Privacy, Notice, and Design

Ari Ezra Waldman*

Design is everywhere. It 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. Design, therefore, poses dangers and offers opportunity to protect privacy online. 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 designed 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 design. 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, Adam Oestreicher, 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.

INTRODUCTION

Critical accounts of privacy notices focus, among other things, on confusing language,[1] inconspicuousness,[2] and inscrutability.[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 the design of privacy policies.

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] difficult to understand,[8] and inaccessible. Even experts find them misleading.[9]

---

[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*") (this "undermines the ability of privacy policies to effectively convey notice of data practices to the general public").

[2] Janice Y. Tsai, Serge Egelman, Lorrie Cranor, & Alessandro Acquisti, *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* Mark S. Ackerman, Lorrie Faith Cranor, & Joseph Reagle, *Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences*, ACM CONFERENCE ON ELECTRONIC COMMERCE (1999); 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 (JEFFREY K. MACKIE-MASON & DAVID WATERMAN EDS. 1998).

[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, 490-6 (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.*, 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), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465; 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 (2004).

[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. 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 he or she encountered. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543, 563 (2008).

[8] *See* Mark A. Graber, Donna M. D'Alessandro, & Jill Johnson-West, *Reading Level of Privacy Policies on Internet Health Web Sites*, 51 J. OF FAMILY PRACTICE 642, 642 (2002).

[9] Reidenberg et al, *Privacy Policies*, *supra* note 1, 87-88.

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. This is because they are designed without the needs of real people in mind. Privacy policies are written by lawyers and for lawyers.[10] Privacy law, for the most part, has exacerbated the problem. It primarily mandates the content of notice and ignores how that content is conveyed: for example, 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.[11] 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.[12] Rather, we are embodied, situated users who make choices based on context.[13] Proposals like ameliorating term ambiguity[14] or locating policies in more noticeable places[15] are fine starts: they recognize that, at a minimum, content isn't king. But those 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 as users are limited and constrained by the design of the digital spaced 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 various scholars have argued, design configures users, limiting our

---

[10] *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE __ (2015); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, ___ (2011). Bamberger's and Mulligan's remarkable study looked at the relatively new role of the "chief privacy officer" and other privacy professionals in the implementation and development of privacy law, in general. In forthcoming research, I discuss the role of the relationships between privacy lawyers and programmers, designers, and engineers in the design of privacy policies. *See* Ari Ezra Waldman, *Notice and Design on the Ground* (forthcoming).

[11] *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.*, Decision and Order at 2, In re Sony BMG Music Entm't, FTC File No. 062 3019, No. C-4195 (F.T.C. June 29, 2007), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019do070629.pdf; Cal. Bus. & Prof. Code § 22575(b)(1) and (3) (CalOPPA's clear and conspicuous link requirement). But 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 focus of the lion's share of enforcement is content.

[12] 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) (online disclosure decisions are not rational).

[13] *See* Julie E. Cohen, *Cyberspace As/And Space*, 107 COLUMB. L. REV. 210, 225-7 (2007).

[14] Reidenberg et al., *Privacy Policies*, *supra* note 1, 87-88.

[15] Janice Y. Tsai, Serge Egelman, Lorrie Cranor, & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 254, 266-67 (2011).

freedom in ways predetermined by the designer.[16] 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.[17] Furthermore, design is not neutral. Much like designing public spaces to be welcoming or hostile to users,[18] design can discourage us from reading privacy notices, make them transparent, or coerce us into mismanaging our privacy contrary to our 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.[19] By designing policies so no reasonable user could ever read, process, and understand them,[20] 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 first-of-its-kind study 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 has been left largely undocumented. This Article attempts to fill that gap, proceeding as follows: Part I discusses notice-and-choice today. It reports on the results of an informal canvas of current policies and argues that these notices are 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.

---

[16] *See, e.g.*, LUCY A. SUCHMAN, HUMAN-MACHINE RECONFIGURATION 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 13, at 210, 221, 225, 233-36 (2007).

[17] *See infra* Part II.A. *See also* Neal Katyal, *Architecture as Crime Control*, 111 YALE L. J. 1039 (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").

[18] *See* 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).

[19] This is not my phrase. *See id. See also* Roman Mars, Unpleasant Design & Hostile Urban Architecture (July 5, 2016), http://99percentinvisible.org/episode/unpleasant-design-hostile-urban-architecture/ (last visited July 14, 2016).

[20] 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* Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH. L. 273, 274 (2012). That is about 54 billion hours per year. *See* McDonald & Cranor, *supra* note 7, at 563.

Part II relies on socio-legal scholarship on configuring the user and the social construction of technology to challenge that conception of the user. This section concludes by discussing and analyzing the results of an empirical study on the impact of privacy policy design on user disclosure decisions.

Part III 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. And the FTC should investigate internet companies that design their privacy policies to deceive users. With respect to the on the ground implementation of notice and choice, this research recommends several strategies for online platforms, including increased 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.

I. 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. But at the time, 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 was misused. Plaintiffs tried privacy torts, but to no avail.[21] Frustrated users even turned to statutes originally intended to regulate wiretapping.[22] Again, they failed.

Privacy policies have since become ubiquitous, developing first as industry's way to stave off regulation[23] and spreading further under state and federal

---

[21] *See, e.g.*, 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). *See also* Solove & Hartzog, *supra* note 5, at 590-2 (2014). There are four so-called "privacy torts," as defined in William Prosser's article, *Privacy*, in the California Law Review: 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 (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 Confidentiality*, 96 GEO. L. J. 123 (2007).

[22] In re DoubleClick, Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (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); Brief on Rehearing En Banc for Senator Patrick J. Leahy as Amicus Curiae Supporting the United States and Urging Reversal, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc) (No. 03-1383).

[23] 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

mandates.[24] 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 and give us the opportunity to opt out. That sounds reasonable. But for some time, privacy policies have been under attack. It is impractical, the argument goes, for ordinary users to read long and complex privacy notices littered with legal terms.[25] We should instead rely on visceral forms of notice[26] or a website's user-controlled privacy settings to set platform privacy obligations.[27] These critiques and proposals have considerable merit. But ever since the earliest iterations of privacy norms, some form of notice has always been at the top. And 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 on the ground and in the books. 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 in 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, regulatory enforcement, and practice guides. 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. And 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.[28] We identified several design-related characteristics, including aesthetics

---

by websites"). *See also* Solove & Hartzog, *supra* note 5, at 593-4; 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).

