Notre Dame Law Review Online

Volume 93 | Issue 1 Article 12

5-2018

A Statistical Analysis of Privacy Policy Design

Ari E. Waldman
New York Law School

ESSAY

A STATISTICAL ANALYSIS OF PRIVACY POLICY DESIGN

*Ari Ezra Waldman**

INTRODUCTION

Privacy policies are essential to the notice-and-choice approach to online privacy in the United States.[1] They are at the core of the privacy jurisprudence of the Federal Trade Commission (FTC)[2] and the privacy policymaking of state attorneys general.[3] And countless federal and state statutes envision privacy policies as the foundation of the legal relationship between internet users and data collectors.[4]

* Associate Professor of Law and Director, Innovation Center for Law and Technology, New York Law School. Ph.D., Columbia University; J.D., Harvard Law School. Affiliate Scholar, Princeton University, Center for Information Technology Policy. A few paragraphs of this Essay were adapted from Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74 (2018), but the study and analysis are entirely new.

1 "Notice-and-choice" refers to the legal regime whereby web platforms are required to tell consumers what information they collect, how and for what purpose they collect it, and with whom they share it (notice). *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 592 (2014). Consumers then have the opportunity to opt out (choice). *See id.* This Essay leaves to one side the broader debate over whether privacy law should maintain or replace notice-and-choice. Rather, it accepts notice-and-choice as the current approach to consumer privacy law and seeks to improve notice within that regime.

2 *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 145–305 (2016) (discussing the FTC's regulation of privacy); Solove & Hartzog, *supra* note 1, at 627–66 (discussing the FTC's jurisprudence on the new common law of privacy).

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

4 For example, 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. 15 U.S.C. §§ 6803(a)(1)–(2) (2012); 16 C.F.R. §§ 313.6(a)(3), (6) (2018). The Children's Online Privacy Protection Act, which guards against unauthorized use, collection, and dissemination of information of children thirteen years old and younger, requires certain child-oriented websites to post privacy policies with what data

Yet, privacy policies are confusing,[5] inconspicuous,[6] long,[7] and difficult to understand.[8] They are also ineffective: most people never read them,[9] and even experts find them misleading.[10] And, as I argue elsewhere, privacy notices are often designed, displayed, and presented to users in ways that make their substance even more inscrutable.[11] For example, many are written in grey tones on white backgrounds, in small font sizes and single-spaced text, without white spaces or noticeable headings.[12] And even aesthetically pleasing designs can be deployed to trick confused consumers into making risky privacy choices.[13]

This Essay takes a further step in a developing research agenda on the design of privacy policies. As described in more detail in Part II, I created an online survey in which respondents were asked to choose one of two websites that would better protect their privacy given images of segments of their privacy policies. Some of the questions paired notices with, on the one hand, privacy protective practices

---

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. 15 U.S.C. §§ 6502(b)(1)(A)(i)–(ii) (2012). For a more comprehensive list of consumer privacy statutes, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 37–39 (4th ed. 2011).

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

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

7 *See* George R. Milne et al., *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. Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 274 (2012). This translates to about 54 billion hours per year for every U.S. consumer to read all the privacy policies he or she encountered. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR THE INFO. SOC'Y 543, 563 (2008).

8 *See* Mark A. Graber et al., *Reading Level of Privacy Policies on Internet Health Web Sites*, 51 J. FAM. PRAC. 642, 642 (2002).

9 *See, e.g.*, George R. Milne & Mary J. Culnan, *Strategies For Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15 (2004); Jonathan A. Obar & Anne Oeldorf-Hirsch, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services 19–22 (Aug. 24, 2016) (unpublished paper), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465.

10 Reidenberg, *supra* note 5, at 87.

11 *See* Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74 (2018).

12 *Id.* at 81–84.

Although most privacy policies were displayed in black text on white backgrounds, 35% were written in grey on white. Half of those greys were light-to-medium (40%–60% opaque). The median font size was 11: nearly 20% were written in the median size (*n*=37), which is roughly the same number of policies that were written in size seven or eight. 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.

