its behavior. But there is some evidence that modern, pleasing designs can actually help deceive users. Drop down Q&A-style policies hide part of the policy and structure information around specific questions, even when those questions

208. *See* MARY MADDEN & LEE RAINE, PEW RES. CTR., AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY, AND SURVEILLANCE 6-7, (May 20, 2015), http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf [https://perma.cc/7P32-FWPH].

209. *Id.* at 7.

210. John, Acquisti & Loewenstein, *supra* note 11.

211. Li et al., *supra* note 120.

might not be at the forefront of users' minds. Pop-up boxes can say one thing at the start of an online interaction and may be hedged or made less clear in a follow up policy. It may not be evident from this survey whether particular users were confused, fooled, or misled; but, at a minimum, it seems clear that design strategies can be forces for good, as in Part V, and for evil, as in some of the results of Part IV.

IV. EFFECTIVE NOTICE DESIGN

Whether obfuscated through unpleasant design or manipulated through graphical designs, these privacy policies constrain user freedom and choice.[212] Instead of staying silent, privacy regulators should address the deceptive capacity of design. With the help of the FTC, state privacy regulators, and federal and state legislation, internet users could start to reclaim control over their privacy online.[213]

Proposals for reforming notice and choice should adhere to three overarching principles. First, given that internet users, as Lessig and others have shown,[214] are constrained by the designs of digital environments, notice should reflect their embodied experience. That is, notice policy must consider how we actually make disclosure decisions and the myriad social, design, and contextual factors that limit or inform our free choice. Second, improving notice means making it more transparent for real users while limiting the coercive effects of design. Notice design can either enhance transparency or hinder it; effective reform must harness its illuminating potential. Finally, notice must actually work—namely, the effectiveness of notice reforms should be judged on their capacity to increase user knowledge of data use practices.

In this section, I discuss avenues for reform that meet these objectives. In particular, federal and state regulators must include transparency-enhancing design requirements when they enforce privacy law on the books. Corporations must also operationalize design on the ground by embedding the importance of the design of privacy notices among the lawyers and technologists that create and design them. Platforms that collect user data should design separate privacy notices just for users that reflect how users make disclosure decisions. And both regulators and platforms should engage in rigorous testing of notice designs to determine which designs foster understanding and which confuse and obscure. After detailing these proposals, I then conclude by responding to potential objections.

---

212. *See* FINDLEY, *supra* note 150, at 5.

213. *See id.* at 28 (arguing that when marginalized groups seek to reclaim control over a physical space, they are really engaging in a search for agency and freedom).

214. *See supra* notes 125-128.

A. *Considering Design in Privacy Law on the Books*

To ensure that user-oriented privacy policies are effective, privacy law on the books must consider design.[215] That starts by including design among the privacy norms that inform the law. Laws generally reflect powerful and persistent norms, societal and beyond.[216] This is especially true in privacy law, where the substantive norms expressed in the FIPPs have bled into law through FTC enforcement actions and state and federal mandates.[217] Leading influencers, including the FTC, state attorneys general, the Electronic Privacy Information Center, and consumer advocacy groups should include design recommendations in their best practice guides. This is starting to happen. The FTC has stated that disclosures by data collectors must be presented to users in user-friendly ways that make it easy for users to identify and understand their rights.[218] Former California State Attorney General Kamala Harris included more specific design requirements in her office's publications and best practice guides.[219]

When transparent design is among privacy's best practice norms, state and federal laws that mandate privacy policies should take the next step and require transparent and understandable policy designs. Federal statutes like COPPA, Gramm-Leach-Bliley, HIPAA, and the E-Government Act, and state laws from California to Delaware, could add design requirements to their substantive mandates. Implementing agencies could then issue rules on design. While these guidelines need not specify specific designs and aesthetics that must be used, it is not sufficient to simply suggest that notices use "visualizations" where possible.[220] As the above survey suggests, even seemingly user-friendly designs can be used in manipulative ways. These statutes and regulations have to start taking design seriously, recognizing that design and aesthetics are essential to conveying information to users.