[24] *See infra* Parts I.B.3 and I.B.4.

[25] *See* Cranor, *supra* note 20, at 274; McDonald & Cranor, *supra* note 7, at 563.

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

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

[28] The raw data is available online at the Data Privacy Project, New York Law School. 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 II.B. I recruited 10 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

(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, and contrast between text color and background, use of charts or icons), notification timing, the existence of privacy "centers" and Frequent Asked Questions, and layering, 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 written 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).

The longest policy, from Ceasar's Entertainment, was 9,965 words and took 20 seconds of continuous scrolling to reach the end.[29] At 248 words, the online technology magazine, "How to Geek," had the shortest privacy policy.[30] 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 on first glance.[31] 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; 5 policies required postal mail. Only 4 policies included charts providing clear, easy to understand information. One hundred and fifty seven policies, or 82%,

---

frequently, regularly, or somewhat regularly. I imposed two limitations. First, no more than 2 websites could be of the same type—namely, no more than 2 news sites, 2 social networking sites, 2 e-commerce sites, 2 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.

[29] Try it. Twenty seconds is a long time. *See* Privacy, Caesar's Entertainment, http://caesarscorporate.com/privacy/?_ga=1.200037294.1872875718.1467234380 (last visited June 29, 2016).

[30] It was also the funniest privacy policy we saw. *See* How to Geek, Privacy Policy, http://www.howtogeek.com/privacy-policy/ (last visited June 29, 2016) ("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.").

[31] The definition of the word "noticeable" already encompasses ease. *Noticeable*, Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/noticeable.

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.[32]

Less than 20% of the websites reviewed included popup 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—Facebook—had anything akin to a "privacy center" where users could manipulate and make changes to their privacy settings.[33] Even these settings were designed to mislead users into thinking they had control over their data on the platform.[34]

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 made even harder to understand when they are 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. The privacy policy survey discussed below tests that hypothesis.

Some anecdotal evidence alludes to this nihilism. In addition to coding and analyzing each privacy policy's design, my team of researchers offered their general impressions on how the website's interface presents its privacy policy. Positive emotional responses—"This was easy to read," "I didn't mind this one," or "This one was the best of all the ones I read," for example—were associated with privacy policies that had several common characteristics: pop-up notifications, wide line spacing, varied colors, large print, and strong color contrast. Policies that had a more modern aesthetic—large sans serif fonts, significant white space, and functional drop down menus, for example—were also associated with positive impressions, as well. One researcher even volunteered that user friendly designs "made [her] feel better about the website in general." Another student went so far as to say, "I trust this website more." Policies that were difficult to read elicited exasperation from the research team: "I just couldn't get through this one," "It was only about 1,000 words but it felt like pages and pages of reading," "My eyes hurt. My heart hurt with this one," and "Who thought 7-point font was a good idea. My mom can barely read 12!" These initial, off-the-cuff reactions from students who had taken a course in Information Privacy Law, volunteered for the research assignment, and had

---

[32] FitBit, the wearable activity tracker, is one of them. However, FitBit does not just use icons. It 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* FitBit, Let's Talk About Privacy, Publicly, https://www.fitbit.com/legal/privacy (last visited June 29, 2016).

[33] *See* Privacy Settings and Tools, https://www.facebook.com/settings/?%20tab=privacy (last visited July 14, 2016).

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

significant background knowledge in consumer privacy may hint at even more negative responses from the general population of Internet users.

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 is another questions at the heart of the privacy policy survey discussed in Part II. 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? But platforms may not be *designing* privacy policies at all; design does not appear to be a 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 explanation speaks to an oversight, not deception. A 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 in the books is factor. In the next section, I show that privacy law has generally ignored the impact of design on disclosure decisions, focusing instead on privacy policy content. As such, it has failed to generate and embed notice design as an important norm among privacy professionals.

B. Privacy Policies in the Books

Today's privacy policies are manifestations of federal and state data privacy law that focuses almost exclusively on a what-when-how of user data: websites have to disclose *what* data is collected, *when* it is collected, and *how* it is used. In other

---

[35] Trust is an essential part of a user's willingness to disclose information or do business with a website. *See* Ari Ezra Waldman, *Privacy, Sharing, and Trust*, 67 CASE W. RES. L. REV. __ (forthcoming 2017) (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 whom we trust); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STANFORD TECH. L. REV. __, at 37-41 (forthcoming 2016), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2655719 (protecting privacy can build trust between online platforms and consumers). *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.

[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, *Notice and Design on the Ground* (in progress). So far, 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 15 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 Fred Jennings of Tor Ekeland, P.C., Mar. 26, 2016 (notes on file with author).

[38] *See* SAVICIC & SAVIC, *supra* note 18 (collecting examples of designs of public spaces that discourage antisocial behavior).

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 40 years ago, when data privacy principles were first articulated.

1. Fair Information Practices

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 (FIPs), which developed out of a 1973 report from the federal Department of Housing, Education, and Welfare (HEW),[39] recommended that users be told of an entity's data use practices, that they should have the opportunity to correct their data, and that they should have to consent to any secondary uses of their information.[40] Several years later, the Organization for Economic Cooperation and Development issued similar guidelines, requiring, for example, that data gatherers disclose the purpose and scope of data collection, any security protocols, and all user rights.[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]

In so doing, the FTC identified "notice" as the most important FIP. 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 Dan Solove and Woodrow

---

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

[40] HEW Report, *supra* note 39, at 41-42.

[41] ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD), OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2001), *available at* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[42] FTC, PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON "PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE", BEFORE THE SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION § III(1) (May 25, 2000), http://www.ftc.gov/os/2000/05/testimonyprivacy.htm.