Id. at 82.

13 *Id.* at 112, 115–16.

displayed in difficult-to-read designs, and, on the other hand, invasive data use practices displayed in graphical, aesthetically pleasing ways. Many survey respondents seemed to make their privacy decisions based on design rather than substance. Furthermore, using statistical modeling, this Essay shows that increased knowledge about the legal implications of privacy policies is associated with lower odds of being confused by aesthetically pleasing designs. Although this study is subject to certain limitations, all of which are discussed at the end of Part II, it suggests several avenues for future research and several ways policymakers can improve the efficacy of notice-and-choice.

I. THE IMPORTANCE OF DESIGN

The law has occasionally recognized that the design of legal documents is an important part of validity and transparency. In *Carnival Cruise Lines, Inc. v. Shute*,[14] for example, Justice Stevens argued in dissent that a forum selection clause written in tiny print on the back of a passenger ticket should not be enforceable because it was designed in a way to give consumers "little real choice."[15] Similarly, the D.C. Circuit held that incomprehensible design, typified by tiny fine print, could make a contract unconscionable.[16] And states have passed laws with design requirements. South Carolina requires employers to design disclaimers in employee handbooks so that they stand out.[17] California prescribes both the design and content of arbitration agreements[18] in the name of enhancing understanding, transparency, and comprehension.

The executive branch has taken notice, too. The Securities and Exchange Commission has a Plain English Handbook that requires individuals to design documents in aesthetically pleasing ways so investors and other members of the public can understand them.[19] The Consumer Financial Protection Bureau (CFPB) has gone even further. Its Design+Technology program recruited graphic designers to, among other things, create "[d]esign tools that enable millions of people to make

14 499 U.S. 585 (1991).

15 *Id.* at 600–01 (Stevens, J., dissenting) (quoting Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449–50 (D.C. Cir. 1965)).

16 *Williams*, 350 F.2d at 449–50; *see also In re* RealNetworks, Inc., Privacy Litig., No. 00-C-1366, 2000 WL 631341, at *5 (N.D. Ill. May 8, 2000) ("[B]urying important terms in a 'maze of fine print' may contribute to a contract being found unconscionable . . . .").

17 *See* S.C. CODE ANN. § 41-1-110 (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.").

18 *See* CAL. CIV. PROC. CODE § 1295(b) (West 2016) ("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.'").

19 SEC. & EXCH. COMM'N, A PLAIN ENGLISH HANDBOOK: HOW TO CREATE CLEAR SEC DISCLOSURE DOCUMENTS 3, 37–42, 44–51 (1998), https://www.sec.gov/pdf/handbook.pdf.

informed financial choices."[20] And it follows an open source design manual for its own documents.[21] This manual, which provides guidance on anything from the CFPB color palette to typography and different types of icons, is used to create "[h]onest, transparent design that wins the public's trust" and empowers users.[22]

Nor have the design and aesthetics of privacy policies gone entirely unnoticed. In 2001, for example, former FTC Commissioner 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.[23] Commissioner Anthony recognized that inconsistent and confusing policy design was preventing consumers from becoming aware of their data privacy rights.[24] This was one of the reasons why implementing regulations of the Gramm-Leach-Bliley Act (GLBA), which regulates certain financial information, included some voluntary standardized notice design elements.[25] In a report on how to comply with the California Online Privacy Protection Act, the California Attorney General's Office included a recommendation that policies be drafted in "a format that makes the policy readable, such as a layered format."[26] In reaction, the International Association of Privacy Professionals suggested "us[ing] graphics and icons in [ ] privacy policies to help users more easily recognize privacy practices and settings."[27] California also went so far as to recommend that companies publish two different policies, one that is easy to read and geared toward ordinary consumers and another for regulators.[28]

---

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

21 *See CFPB Design Manual*, CFPB, https://cfpb.github.io/design-manual/index.html (last visited Apr. 7, 2018).