---

215. Woodrow Hartzog's forthcoming book offers a blueprint for precisely how to do this. *See* HARTZOG, *supra* note 148.

216. ÉMILE DURKHEIM, THE DIVISION OF LABOR IN SOCIETY 24 (W.D. Halls trans. 1997) (noting how law both reflects and animates social norms).

217. *See supra* Part II.B. *See also* Rotenberg, *supra* note 81.

218. FED. TRADE COMM., PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 3-4 (2000), https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission [HTTPS://PERMA.CC/WY79-GLEH].

219. *See* CAL. DEPT. OF JUSTICE, PRIVACY PRACTICES, *supra* note 108, at 2, 4, 10 (recommending a layered format that calls attention to important rights). *See also* Citron, *supra* note 89, at n.20.

220. Regulation (EU) 2016/679 General Data Protection Regulation, 2016 O.J. (L119) 11. ("The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.").

And they would have precedent to follow. The Securities and Exchange Commission (SEC), for example, requires that prospectuses and other documents be written in "plain English"[221] so that investors and other members of the public can understand them.[222] A requirement of plain English is for more than simple prose. Rather, it considers design: "The right design choices make a document easier to read and its information easier to understand. The wrong design choices can make even a well-written document fail to communicate. . . . In a plain English document, design serves the goal of communicating the information as clearly as possible."[223] The SEC's Plain English Handbook discusses how to design effective section headings, what makes a readable font, why certain typefaces are more understandable than others, and how to determine the appropriate size to maximize readability.[224] It devotes several pages to document layout, discussing how to use white spaces effectively[225] and how appropriate line spacing can increase readability.[226] The Handbook's discussion of color reminds readers that for black-and-white documents, black is a color that can be leveraged to communicate with readers. Light-to-medium grays on white backgrounds, like those used in many online privacy policies today, would fail the SEC's "plain English" requirement.[227]

The Handbook also encourages the use of "simple" graphics and charts because they "often illuminate information more clearly and quickly than text."[228] In this vein, the Handbook quotes approvingly the work of Edward R. Tufte, a statistician and pioneer in the field of data visualization, who wrote a seminal treatise on how the design of a document can help improve reader understanding of complex data.[229] In that text, Tufte captured the importance of considering the design of privacy policies as a factor in providing adequate notice and choice to

---

221. *See* 17 C.F.R. § 230.421 (2016).

222. SEC. & EXCH. COMM'N, A PLAIN ENGLISH HANDBOOK: HOW TO CREATE CLEAR SEC DISCLOSURE DOCUMENTS [hereinafter, PLAIN ENGLISH HANDBOOK] 3 (1998), https://www.sec.gov/pdf/handbook.pdf [https://perma.cc/JF8T-QT2F] ("Investors need to read and understand disclosure documents to benefit fully from the protections offered by our federal securities laws. Because many investors are neither lawyers, accountants, nor investment bankers, we need to start writing disclosure documents in a language investors can understand: plain English.").

223. *Id.* at 37.

224. *Id.* at 38-42.

225. *Id.* at 44.

226. *Id.* at 46.

227. By way of example, Tinder Inc.'s and LinkedIn's privacy policies are both written in a light-to-medium gray on a white background. *See* Privacy Policy, TINDER, INC., https://www.gotinder.com/privacy [https://perma.cc/36YK-AL77]; Your Privacy Matters, LINKEDIN, https://www.linkedin.com/legal/privacy-policy?trk=uno-reg-guest-home-privacy-policy [https://perma.cc/PY7N-A76Y].

228. PLAIN ENGLISH HANDBOOK, *supra* note 222, at 49-50.

229. *Id.* at 49.

consumers: "Graphical excellence is that which gives to the viewer the greatest number of ideas in the shortest time with the least ink in the smallest space. . . . And graphical excellence requires telling the truth about data."[230] User-friendly designs, which include proper typefaces choices, effective use of white spaces, and simple graphics, can help websites communicate privacy protective practices. When they are used to obfuscate or hide, however, they are tools of deception.