Hartzog point out, organizations such as TRUSTe took the FIPs and the FTCs recommendations to heart, issuing privacy "seals" based on a website's compliance. TRUSTe would award one of its coveted seals if the 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 lay person—was less important.

2. The FTC Focuses on Substance

Federal Trade Commission enforcement actions have been one path through which the substantive privacy norms expressed in the FIPs translated 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] 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 both in 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—"Personal information voluntarily submitted by visitors to our site … is never shared

---

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

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

[45] *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2114 (2004) ("the 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] 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, please see CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 135-305 (2016) and Solove & Hartzog, *supra* note 5, at 627-66.

with a third party"[48]—and does the opposite. In *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 a different broken promise. An online toy store, Toysmart.com collapsed after the dot-com boom, ceasing operations in May 2000.[52] Its privacy policy stated that the company would never share customer information with any third party.[53] But during bankruptcy, Toysmart sought permission to auction off a trove of customer data—purchase histories, demographics, location, preferences and interests, and credit cards used, just to name a few—to pay its creditors.[54] The FTC sued Toysmart in 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.[55]

The FTC has also moved against companies that have promised, yet failed, to protect the confidentiality of their users' data,[56] to collect only certain types of data,[57] to put in place adequate security safeguards,[58] and to maintain user anonymity,[59] just to name a few examples. Broken promise litigation, which, by its very nature, is keyed to the substantive disclosures in privacy policies, remains a significant share of the FTC's overall privacy enforcement actions.[60]

The second way the FTC focuses on the substantive of privacy policies is by requiring companies to include specific content as part of its settlement orders. At the same time, the FTC says very little about what proper notice looks like. This has

---

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

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

[50] *Id.* at 765-6.

[51] Toysmart Complaint, *supra* note 48.

[52] *Id.* at ¶ 10.

[53] *Id.* at ¶ 9.

[54] *Id.* at ¶11.

[55] *Id.* at ¶¶ 16-18.

[56] Eli Lilly, *supra* note 49.

[57] In re Microsoft Corp., 134 F.T.C. 709, 715 (2002) (complaint).

[58] *See, e.g.*, In re Microsoft Corp., 134 F.T.C. 709, 712 (2002) (complaint); Complaint for Permanent Injunction and Other Equitable Relief ¶ 43, FTC v. Rennert, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm.

[59] In re Compete, Inc., FTC File No. 102 3155, No. C-4384 (F.T.C. Feb. 20, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf (the company had allegedly failed to anonymize data prior to transmission).

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

always been the case. In its first privacy enforcement action, the FTC alleged that GeoCities sold its customers' personal information in express violation of its privacy policy.[61] As part of a settlement, the FTC ordered GeoCities 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.[62] 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.[63] And in *In re Sony BMG Music Entertainment*, the FTC alleged that Sony failed to inform customers that the software it installed on certain CDs would transmit music listening data back to Sony.[64] The FTC settled both cases. In each settlement, the FTC ordered Frostwire and Sony to make specific what-when-how disclosures to its customers. Frostwire, for example, had to state, among other things, "which files … it will share and the audience with whom those files will be shared."[65] Sony had to inform users precisely what the installed software would do and give them the opportunity to opt out.[66] 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.[67] The Wizard consisted of several well-designed and 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."[68] Users could click through and select

---

[61] Complaint at ¶¶ 13-14, In re GeoCities, FTC File No. 982 3015, No. C-3850 (F.T.C. Aug. 13, 1998), *available at* https://www.ftc.gov/sites/default/files/documents/cases/1998/08/geo-cmpl.htm.

[62] Decision and Order, In re GeoCities, FTC File No. 982 3015, No. C-3850 (F.T.C. Feb. 12, 1999), *available at* https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do_.htm (decision and order).

[63] 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], available at http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf.

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

[65] Frostwire Complaint, *supra* note 63, at 6.

[66] Sony Complaint, *supra* note 64, at 4.

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

[68] *Id.* at 7.

privacy settings for different categories of information, from photos to birthdays to family.[69] Facebook thus used a pleasantly designed 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.[70] In *In re Sears Holdings Management Corp.*, Sears did not create a user friendly interface to confuse customers into thinking their data was secure. Instead, it used policy design. The FTC charged Sears with misleading consumers about software that, when installed, acted like a vast fishing net, sweeping in extraordinary amounts of data.[71] 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.[72] That license agreement was inscrutable: it was 19 pages long of small print, with only a handful of subheadings.[73]

In both *Facebook* and *Sears*, the companies used design to manipulate and misinform users: Facebook designed an entire interface to give users a false sense of security; Sears tried to hide its data collection practices in a policy it knew no one could (or would) read. And yet, the Sears complaint virtually ignored the design of Sears's policy when it came time to allege counts of unfair and deceptive practices. The settlement order also ignored it. Other than stating that the companies had to "clearly and prominently" inform consumers, the orders listed particular substantive disclosures to include in a policy.[74] Sears's policy design tactic was relegated to an afterthought.[75]

---

[69] *Id.* at 8.

[70] *Id.*

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

[72] *Id.* at 5.

[73] Exhibit E, Sears Complaint, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscomplaintaf.pdf.

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

[75] 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 contracts highly with the background on which they appear" and "of understandable language and syntax." Facebook Order 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, please see *infra* Part I.B.4.

As Solove and Hartzog found, almost all FTC enforcement actions settle.[76] 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.[77] 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.

4. Federal and State Laws and Privacy Policy Content

There are dozens of federal and countless state laws that purport to protect information privacy.[78] But, unlike in the European Union, there is no comprehensive nationwide privacy protection law in the United States.[79] Instead, federal data privacy protection in the United States is "sectoral," or limited to specific types of information. For example, the Health Information Portability and Accountability Act (HIPAA) helps protect the privacy of medical information[80] and the Gramm-Leach-Bliley Act gives individuals notice and control over information held by certain financial institutions.[81] HIPAA and Gramm-Leach-Bliley, along with the Children's Online Privacy Protection Act (COPPA)[82] and the E-Government Act,[83] 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,[84] the statutes pay most of their attention to privacy policy content. A similar pattern is playing out in the states,

---

[76] Solove & Hartzog, *supra* note 5, at 610-11.