22 *CFPB Design Manual: Design Principles*, CFPB, https://cfpb.github.io/design-manual/best-practices/design-principles.html (last visited Apr. 7, 2018).

23 Sheila F. Anthony, *The Case for Standardization of Privacy Policy Formats*, FED. TRADE COMM'N (July 1, 2001), https://www.ftc.gov/public-statements/2001/07/case-standardization-privacy-policy-formats.

24 *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 Labelling: A Systematic Review*, 8 PUB. HEALTH NUTRITION 21 (2005) (arguing that standardized labeling does not alleviate all comprehension problems).

25 *See* Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62,890 (Dec. 1, 2009).

26 KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, MAKING YOUR PRIVACY PRACTICES PUBLIC: RECOMMENDATIONS ON DEVELOPING A MEANINGFUL PRIVACY POLICY 2 (2014)], https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

27 Lei Shen, *Unpacking the California AG's Guide on CalOPPA*, IAPP (May 27, 2014), https://iapp.org/news/a/unpacking-the-california-ags-guide-on-caloppa.

28 *See* HARRIS , *supra* note 26, at 4–5.

Scholarship on the impact of design and aesthetics on user disclosure and comprehension of privacy practices has been similarly rare. Leslie John has found that individuals are, perhaps counterintuitively, more willing to admit to bad behavior on unprofessional looking websites.[29] These platforms were perceived to be more casual, relaxed, and informal rather than less secure.[30] And other scholars have found that disclosure can be emotionally manipulated: positive emotional feelings about a website, inspired by website design, the type of information requested, and the presence of a privacy policy, correlate with a higher willingness to disclose.[31] What's more, as Paula Bruening and Mary Culnan note, only a few privacy notice design strategies have been tested with any rigor.[32] Nutrition label style notices and GLBA form notices, for example, are imperfect.[33] 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.[34] Layered notices were also inadequate: average users were able to process information from layered notices faster than from long forms, but they were not as accurate.[35] Table formats, however, tended to be most effective at conveying information absent holistic standardization.[36] These infrequent nods toward the importance of privacy policy design in informing the public of corporate data use practices suggest an underlying recognition of the problem. But these studies did not try to describe the population of internet users that are able to discern privacy protective practices despite potentially manipulative policy design. This study takes this next step.

II. PRIVACY POLICY DESIGN AND USER COMPREHENSION

Elsewhere, I show that the design of privacy policies can affect users' decisions to trust or do business with a website.[37] I show that, "when given the opportunity,

29 Leslie K. John et al., *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. CONSUMER RES. 858, 862, 868 (2011).

30 *Id.* at 868.

31 *See* Han Li et al., *The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors*, 51 DECISION SUPPORT SYS. 434, 435–36 (2011).

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

33 *See, e.g.*, NAT'L TELECOMM. & INFO. ADMIN., SHORT FORM NOTICE CODE OF CONDUCT TO PROMOTE TRANSPARENCY IN MOBILE APP PRACTICES (2013), https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf; Patrick Gage Kelley et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, CARNEGIE MELLON UNIV. CYLAB (2010), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1002&context=cylab.

34 *See* Lorrie Faith Cranor et al., *Are They Actually Any Different? Comparing Thousands of Financial Institutions' Privacy Practices*, THE TWELFTH WORKSHOP ON THE ECONS. OF INFO. SEC. (2013), http://www.econinfosec.org/archive/weis2013/papers/CranorWEIS2013.pdf.

35 *See* Aleecia M. McDonald et al., *A Comparative Study of Online Privacy Policies and Formats*, *in* PRIVACY ENHANCING TECHNOLOGIES: 9TH INTERNATIONAL SYMPOSIUM 37, 49–50 (Ian Goldberg & Mikhail J. Atallah eds., 2009).

36 *See* Kelley et al., *supra* note 33, at 9.