Nor is the SEC alone in considering the design of a document relevant for its legal validity. Contract and employment law have recognized the importance of design for some time. In *Carnival Cruise Lines v. Shute*,[231] a case involving the enforceability of a forum selection clause written in tiny print on the back of a passenger ticket,[232] Justice Stevens argued that a consumer cannot be "fully and fairly notified" about the substance of the provision when it is written in "fine print on the back of the ticket" in the eighth of a twenty-five-paragraph contract.[233] The design, likely employed to keep consumers uninformed, reminded Justice Stevens of contracts of adhesion at common law: the cruise line designed the contract the way it did to give consumers "little real choice," thus invalidating the consumer's supposed consent.[234] In an opinion written by Judge Skelly Wright, the D.C. Circuit held that incomprehensible design, typified by the tiny fine print by which no reasonable consumer could be informed, could make a contract unconscionable.[235] Similarly, states have passed laws with design requirements where the goal is conveying information to real people. For example, South Carolina mandates particular design requirements for disclaimers in employee handbooks.[236] California prescribes both the design and content of arbitration agreements.[237]

The Consumer Financial Protection Bureau (CFPB) has gone even

230. *Id.* at 51.

231. Carnival Cruise Lines v. Shute, 111 S.Ct. 1522 (1991).

232. *Id.* at 1534-38 (Stevens, J., dissenting) (appending copies of the ticket in question).

233. *Id.* at 1529.

234. *Id.* at 1531.

235. Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449-50 (1965). *See also In re* Real Networks, Inc., Privacy Litigation, 2000 WL 631341, No. 00 C 1366, *5 (N.D. Ill. May 8, 2000) (dictum; "burying important terms in a 'maze of fine print' may contribute to a contract being found unconscionable").

236. S.C. CODE ANN. § 41-1-110 (West 2016) ("a disclaimer in a handbook or personnel manual must be in underlined capital letters on the first page of the document and signed by the employee. For all other documents referenced in this section, the disclaimer must be in underlined capital letters on the first page of the document.").

237. CAL. CIV. PROC. CODE § 1295 (West 2016) ("(b) Immediately before the signature line provided for the individual contracting for the medical services must appear the following in at least 10-point bold red type: 'NOTICE: BY SIGNING THIS CONTRACT YOU ARE AGREEING TO HAVE ANY ISSUE OF MEDICAL MALPRACTICE DECIDED BY NEUTRAL ARBITRATION AND YOU ARE GIVING UP YOUR RIGHT TO A JURY OR COURT TRIAL. SEE ARTICLE 1 OF THIS CONTRACT.'").

further, embracing the symbiotic relationship between design and notice in several ways. It requires that credit reports be designed to enhance transparency and readability. Its Design+Technology program recruited graphic designers to, among other things, create "[d]esign tools that enable millions of people to make informed financial choices."[238] And it follows an open source Design Manual for its own documents.[239] This Manual, which provides guidance on anything from the CFPB color palette[240] to typography and different types of icons, is used to create "honest, transparent design that wins the public trust" and empowers users.[241] Those goals—honesty, transparency, and trust—have long been features of the Fair Information Practices and the notice-and-choice regime that emerged from them. Privacy regulators could learn lessons from the CFPB, and securities and contract law to incorporate similar design requirements in their regulations.

B. Considering Design on the Ground

Including design considerations in privacy norms and statutes is an important first step. But, as Kenneth Bamberger and Deirdre Mulligan have argued, what happens on the ground, where technology companies operationalize laws into practice, also matters.[242] Technology companies need to prioritize design as an important element of privacy notices—from the executive level all the way down to the lawyers writing privacy notices and the designers building new technology products.[243]

In their book *Privacy on the Ground*, Bamberger and Mulligan found

---

238. Chris Willey, *Design+Technology Fellows: Changing the Way Government Works*, CFPB BLOG (June 21, 2012), http://www.consumerfinance.gov/about-us/blog/designtechnology-fellows-changing-the-way-government-works/ [https://perma.cc/MB59-SFMT].