[77] *Id.* at 614-19.

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

[79] 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, *available at* http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046. 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.

[80] 42 U.S.C. § 300gg, 29 U.S.C. § 1181 et seq., and 42 U.S.C. 1320d et seq..

[81] 15 U.S.C. §§ 6801-6809.

[82] 15 U.S.C. §§ 6501-6506 (protecting information websites gather from children under 13 years old).

[83] Pub. L. No. 107-347, 116 Stat. 2899 (regulating federal agencies that gather and store personal data).

[84] *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).

where laws that envision privacy policies—like California's Online Privacy Protection Act[85] and New York's Internet Security and Privacy Act[86]—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,[87] 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 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.[88] The E-Government Act mandates similar disclosures from federal government agencies and contractors.[89]

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.[90] 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.[91] 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

Laws from California to Delaware 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.

---

[85] Cal. Bus. & Prof. Code §§ 22575-22579.

[86] N.Y. State Tech. Law § 203.

[87] 15 U.S.C. §§ 6502(b)(1)(A)(i)-(ii) (2015).

[88] 15 U.S.C. § 6502(b)(1)(A)(i)

[89] 44 U.S.C § 3501(c)(1)(B)(i)-(viii) (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).

[90] 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).

[91] 45 C.F.R. § 1640.520(b)(1).

State attorneys general have issued guidance documents, pressured Internet companies, and initiated privacy enforcement litigation to enhance user notice and choice, as well.[92] 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.

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.[93] 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.[94] 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 with in the last year to disclose their data use and information sharing practices.[95]

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.[96] Once again, the statute requires a what-when-how of data use practices: the policy must disclose what and under what circumstances information is being collected, 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 her information, and what steps the state is taking to secure the data.[97] Connecticut and Michigan have laws requiring similar disclosures of any person or entity that collects Social Security numbers in the course of business.[98] In Utah, the state'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.[99] And Delaware recently passed its Online Privacy and

---

[92] *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. __ (forthcoming 2017), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.

[93] *See* Cal. Bus. & Prof. Code §§ 22575-22579. The law sets a de facto national standard because companies have an incentive to comply with the most strict law rather than navigating 50 different requirements. *See* Citron, *supra* note 92, at *11.

[94] *Id.* at §§ 22575(b)(1), (3).

[95] Cal. Civ. Code § 1789.83.

[96] N.Y. State Tech. Law § 203.

[97] *Id.* at § 203(1)(a)-(g).

[98] Conn. Gen. Stat. Ann. § 42-471(b); Mich. Comp. Laws § 445.841(1).

[99] Utah Code Ann. §§ 63D-2-103(2).

Protection Act, which, among other things, requires the operator of any online service that collects data on Delawareans to post a privacy policy. The law requires the same what-when-how content of CalOPPA.[100]

As Danielle Citron shows, state attorneys general (AGs) have used these and other laws to be more aggressive privacy regulators than the FTC.[101] This is true for various legal, historical, and practical reasons that need not be repeated here.[102] Suffice it 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 10 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 with the what-when-how of data use: data collection practices, a promise to comply, and an opt out option.[103] Policy design was not a factor.

In the mobile space, however, where California AG Kamala Harris has been particularly successful, regulatory efforts included at least one important policy design feature: timing. AG Harris's working group on mobile privacy secured commitments from Amazon, Apple, Google, Microsoft, Facebook, and others to not just display privacy policies on mobile apps, but to show them *before* users download the app rather than after.[104] This is an important step toward considering the design of privacy policies, but one still too rare among privacy regulators today.

5. Moving Beyond Content

Privacy regulators are not wrong to focus at least some of their energy on content. In a notice-and-choice regime, regulators must require some specific substantive disclosures; otherwise, notice and choice would be impossible. Notice requirements also help embed 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 makes privacy enforcement easier. 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 policies and their related laws are all lawyers. Trained and well-practiced in drafting contracts, lawyers' skill and knowledge base lie in the substantive terms of privacy policies, not what those policies look like. As one leading attorney in private practice who leads her firm's privacy group told me:

---

[100] Del. Code Ann. § 1201.

[101] *See* Citron, *supra* note 92.

[102] *Id.* at *4, 6-10.

[103] *Id.* at *19 (*citing* Stephanie Miles, *DoubleClick Reaches Deal with State Attorneys General*, Wall Street Journal (Aug. 26, 2003 5:37 PM), http://www.wsj.com/articles/SB1030381164280449795.

[104] *Id.* at *20. See Attorney General 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.

Privacy policies "are seen as legal documents, and they are regulated like ones. So we write them as if they are."[105]

But although the substance of a company's data use disclosures is a necessary part of a notice-and-choice approach to information privacy, it cannot be the only part. The FTC and state privacy regulators seem to recognize this. Many of the content requirements described above also mandate that the policies be readable[106] and clearly and conspicuously posted.[107] An understandable policy that is available via a prominent link is an important step toward achieving adequate notice and choice. However, while promulgating a rule that defines the "clear and conspicuous" requirement as, at a minimum, requiring a link that is of a font, size, and color designed to call attention to itself,[108] 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 Commission Sheila Anthony called for a "standard format" for privacy policies along the lines of the Nutritional Labeling and Education Act's standard format for food labels.[109] Commissioner Anthony recognized that inconsistent and confusing policy design was preventing consumers from becoming aware of their data privacy rights.[110] In a report on how to comply with CalOPPA, Attorney-General Kamala

---

[105] Telephone interview with "Private Practice Attorney 1" (name redacted per wishes of interviewee), Mar. 16, 2016 (notes on file with author).

[106] *See e.g.*, 16 C.F.R. § 312.4(a) (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 using "clear, concise sentences, paragraphs, and sections; (2) … short explanatory sentences or bullet lists whenever possible; (3) … 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). As Joel Reidenberg and others have shown, however, privacy policies are generally not "reasonably understandable." *See* Reidenberg et al., *Privacy Harms*, *supra* note 9.

[107] *See, e.g.*, Facebook Order, *supra* note 74, at 2; Sears Order, *supra* note 74, 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 29, 2007), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019do070629.pdf; Cal. Bus. & Prof. Code § 22575(b)(1) and (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).