37 *See* Waldman, *supra* note 11.

users consider design," not just the substance of a website's data use practices, "when making privacy choices."[38] "[H]olding data use practices constant, users prefer to do business with websites that post privacy policies designed with real people in mind," that is, using an aesthetic that makes them easier to read.[39] I also show that design can be used to manipulate and harm consumers. "[U]sers tended to opt for websites with [aesthetically] pleasing privacy policy designs"—including charts, graphics, colors, large font sizes, and so on—"even when those websites' data use practices were invasive and unsafe."[40] This Essay builds on that analysis and asks whether certain types of internet users are more or less likely to overcome or be confused by manipulative privacy policy design. In particular, this Essay seeks to ascertain whether any demographic data, including age, education, gender, or income, has any effect on the ability of users to resist manipulative privacy policy design. It also asks whether factors that should speak to privacy savviness—e.g., the extent to which internet users read privacy policies and their knowledge of the legal implications of privacy notices—have any effect. As shown below, the data shows that greater knowledge of the legal implications of privacy policies is associated with greater odds of not being confused by aesthetically pleasing designs that obscure radically invasive data use practices.

A. Research Design and Methodology

I designed a survey that asked respondents to choose one website over another based solely on images of privacy policies. The survey was created using Google Forms and conducted through Amazon Mechanical Turk.[41] A total of 513 unique Turkers took the survey. Eighteen responses were eliminated from the analysis due to missing or incomplete data.

The first part of the survey asked for basic demographic data. Respondents listed their age, gender, income, and education level, how much time they spend online per day, and to what extent they read privacy policies. 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. Time online and number of social networking profiles help assess how "networked" an individual is—significant time online per day and a high number of active profiles may all be correlated with an increased digital savviness.

The next question, building on research by Joseph Turow and others,[42] asked respondents about their knowledge of privacy policies in general. The survey listed

38 *Id.* at 107.

39 *Id.*

40 *Id.*

41 Several studies have shown that Amazon Turk offers researchers a random sample of respondents with a demographic distribution roughly comparable to the United States population. *See, e.g.*, Tara S. Behrend et al., *The Viability of Crowdsourcing for Survey Research*, 43 BEHAV. RES. METHODS 800 (2011); Gabriele Paolacci et al., *Running Experiments on Amazon Mechanical Turk*, 5 JUDGMENT & DECISION MAKING 411 (2010).

42 *See* JOSEPH TUROW ET AL., ANNENBERG SCH. FOR COMMC'N, THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO

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

The next three sections asked respondents whether they trusted a website given an image of a portion of its privacy policy. In the first part, respondents were shown four 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." The questions included images of policies ranging from protective to invasive. 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."[43] Answers to these questions should help us understand how users respond to privacy policies today.

To test the impact of design, the third part of the survey varied designs, but kept the underlying data use practices constant.[44] The final part changed designs and data use practices. Sometimes, designs were paired with privacy protective practices; in other questions, the designs displayed highly invasive practices. The pairs were mixed and matched.

The responses relevant for this Essay—namely, the choices between modern designs/invasive practices and obscure design/protective practices—were collapsed into dichotomous pairs. As such, binomial logistic regression was used to analyze the data. Binomial logistic regression predicts the probability that a given observation falls into one of two categories of a dichotomous variable based on one or more independent variables.[45] For example, the statistical modeling technique

---

EXPLOITATION 4–5 (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf; Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J. L. & POL'Y FOR THE INFO. SOC'Y 723, 740 (2007); *see also* Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR. (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/.

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

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

45 *See generally* Jason E. King, *Binary Logistic Regression*, *in* BEST PRACTICES IN QUANTITATIVE METHODS 358 (Jason W. Osborne ed., 2008).

can be used to predict whether Bar Exam performance, measured in "pass" or "fail," can be predicted based on LSAT scores, law school GPA, race, gender, class attendance, and quantity of beer consumed during law school. Here, logistic regression modeling is being used to determine if resistance to the manipulative potential of privacy policy design—namely, choosing hard to read designs with stronger privacy protections as better protective of privacy than aesthetically pleasing designs with invasive data use practices—can be predicted by demographics, a tendency to read privacy policies (measured on a Likert scale of "never" to "always"[46]), and knowledge of privacy law (based on responses to Turow's True/False questions about privacy policies[47]).