239. CFPB DESIGN MANUAL, CONSUMER FIN. PROT. BUREAU, https://cfpb.github.io/design-manual/index.html [https://perma.cc/DA5E-3T4D].

240. *Color*, CFPB DESIGN MANUAL, CONSUMER FIN. PROT. BUREAU, https://cfpb.github.io/design-manual/identity/color-principles.html [https://perma.cc/ML3C-TDN6].

241. *Design Principles*, CFPB DESIGN MANUAL, CONSUMER FIN. PROT. BUREAU, https://cfpb.github.io/design-manual/guides/design-principles.html [https://perma.cc/H5JZ-2F8J].

242. *See* Kenneth Bamberger & Deirdre Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (2015). Bamberger and Mulligan also published their initial research and preliminary arguments in the Stanford Law Review. *See* Kenneth Bamberger & Deirdre Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011), https://www.stanfordlawreview.org/print/article/privacy-on-the-books-and-on-the-ground [https://perma.cc/WAU5-37QG].

243. Bamberger and Mulligan's research focused primarily on chief privacy officers and executive-level privacy leads. Although their work was groundbreaking, it left open the question of how, if at all, engineers, computer programmers, web designers, and others integrate privacy considerations into product design. That is the subject of forthcoming work on embedding privacy norms throughout a company. *See* Ari Ezra Waldman, *Trickle Down/Up Privacy* (forthcoming).

that empowered Chief Privacy Officers (CPOs) are creating dynamic, forward-looking privacy practices that put user trust first.[244] Several CPOs talked about their jobs in fiduciary terms: they saw themselves as "steward[s]" of data and "responsibl[e]" to consumers[245] and believed that their primary objective was creating and maintaining "the company's trusted relationship" with customers, employees, and society.[246]

If that is the case, privacy notices have not been part of that worldview. As discussed above, today's notices are difficult to read and may deploy unpleasant design techniques that actually deter users from learning about a website's data use practices. And there is evidence to suggest that those involved in developing privacy policies do not take their design seriously. Lawyers draft them for regulators;[247] engineers do not really care about them.[248] This is unfortunate. As Paula Bruening and Mary Culnan have argued, the design of notices should be fully integrated into system development rather than an afterthought.[249] This means more than creating a policy or hosting engineers for a half-day assembly about the importance of privacy, as many technology companies do with their new tech hires. Rather, corporations need to embed notice design considerations into the organizational ethos, practice, and routine.[250]

---

244. Bamberger & Mulligan, *Privacy on the Ground*, *supra* note 242, at 6.

245. *Id.* at 66. Many scholars, including Daniel Solove, Jack Balkin, Jonathan Zittrain, Danielle Citron, and others, have recommended a shift toward a fiduciary or trustee model to ensure corporations take consumer privacy seriously. Notably, scholars suggested that changes to law on the books would be necessary before any such fiduciary relationship took hold. *See, e.g.*, Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* 102-03 (2004) (positing that businesses that are collecting personal information from us should "stand in a fiduciary relationship with us"); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 UC DAVIS L. REV. 1183, 1186 (2016) ("[M]any online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries toward their customers and end-users."); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016, 9:48 AM), http://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://perma.cc/S9ZK-6XVK]; Danielle Citron, *Big Data Brokers as Fiduciaries*, CONCURRING OPS. (June 19, 2012, 5:08 PM), http://www.concurringopinions.com/archives/2012/06/big-data-brokers-as-fiduciaries.html [https://perma.cc/8DV4-TUXQ] (arguing that a fiduciary relationship between data brokers and users would help fight the massive power imbalance that exists in today's unregulated environment).

246. Bamberger & Mulligan, *Privacy on the Ground*, *supra* note 242, at 67.

247. Telephone interview with "Privacy Attorney at AmLaw Top 50 Law Firm" (name redacted per wishes of interviewee), Mar. 16, 2016 (notes on file with author).