[108] 16 C.F.R. § 313.3(b)(2)(ii)(A)-(E).

[109] Sheila F. Anthony, *The Case for Standardization of Privacy Policy Formats* (July 1, 2001), https://www.ftc.gov/public-statements/2001/07/case-standardization-privacy-policy-formats.

[110] *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 (2005) (arguing that standardized labeling does not alleviate all comprehension problems).

Harris included a recommendation that policies be drafted "in a format that makes the policy readable, such as a layered format."[111] In reaction, the International Association of Privacy Professionals suggested "using graphics and icons in … privacy policies to help users more easily recognize privacy practices and settings."[112] AG Harris has also gone so far as to recommend that companies publish two different policies, on which is easy to read and geared toward ordinary consumers.[113] These infrequent nods toward the importance of privacy policy design in informing the public of its data privacy rights suggests an underlying recognition of the problem. But little has been done about it. Nor are these minimal design recommendations sufficiently supported by data for implementation. We need to bring privacy policy design out of the closet.

II. 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 "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."[114] Laws and norms regulating internet social life, therefore, cannot ignore our embodied experiences.[115] 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 recognize that we are actually constrained by policy design and 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,[116] as has Julie Cohen,[117] Ryan Calo,[118] and Woodrow Hartzog.[119] 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

---

[111] CAL. DEPT. OF JUSTICE, MAKING YOUR PRIVACY PRACTICES PUBLIC: RECOMMENDATIONS ON DEVELOPING A MEANINGFUL PRIVACY POLICY [hereinafter, "PRIVACY PRACTICES"] 2 (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

[112] 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.

[113] *See* CAL. DEPT. OF JUSTICE, PRIVACY PRACTICES, *supra* note 111.

[114] Cohen, *Cyberspace*, *supra* note 13, at 218.

[115] 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.

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

[117] *See generally* Cohen, *Cyberspace*, *supra* note 13.

[118] *See generally* Calo, *supra* note 26.

[119] *See generally* Hartzog, *supra* note 27.

is configured by technology and design as an alternative to the user at the heart of notice and choice today. I then discuss the results of a first-of-its-kind 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 can constrain freedom.[120] The sociologist Anthony Giddens argued that the social world is "made to happen" within the rules and available resources of a society into which we are born.[121] Pierre Bordieau agreed: his concept of the *habitus* suggests that a complex web of pre-existing norms socialize and situate us in society from very early on.[122] These rules, manifest in everyday life, coerce us with and without our knowledge. They are everything from subtle tactics like Cass Sunstein's "nudges"[123] to the blunt axe of New York City's subway tracks, which make it difficult to get from Chelsea to the Upper East Side.

These structures constrain or, to borrow Steve Woolgar's term, configure us.[124] When he coined that phrase, Woolgar 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.[125] 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, that is, it obtains meaning and changes through the embodied experience of those involved, from the engineers to the users.[126] 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.[127] Ronald Kline and Trevor Pinch have demonstrated how rural America helped change the design and use of the car.[128] They are not alone.[129]

---

[120] EMILE DURKHEIM, THE RULES OF SOCIOLOGICAL METHOD 50–51 (Steven Lukes ed., W.D. Halls trans., 1982) (1895), *available at* http://comparsociology.com/wp-content/uploads/2013/02/Emile-Durkheim-Rules-of-Sociological-Method-1982.pdf.

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

[122] *Id.* at 20-21.

[123] RICHARD THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

[124] Woolgar, *supra* note 16, at 61.

[125] *Id.* at 59, 61, 89.

[126] SUCHMAN, *supra* note 16, at 187.

[127] SUSAN DOUGLAS, INVENTING AMERICAN BROADCASTING, 1899-1922 (1987).

[128] Ronald Kline and Trevor Pinch, *Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States*, 37 TECH. & CUL. 763, 768-94 (1996).

[129] *See, e.g.*, CLAUDE FISHER, AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940 (1992) (telephone); MICHELE MARTIN, HELLO CENTRAL?: GENDER, TECHNOLOGY AND CULTURE IN THE FORMATION OF TELEPHONE SYSTEMS (1991) (same); DAVID E. NYE, ELECTRIFYING AMERICA:

This social narrative of technology envisions users differently than Kant and notice and choice today. Rather than disembodied purely rational actors, we are real people, doing real things with technology, and situated in an actual time where needs are contingent and decisions are contextual.[130] We may have an impact on the design of new technologies if our needs trickle down to the engineers,[131] but we are always configured, or affected and constrained, by the designs of the technologies we use and the spaces with inhabit.

Art and design are part of this story[132] because they, like invisible yet constraining social forces, frame and limit our agency in a space.[133] Indeed, as Henri Lefebvre argued, the nature of a space is determined by what designers want to happen or not to happen in it.[134] 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 platforms' 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, the privacy notices, and the laws that govern them, should reflect this reality.

B. The Design of Privacy Policies

To what extent do designs of privacy notices influence users' decisions to share personal information? In this section, I discuss and 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

---

SOCIAL MEANINGS OF A NEW TECHNOLOGY, 1880-1940 (1990) (electricity and electric appliances, streetlights, and trolleys).

[130] SUCHMAN, *supra* note 16, at 191; Nissenbaum, *supra* note **Error! Bookmark not defined.**.

[131] 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 16, at 70, 71, 73-4.

[132] Michel Foucault, *On Power*, *in* MICHEL FOUCAULT: POLITICS, PHILOSOPHY, AND CULTURE: INTERVIEWS AND OTHER WRITINGS, 1977-1984 (Lawrence Kritzman ed. 1988) (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").

[133] DOVEY, *supra* note 121, at 1.

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

used to obfuscate—users are much more likely to make risky privacy choices. As such, privacy regulators who seek to protect consumers from unfair, coercive, and deceptive practices should not only consider how a company's disclosures conform with its actual data practices. They should also investigate how websites use design to transmit those disclosures.

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.[135] 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.[136] 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[137] to website design.[138] 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 of privacy policies and cookie notifications. The

---

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

[136] *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).