B. Results

The sample population can be characterized as follows: there were 495 valid responses, of which 39.8% (197) identified female and 60% (297) identified male. College graduates made up 45.3% of the sample, and those with postcollege advanced degrees constituted an additional 12.5%, for a total of 286 respondents. Income levels varied: 32.7% earned under $30,000 per year; 23.2% earned between $30,000 and $50,000 per year; 24.2% earned between $50,001 and $75,000; and 19.8% earned $75,001 or above. More than 82% of the sample reported that they are online more than three hours per day. The sample was also relatively networked. Nearly half of the respondents maintain active profiles on three or more social networking sites.

The majority of respondents concede that they never (16.2%) or rarely (43%) read privacy policies. Another 32.1% suggest that they "sometimes" read privacy notices. Fewer than 9% of respondents do so "always" or "often."[48] Finally, a majority of the sample exhibited incomplete or inadequate knowledge of the legal implications of privacy policies: 57.8% answered incorrectly; 30.1% answered True to one correct statement, while 12.1% answered True to both correct statements.

In two questions, the survey asked users to choose between policies with identical substance, but different designs: 74.5% and 68% of respondents recognized that the policies were the same. Sizeable majorities were expected here, as it is easy to compare identical language in side by side images.

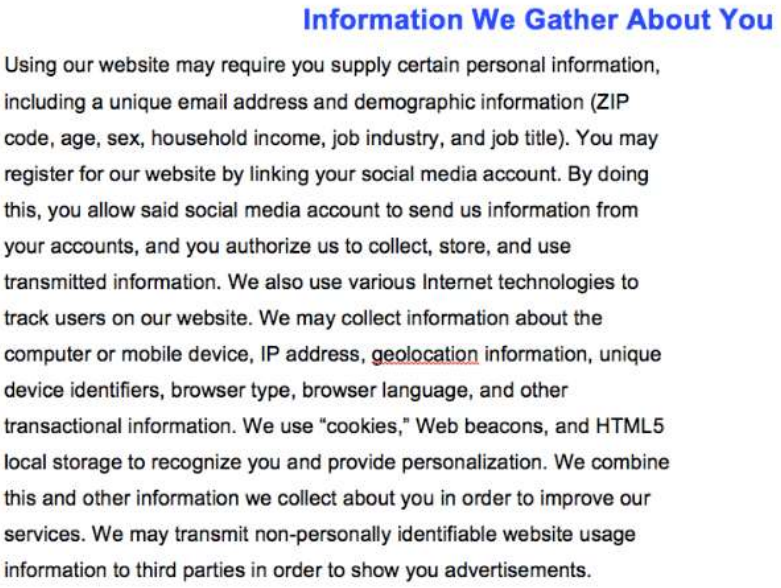
Survey respondents then had two opportunities to choose between an invasive policy designed with a readable, modern aesthetic and a privacy protective policy presented in the traditional way. The first question offered the following choice:

46 *See* TOM TULLIS & BILL ALBERT, MEASURING THE USER EXPERIENCE: COLLECTING, ANALYZING, AND PRESENTING USABILITY METRICS 124 (2008).

47 *See* TUROW ET AL., *supra* note 42, at 4–5.

48 These numbers likely suffer from response biases. Individuals are often disinclined to admit that they do not do things they know or perceive they really should. *See generally* Eunike Wetzel et al., *Response Biases*, *in* THE ITC INTERNATIONAL HANDBOOK OF TESTING AND AESSESSMENT 34963 (Frederick T.L. Leong & Dragos Iliescu eds., 2016).