248. Telephone interview with "Google Engineer" (name redacted per wishes of interviewee), Sept. 12, 2016 (notes on file with author).

249. Paula J. Bruening & Mary J. Culnan, *Through a Glass Darkly: From Privacy Notices to Effective Transparency*, 17 N.C. J. L. & TECH. 515, 547-52 (2016).

250. I expand on this in Ari Ezra Waldman, *Designing Without Privacy*, 50 HOUSTON L. REV. __ (forthcoming 2018) and in a forthcoming book of the same name. *See generally* Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and*

One manifestation of considering design, and perhaps the best way to provide effective, transparent notice, is to have separate notices just for users. Based on Danielle Citron's research into the privacy enforcement strategies of state attorneys general, this appears to already be the policy of the State of California.[251] But most rules governing user-focused notices today stop at recommending brevity and conspicuousness. We must go further. We have to demand transparency-enhancing design.

As Bruening and Culnan demonstrate, we already know a little bit about the effects of such designs.[252] Among the proposals tested have been standard "nutrition label"-style standard notices,[253] the Gramm-Leach-Bliley notice form,[254] and layered notices. These solutions are not perfect. Researchers at Carnegie Mellon University found that standardization may have made it easier to compare data use practices across platforms, but it also required companies to omit certain information or describe their practices less clearly.[255] Layered notices were also imperfect: ordinary users were able to process information from layered notices faster than from long forms, but they were not as accurate.[256] Table formats tend to be most effective at conveying information.[257] What these researchers did not test, however, was whether

---

Collective Rationality in Organizational Fields, 48 AM. SOC. REV. 147 (1983) (describing, among other things, how organizations tend to act out of a desire to achieve legitimacy rather than productivity); Martha S. Feldman & Brian T. Pentland, *Reconceptualizing Organizational Routines as a Source of Flexibility and Change*, 48 ADMIN. SCI. Q. 94 (2003) (arguing that organizational routines can actually encourage creative decision making and change); Andrew C. Inkpen & Eric W. K. Tsang, *Social Capital, Networks, and Knowledge Transfer*, 30 ACAD. MGMT. REV. 146 (2005) (discussing the structural elements of an organization that can enhance learning and adaptation).

251. *See* Citron, *supra* note 89, at 20 & n.122.

252. Bruening & Culnan, *supra* note 249.

253. Although some commentators have called for a privacy "nutrition label" that standardizes privacy policy design, *see, e.g.*, Anthony, *supra* note 106, a single uniform design has not gained traction among legislators and regulators. *See also* NAT'L TELECOMM. AND INFO. ADMIN. SHORT FORM NOTICE CODE OF CONDUCT TO PROMOTE TRANSPARENCY IN MOBILE APP PRACTICES, (July 25, 2013), https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf [https://perma.cc/FU96-4TGX].

254. *See* Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62890 (West 2016).

255. *See* Lorrie Faith Cranor et al., *Are They Actually Any Different? Comparing Thousands of Financial Institutions' Privacy Policies*, WEIS 2013, http://www.econinfosec.org/archive/weis2013/papers/CranorWEIS2013.pdf [https://perma.cc/9UGQ-TDFY] (*cited in* Bruening & Culnan, *supra* note 249, at 557).

256. *See* Aleecia M. McDonald et al., *A Comparative Study of Online Privacy Policies and Formats*, *in* PRIVACY ENHANCING TECHNOLOGIES: 9TH INTERNATIONAL SYMPOSIUM, PETS 2009, SEATTLE, WA, USA, AUGUST 5–7, 2009, 37–55 (Ian Goldberg & Mikhail J. Atallah eds., 2009) (*cited in* Bruening & Culnan, *supra* note 249, at 551-2).

257. *See* Patrick Gage Kelley et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, CARNEGIE MELLON CYLAB, 6-7 (Jan. 12, 2010), https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf

certain designs lent themselves naturally to transparency and whether other designs were more effective at obfuscation. Either way, designing user-focused privacy notices to reflect the embodied experiences of real users is a step in the right direction.