[137] If we perceive that others are willing to disclose, we are more likely to disclose. *See* Acquisti, John, & Loewenstein, *supra* note **Error! Bookmark not defined.**, at 160. Acquisti and his colleagues ran a study in which respondents were asked to respond to a series of ethics questions, some of which required them to admit to stigmatizing behavior. They were more likely to respond that they had engaged in bad behaviors when told that many previous respondents had admitted to them, as well. *Id.* at 160, 171.

[138] *See supra* notes **Error! Bookmark not defined.**-**Error! Bookmark not defined.** and accompanying text.

survey was created using Google Forms and conducted through Amazon Mechanical Turk. A total of 576 unique Turkers took the survey. Only 12 were eliminated from consideration for completing the survey improperly. The entire survey had 24 substantive questions, including ones on demographics.

Part I asked for basic demographic data: 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, 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: significant time online per day, a high number of active profiles, and use of many e-commerce platforms may all be correlated with an increased willingness to disclose personal information.

Parts II through V asked respondents whether they trusted a website given an image of a portion of its privacy policies.[139] In Part II, policy designs reflected the vast majority of designs that make today's policies difficult to read. Data use practices were changed, varying from privacy-protective to invasive. In Part III, designs changed, but data use practices stayed at a median point evident from the policy canvas discussed above. Some designs were similar to those in Part I; others used strategies that elicited positive emotional responses from the privacy policy research team. Part IV changed designs and data use practices: sometimes, user friendly or poor designs were paired with privacy-protective practices; in other questions, the designs displayed highly invasive practices. Part V offered a potpourri of options, stepping out of the pattern of the previous sections.

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.[140] Users ages 18-24 constituted 19.5% of the sample; 25-34 year-olds made up just over 41%; 26% of the sample where 35-44 year-olds; 12.8% were 45 and older.[141] More

---

[139] Policies are too long to include in their entirety. I recognize that length of the policy as a whole is a design technique that makes website data practices incomprehensible to the average internet users. 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.

[140] This departs somewhat from evidence that suggests Facebook users are more likely to be female. *See* Maeve Duggan, *Mobile Messaging and Social Media*, at 10, PEW RESEARCH CENTER (Jan. 9, 2015), http://www.pewinternet.org/files/2015/08/Social-Media-Update-2015-FINAL2.pdf.

[141] The 25-34 year old age bracket may be overrepresented, according to the best statistics available. *See* Maeve Duggan, Nicole B. Ellison, Cliff Lampe, Amanda Lenhart, & Mary Madden, *Social Media Update 2014*, at 5, PEW RESEARCH CENTER (Jan. 9, 2015), http://www.pewinternet.org/files/2015/01/PI_SocialMediaUpdate20144.pdf. *See also* Mark Hoelzel, *Update: A Breakdown of the Demographics For Each of the Different Social Networks*, Business 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.

than 81% of the sample reports that they are online more than 3 hours per day.[142] 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 3 or more social networking sites.[143]

Part II of the survey included five policy pairs: All policies were designed like today's privacy policies, 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 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.[144] The policy in Figure 1 allows the company to do more with user data than the policy in Figure 2. The questions included images of policies along a range of protective to invasive.

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.

Figure 1

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.

Figure 2

Respondents could choose to trust or do business with either website, or could select "I don't trust either of them" or "I trust them both the same."[145] Answers to these questions should help us understand how users, when given the opportunity, respond to privacy policies today. Of the entire survey, "I don't trust

[142] This number likely suffers from a reporting bias. Individuals are often disinclined to admit that they spend so much time online.

[143] This is also in line with Pew findings. *See* Duggan, Ellison, Lampe, Lenhart, & Madden, *supra* note 141.

[144] 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, http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html (last visited June 30, 2016).

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

either of them" was the most popular answer in this section. When the substantive policies differed the most, as with Figures 1 and 2 above, most respondents (68%) were able to identify that the website represented by Figure 1 had more extensive 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.[146]

As the content of the policies started to change, respondents had trouble trusting one over the other. This was true even when there were significant differences. Between a policy that, on the one hand, gave users a means of opting out and provided notice before any data sharing outside the company, and, on the other hand, 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.

To test the impact of design, Part III of the survey varied designs, but kept the underlying data use practices constant at some median point.[147] Examples of pairings are seen in Figures 3 and 4 below.[148]

---

[146] *See, e.g.*, Leon et al, *supra* note 135. Kirsten Martin is also doing excellent work in this area. *See* Kirstin Martin, *Formal Versus Informal Privacy Contracts: Comparing the Impact of Privacy Notices and Norms on Consumer Trust Online* (unpublished manuscript), *available at* http://www.law.uchicago.edu/files/file/martin_formal_versus_informal_privacy_contracts.pdf.

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

[148] 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, https://www.chase.com/digital/resources/privacy-security/privacy/consumer-privacy-notice (last visited June 30, 2016). 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), also uses charts. *See* U.S. Consumer Privacy Notice, Printer Friendly Version, https://www.chase.com/content/dam/chase-ux/documents/digital/resources/consumer-privacy-policy.pdf (last visited June 30, 2016).

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.

Figure 3

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

Figure 4

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.[149] By a more than eight to one margin, 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.[150] 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 could provide evidence on how users react to the potential scenario where different 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 over a traditionally designed policy that permitted none.[151] 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 with 15-point lettering that described wildly invasive data use practices was trusted by 43% of respondents. Thirty-nine percent trusted a traditionally designed policy with promised to seek user consent before data sharing. Only 13% trusted neither. Finally,

---

[149] 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.

[150] Though its design can certainly be improved, Uber deploys some of these design strategies in its privacy policy. *See* User Privacy Statement, https://www.uber.com/legal/privacy/users/en/ (last visited June 30, 2016).

[151] The graphical policy was an almost exact copy of FitBit's user-focused privacy policy. *See* Let's Talk About Privacy, Publicly, https://www.fitbit.com/privacy (last visited June 30, 2016).

a cookie policy that presented in a popup 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 1.5 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 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 popup notification that the website deployed cookies to track users and a traditionally designed policy that promised no tracking or data sharing, users split again: 39% trusted the graphically designed popup; 40% trusted the strict policy in a traditional design.