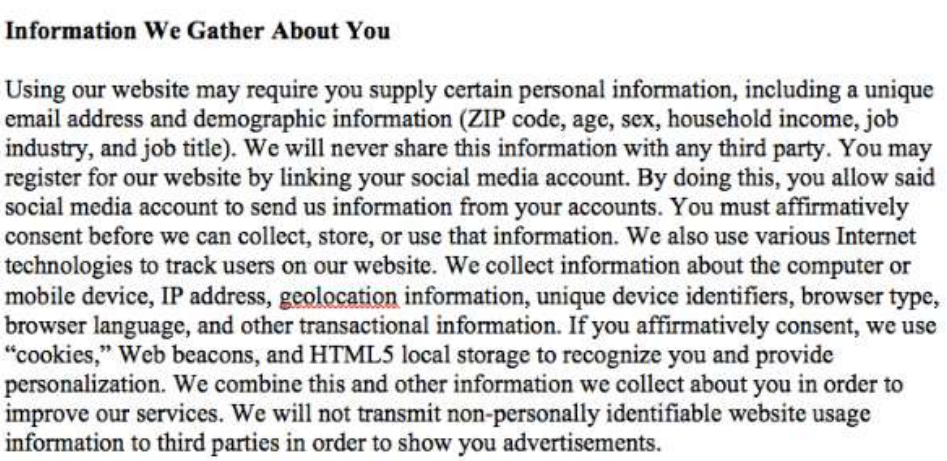
Figure 1



Information We Gather About You

Using our website may require you supply certain personal information, including a unique email address and demographic information (ZIP code, age, sex, household income, job industry, and job title). You may register for our website by linking your social media account. By doing this, you allow said social media account to send us information from your accounts, and you authorize us to collect, store, and use transmitted information. We also use various Internet technologies to track users on our website. We may collect information about the computer or mobile device, IP address, geolocation information, unique device identifiers, browser type, browser language, and other transactional information. We use "cookies," Web beacons, and HTML5 local storage to recognize you and provide personalization. We combine this and other information we collect about you in order to improve our services. We may transmit non-personally identifiable website usage information to third parties in order to show you advertisements.

Figure 2



Information We Gather About You

Using our website may require you supply certain personal information, including a unique email address and demographic information (ZIP code, age, sex, household income, job industry, and job title). We will never share this information with any third party. You may register for our website by linking your social media account. By doing this, you allow said social media account to send us information from your accounts. You must affirmatively consent before we can collect, store, or use that information. We also use various Internet technologies to track users on our website. We collect information about the computer or mobile device, IP address, geolocation information, unique device identifiers, browser type, browser language, and other transactional information. If you affirmatively consent, we use "cookies," Web beacons, and HTML5 local storage to recognize you and provide personalization. We combine this and other information we collect about you in order to improve our services. We will not transmit non-personally identifiable website usage information to third parties in order to show you advertisements.

Thirty-six percent recognized that Figure 2 offered stronger privacy protections. The only statistically significant predictor of seeing through the manipulative potential of privacy policy design was knowledge of the legal implications of privacy notices. In particular, the odds of accurately identifying privacy protective practices in a privacy notice is 1.98 times greater for those who

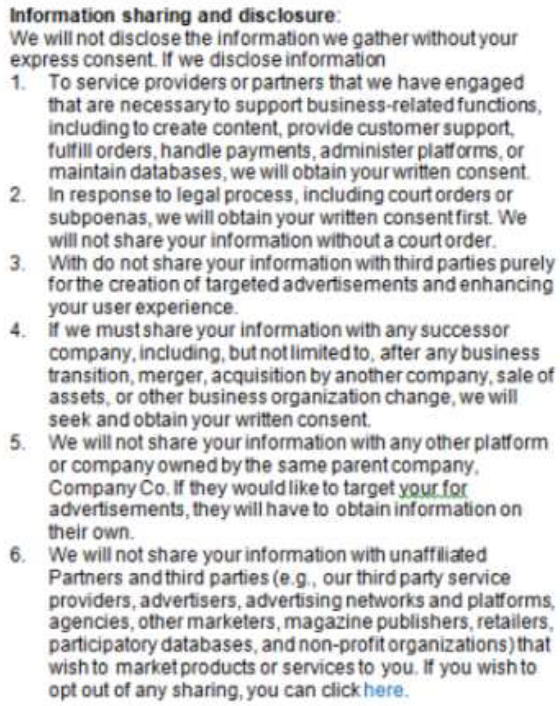
answered questions about the legal implications of privacy policies correctly than those who did not. Table 1 displays the results in more detail, showing that age, education, gender, income level, time online, networked level, and even the extent to which one reads privacy policies are not significant predictors of seeing through policy design.[49]