I argue that we should go further than Gramm-Leach-Bliley's charts or standard, dubiously effective,[258] nutrition labels. FitBit's privacy notices are good examples of policies geared toward two different audiences — users and regulators — where the former uses graphics to convey information. The landing page for www.fitbit.com/privacy is not a long, contract-like privacy policy, but rather a graphical, continuous scrolling page that explains data use practices to users. Letter size is large, line spacing is 1.5, and graphics and brand colors are used to enhance understanding. Compared to the company's long form privacy policy, which is 3,535 words long but deploys large lettering and headers and a modern aesthetic, the user-focused version is both an accurate and clear representation of FitBit's data use practices.

This also suggests that we should engage in rigorous testing to determine the effect of certain designs on user choices. This would ensure that the embodied experience of users is reflected in the design of privacy notices. Such testing could inform notice design on the ground, policy, and enforcement. For example, privacy professionals and regulators could make informed design recommendations if studies show that charts and graphical displays are effective at conveying accurate information quickly. Platforms can also beta test their notices with users. Regulators can deploy consumer testing to evaluate notice design during investigations of manipulative practices.[259] Developing experimental studies to determine the impact of notice design on user comprehension is the next step in this research.

C. Responses to Objections

Some may object to this proposal by suggesting that it saddles privacy regulators with the burden of being art critics. A common rejoinder in the copyright sphere,[260] this argument suggests that letting a rather unrepresentative cadre of regulators or judges determine whether

---

[https://perma.cc/P4B2-MLPW].

258. *See, e.g.*, Delvina Gorton et al., *Nutrition Labels: A Survey of Use, Understanding and Preferences Among Ethnically Diverse Shoppers in New Zealand*, 12 PUB. HEALTH NUTRITION 1359, 1363-64 (2008).

259. We do this now in the trademark context. Counsel commission surveys of user confusion when arguing for or defending against a claim of trademark infringement. *See generally, e.g.*, Shari Seidman Diamond & David J. Franklyn, *Trademark Surveys: An Undulating Path*, 92 TEX. L. REV. 2029 (2014).

260. *See* Bleistein v. Donaldson Lithographing Co., 188 U.S. 239, 251 (1903) ("It would be a dangerous undertaking for persons trained only to the law to constitute themselves final

designs are user friendly or not will unfairly narrow the artistic options open to privacy policy designers. Determining what is art, however, is not at issue in privacy policy design. Rather, the question is: Is this policy's interface designed to help users understand the content within or is it designed to deceive or hide information? Armed with guidance from federal agencies like the SEC and the CFPB, more detailed recommendations from state attorneys general offices, evidence of the ways designs can manipulate consumers, and the results of field tests of actual notice designs, regulators can make general assessments about a particular privacy policy design on a case-by-case basis.

Another objection might be that privacy regulators lack the authority to police what notice looks like. This is certainly not the case when it comes to state attorneys general. Considering manipulation-by-design is also well within the scope of the FTC's authority to regulate unfair and deceptive business practices. As Daniel Solove and Woodrow Hartzog have shown, the FTC has developed a general theory of deception that includes tactics that induce consumers to disclose personal information.[261] Under this theory, the FTC has moved against companies that have induced disclosure by making misleading phone calls,[262] phishing,[263] and suggesting that they are affiliated with trusted entities.[264] Inducement through manipulative privacy policy design may be more subtle than calling customers on the phone, but the tactic is no less deceptive.

A third objection to requiring privacy regulators to consider privacy policy design is that it would infantilize internet users, absolving them of responsibility for their choices. This argument is based on personal responsibility and harkens back to the autonomous user at the heart of notice and choice today: Privacy policies are ubiquitous and, as such, consumers should be aware that statements of data use practices exist for them to consider before sharing their personal information. If they

judges of the worth of pictorial illustrations"); Brandir Int'l Inc. v. Cascade Pac. Lumber Co., 834 F.2d 1142, 1145-46 n.3 (2d Cir. 1987) ("[W]e judges should not let our own view of styles of art interfere with the decision-making process in this area.").