4. Discussion

The choices respondents made based on privacy policy design suggest several areas of concern for regulators, legislators, and online platforms. 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 today's designs, suggesting that current 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 done to fix it.[152] 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.[153] It is no wonder, then, that survey respondents expressed the

---

[152] *See* Mary Madden & Lee Raine, *Americans' Attitudes About Privacy, Security, and Surveillance*, at 6-7, PEW RESEARCH CENTER (May 20, 2015), http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf.

[153] *Id.* at 7.

same helplessness when faced with poorly designed policies. This evidence is also in line with current research that suggests that privacy decision-making tends to be comparative in nature:[154] when users are asked to make data sharing decisions purely on privacy policies that do a poor job at conveying information, decision-making becomes difficult.

When given the opportunity in Part III of this survey, respondents took privacy policy design into account when making privacy choices. This also makes sense given current research on the propensity to disclose.[155] 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 significant 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 modern, user-friendly designs created a more positive emotional reaction among respondents. And we know that feelings of happiness contribute to a greater willingness to share.[156] It could also be that designs meant to help inform readers actually work. 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 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 questions in Part IV.

III. Effective Notice Design

---

[154] Acquisti, John, & Loewenstein, *supra* note **Error! Bookmark not defined.**, at 160.

[155] John, Acquisti, & Loewenstein, *supra* note 12, at 864.

[156] Li, Sarathy, & Xu., *supra* note **Error! Bookmark not defined.**, at 435.

Whether obfuscated through poor design or manipulated through user-friendly designs, user freedom and choice are constrained.[157] Instead of staying silent and being complicit in corporate use of manipulative design, privacy regulators should step in and start paying attention to the deceptive capacity of privacy policy design. With the help of the Federal Trade Commission, state privacy regulators, and federal and state legislation, internet users could start to reclaim control over their privacy online.[158]

Based on the research described in this Article, proposal for reforming notice and choice should adhere to three overarching principles. First, given that internet users, as Lessig and others have shown,[159] are constrained by the designs of digital environments, notice should reflect their embodied experience. That is, notice policy must take into account how we 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. If this research has shown anything, it is that notice design can both enhance transparency or hinder it; effective reform must harness its illuminating potential. Finally, notice has to 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 three avenues of reform that meet these criteria. I then conclude by responding to potential objections.

A. Considering Design in Privacy Law

To ensure that user-oriented privacy policies are effective, privacy law in the books and on the ground needs to strengthen and enhance its consideration of design. That means integrating design into privacy norms and law. Sociocultural norms are important: laws generally reflect powerful and persistent social norms.[160] This is true in privacy law, in particular, where the substantive norms expressed in the Fair Information Practices have bled into law through FTC enforcement actions and state and federal mandates.[161] 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. The FTC could add a new "Design" FIP or include it under "Notice," stating that disclosures by data collectors must be presented to users in a user-friendly way that makes it easy for users to identify and understand their rights.[162] Much like California Attorney General Kamala Harris, state attorneys general can take this

---

[157] *See* FINDLEY, *supra* note **Error! Bookmark not defined.**, at 5.

[158] *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).

[159] *See supra* notes 116-119.

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

[161] *See supra* Part I.B. *See also* Rotenberg, *supra* note 84.

[162] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 3-4 (2000).

further, by including more specific design requirements in their publications and best practice guides.[163]

State and federal laws that mandate privacy policies can 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. Notably, these guidelines need not specify specific designs and aesthetics that must be used. As the above survey suggests, even seemingly user-friendly designs can be used in manipulative ways. Rather, these statutes and regulations have to start taking design seriously, recognizing that design and aesthetics are essential to conveying information to users.

And they would have precedent to follow. The Securities and Exchange Commission, for example, requires that prospectuses and other documents be written in "plain English"[164] so that investors and other members of the public can understand them.[165] A plain English document is more than one written in simple prose. Rather, a "plain English document reflects thoughtful design choices. 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."[166] The same can be true for privacy policies. 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.[167] It devotes several pages to document layout, discussing how to use white spaces effectively[168] and how appropriate line spacing can increase readability.[169] 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 greys on white backgrounds, like those used in many online privacy policies today, would fail the SEC's "plain English" requirement.[170]

---

[163] AG Harris took a first step in this direction. *See* CAL. DEPT. OF JUSTICE, PRIVACY PRACTICES, *supra* note 111, at 2, 4, 10 (recommending a layered format that calls attention to important rights). *See also* Citron, *supra* note 92, at n.20.

[164] *See* 17 C.F.R. § 230.421.

[165] SECURITIES AND EXCHANGE COMM'N, A PLAIN ENGLISH HANDBOOK: HOW TO CREATE CLEAR SEC DISCLOSURE DOCUMENTS [hereinafter, PLAIN ENGLISH HANDBOOK] 3 (1998), *available at* https://www.sec.gov/pdf/handbook.pdf ("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.").

[166] *Id.* at 37.

[167] *Id.* at 38-42.

[168] *Id.* at 44.

[169] *Id.* at 46.

[170] By way of example, Tinder Inc.'s and LinkedIn's privacy policies are both written in a light-to-medium grey on a white background. *See* Tinder, Inc. Privacy Policy,

The Handbook also encourages the use of "simple" graphics and charts because they "often illuminate information more clearly and quickly than text."[171] 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.[172] In that text, Tufte captured the essence of considering the design of privacy policies as a factor in providing adequate notice and choice to 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."[173] 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*,[174] a case involving the enforceability of a forum selection clause written in tiny print on the back of a passenger ticket,[175] 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 25-paragraph contract.[176] 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.[177] As the D.C. Circuit, in an opinion written by Judge Skelly Wright held, incomprehensible design, typified by the tiny fine print by which no reasonable consumer could be informed, could make a contract unconscionable.[178] Similarly, states have passed laws with design requirements where the goal is conveying information to real people. For example, South Carolina mandates particular design

---

https://www.gotinder.com/privacy (last visited Feb. 18, 2016); Your Privacy Matters, https://www.linkedin.com/legal/privacy-policy?trk=uno-reg-guest-home-privacy-policy (last visited Feb. 18, 2016).