261. *See* Solove & Hartzog, *supra* note 5, at 630.

262. Complaint for Permanent Injunction and Other Equitable Relief at 5-6, FTC v. Sun Spectrum Comm'ns Org., Inc., No. 03-CV-8110 (S.D. Fla. Dec. 2, 2003), http://www.ftc.gov/sites/default/files/documents/cases/2004/01/031202cmp0323032.pdf [https://perma.cc/Z8CH-ADQB] (*cited in* Solove & Hartzog, *supra* note 5, at 632).

263. Complaint for Permanent Injunction and Other Equitable Relief at 6-9, FTC v. [a Minor], No. 03-CV-5275 (C.D. Cal. July 23, 2003), http://www.ftc.gov/sites/default/files/documents/cases/2003/07/phishingcomp.pdf [https://perma.cc/3HNK-6ZHP] (*cited in* Solove & Hartzog, *supra* note 5, at 632-33).

264. Complaint for Injunctive and Other Equitable Relief at 22-23, FTC v. Assail, Inc., No. W03CA007 (W.D. Tex. Jan. 9, 2003), http://www.ftc.gov/sites/default/files/documents/cases/2003/01/assailcmp.pdf [https://perma.cc/PEY7-682S] (*cited in* Solove & Hartzog, *supra* note 5, at 633).

choose not read the policies, consumers assume the risk that their data could be used in ways they did not expect.[265] But holding individuals responsible for assuming the risks of disclosures requires voluntary assumption of that risk. Privacy policy design is one factor that has been constraining user freedom and choice online because the designs may manipulate users into sharing their personal data. As with contracts of adhesion, then, the choice was not free to begin with.[266]

V. CONCLUSION

Additional research is necessary to flesh out the details of this proposal. Although this Article suggests that design can induce consumers to make risky privacy choices, it has treated all user-friendly designs as fungible. Further research is needed to determine if certain designs are better at informing readers than others. Although several images of privacy policies in the survey above used so-called "just in time" disclosures, the survey did not test the effect of disclosure timing on user trust and willingness to disclose. Nor did this study address any deceptive design strategies beyond the four corners of a website's privacy policy. There are significant opportunities for further research.

In particular, there are two additional research projects that can help scholars, policymakers, and privacy professionals redesign privacy notices. First, we need to learn how, if at all, norms about privacy trickle down from privacy leads to the designers, programmers, and engineers responsible for product development. Second, we need a model for testing the relationship between notice design and user comprehension of data use practices. These are the subjects of my forthcoming research.

This article argues for incorporating privacy policy design in privacy law's assessment of adequate notice and choice. I have shown that most privacy policies today are not designed with real users in mind. This may be because design has generally been absent from most privacy norms, FTC enforcement actions, and federal and state laws that envision or mandate privacy policies. The article has also provided both theoretical and empirical bases for believing that privacy policy design can indeed manipulate consumers into giving up their personal data.

---

265. *See, e.g.*, Dwyer v. American Express, Co., 652 N.E.2d 1351 (Ill. App. 1995) (finding that American Express cardholders assumed the risk that their data would be disclosed to third parties because, in relevant part, they agreed to the company's terms of service and willingly provided financial and consumer information in the course of use).

266. "Implicit in the concept of assumption of risk is some notion of choice. . . . [U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." Smith v. Maryland, 442 U.S. 735, 749 (Marshall, J., dissenting) (citations omitted).

Privacy policies are designed in that they deploy an underlying structure. They can bury invasive data use practices in 20-page documents written in a 7-point font with minimal margins. Or they could be part of a designed interface that helps users understand what will happen with their data so they could make informed privacy choices. Like painters who use line, color, contrast, and perspective to help guide their audiences through a visual narrative, privacy law and privacy policy designers must do this, too.