[171] PLAIN ENGLISH HANDBOOK , *supra* note 165, at 49, 50.

[172] *Id.* at 49.

[173] *Id.* at 51.

[174] 111 S. Ct. 1522 (1991).

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

[176] *Id.* at 1529.

[177] *Id.* at 1531.

[178] Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449-450 (1965). *See also* In re Real Networks, Inc., Privacy Litigation, 2000 WL 631341, No. 00 C 1366, *5 (N.D. Ill. May 8, 2000) ("burying important terms in a "maze of fine print" may contribute to a contract being found unconscionable") (in dicta).

requirements for disclaimers in employee handbooks.[179] California prescribes both the design and content of arbitration agreements.[180]

The Consumer Financial Protection Bureau (CFPB) has gone even 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."[181] And it follows an open source Design Manual for its own documents.[182] This Manual, which provides guidance on anything from the CFPB color palette[183] to typography and different types of icons, is used to create "honest, transparent design that wins the public trust" and empowers users.[184] 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. Therefore, privacy regulators could learn lessons from the CFPB, and securities and contract law to incorporate similar design requirements in their regulations.

B. Respecting Users

Privacy by design can help, as well. A platform built from the ground up by a company that takes privacy seriously is more likely to make design choices that aid in transparency. Various design strategies may make policies more understandable. Just-in-time notifications about cookies, data sharing, and third-party access to information can be programmed into a user's experience. Platforms can create privacy wizards or centers that take users step-by-step through a comprehensive and transparent process of notice and choice. More generally, as Paula Bruening and Mary Culnan have argued, the design of notices should be fully integrated into system development rather than an afterthought.[185]

---

[179] 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").

[180] 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.").

[181] Chris Willey, *Design+Technology Fellows: Changing the Way Government Works*, At the CFPB Blog (June 21, 2012), http://www.consumerfinance.gov/about-us/blog/designtechnology-fellows-changing-the-way-government-works/ (last visited Apr. 1, 2016).

[182] CFPB Design Manual, https://cfpb.github.io/design-manual/index.html.

[183] CFPB Design Manual, Color, https://cfpb.github.io/design-manual/identity/color-principles.html.

[184] CFPB Design Manual, Design Principles, https://cfpb.github.io/design-manual/guides/design-principles.html.

[185] 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 (2015).

Part of this means engaging in rigorous testing to ensure that user-focused notice designs enhance transparency. This would ensure that the embodied experience of users is reflected in the design of privacy notices.[186] And 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. And regulators can deploy consumer testing to evaluate notice design during investigations of manipulative practices.[187]

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.[188] But rules governing user-focused notices must do more than recommend brevity. They have to demand transparency-enhancing design.

As Bruening and Culnan demonstrate, we already know a little bit about the effects of such designs.[189] Among the proposals tested have been standard "nutrition label"-style standard notices,[190] the Gramm-Leach-Bliley notice form,[191] 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.[192] 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.[193] Table formats tend to be most effective at

---

[186] *See* Woolgar, *supra* note 16; Kline & Pinch, *supra* note 128, at 768-94.

[187] 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).

[188] *See* Citron, *supra* note 92, at *20 & n. 122.

[189] Bruening & Culnan, *supra* note 185, at 547-52.

[190] Although some commentators have called for a privacy "nutrition label" that standardizes privacy policy design, *see, e.g.*, Sheila F. Anthony, *The Case for Standardization of Privacy Policy Formats* (July 1, 2001), https://www.ftc.gov/public-statements/2001/07/case-standardization-privacy-policy-formats, a single uniform design has not gained traction among legislators and regulators. *See also* Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices, National Telecommunications and Information Administration, https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf (last visited July 17, 2016).

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

[192] *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 (*cited in* Bruening & Culnan, *supra* note 189, at 557).

[193] *See* Alecia 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 189, at 551-2).

conveying information.[194] What these researchers did not test, however, was whether 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,[195] 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. When 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.

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,[196] this argument suggests that letting a rather unrepresentative cadre of regulators or judges determine whether 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. And considering manipulation-by-design is also well within the scope of the FTC's authority to regulate unfair and deceptive business practices. As Dan Solove and Woodrow Hartzog have shown, the FTC has developed a general theory of deception that includes tactics that induce consumers to disclose personal

---

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

[195] *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).

[196] 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 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 decisionmaking process in this area.").

information.[197] Under this theory, the FTC has moved against companies that have induced disclosure by making misleading phone calls,[198] phishing,[199] and suggesting that they are affiliated with trusted entities.[200] 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 Kantian conception of the 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 choose not read the policies, consumers assume the risk that their data could be used in ways they did not expect.[201] But holding individuals responsible for assumption of risk 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.

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 done so while treating 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. Another important step in understanding how to reform and redesign notice is to learn how privacy law in the book and on the ground trickles down to designers,

---

[197] *See* Solove & Hartzog, *supra* note 5, at 630.

[198] Complaint for Permanent Injunction and Other Equitable Relief at 5-6, FTC v. Sun Spectrum Commc'ns Org., Inc., No. 03-CV-8110 (S.D. Fla. Oct. 3, 2005), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2004/01/031202cmp0323032.pdf (*cited in* Solove & Hartzog, *supra* note 5, at 632).

[199] 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), available at http://www.ftc.gov/sites/default/files/documents/cases/2003/07/phishingcomp.pdf (*cited in* Solove & Hartzog, *supra* note 5, at 632-3).

[200] Complaint for Injunctive and Other Equitable Relief at 22-23, FTC v. Assail, Inc., No. W03CA007 (W.D. Tex. Nov. 23, 2004), available at http://www.ftc.gov/sites/default/files/documents/cases/2003/01/assailcmp.pdf (*cited in* Solove & Hartzog, *supra* note 5, at 633).

[201] *See, e.g.*, Dwyer v. American Express, 652 N.E.2d 1351 (Ill. App. 1995) (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).

programmers, and engineers responsible for product development. This analysis is the subject of my next project.

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. 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 policy designers can do this, too.