Similarly, when given the choice between another set of policies that paired a graphically designed notice with invasive practices (Figure 3), on the one hand, and a traditionally designed policy with protective practices (Figure 4), on the other, the sample split down the middle, with 49.1% choosing Figure 4. Again, knowledge of privacy law was a statistically significant predictor of identifying the stronger privacy protections.

Figure 3

49 *See infra* Part II(C).

Figure 4



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. With 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. If they would like to target your for advertisements, they will have to obtain information on their own.
6. We will not share your information 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. If you wish to opt out of any sharing, you can click here.

Specifically, in this question, the odds of identifying the privacy protective practices were 1.81 times higher for those who understood the legal implications of privacy policies than for those who did not. These results are also displayed in Table 1.[50]

50 Notably, age was a significant factor here, as well. The data suggests that every one year increase in age is associated with 1.025 greater odds of seeing through design differences to identify the privacy protective practices. Age was not a significant factor anywhere else in this study, suggesting that it does not play a strong role overall.

C. Discussion and Limitations

Table 1:
Factors that Predict Choosing Strong Privacy Protections Despite Notice Design

	Q: Figure 1 or Figure 2		Q: Figure 3 or Figure 4	
	Exp(B)	Sig.	Exp(B)	Sig.
Privacy Law	**1.976**	**.000***	**1.811**	**.000***
Age	1.005	.578	1.025	.006*
Gender	0.767	.189	1.105	.612
Education	1.165	.216	1.038	.751
Income	0.950	.516	1.019	.804
Networked	1.112	.100	0.916	.166
Time Online	1.079	.743	0.733	.160
Read Policies	0.941	.579	1.182	.109

*p < 0.05

The data suggests that greater awareness of the legal implications of privacy notices is associated with a more discerning approach to interpreting those policies. This makes sense. More than twenty years ago, Alan Westin suggested that "privacy fundamentalists," or those who value privacy highly, are more active about protecting their information than the "privacy unconcerned," or people who have few qualms about giving over personal information to others.[51] Assuming Westin was, and still is, correct, greater concern about privacy is likely to translate into greater self-education, which, in turn, will likely result in more effective decisionmaking.

This suggests that if policymakers would like to enhance internet users' ability to make discerning privacy choices under the notice-and-choice regime, the most effective steps involve greater education. Granted, privacy policies must be readable. They also must be designed with real users in mind. But the data presented here suggests that in addition to improving the transparency of the policies themselves, greater public education about privacy and privacy notices can improve consumers' ability to interact with those policies and make the choices they want.

And there is great need for this public education. Recently, Joseph Turow and his colleagues found that large percentages of Americans are making consumer choices based on inaccurate assumptions.[52] Turow found that 65% of people "d[id]

51 *See Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the Subcomm. on Commerce, Trade & Consumer Prot. of the H.R. Comm. on Energy & Commerce*, 107th Cong. 15–16 (2001) (statement of Alan F. Westin, Professor Emeritus, Columbia University, President, Privacy and American Business). Westin referred to everyone else as "privacy pragmatists," or those who make case by case privacy decisions based on midlevel concern about privacy and average distrust in government, business, and technology. *See id.* at 16.

52 *See* TUROW ET AL., *supra* note 42.

not know that the statement 'When a website has a privacy policy, it means the site will not share my information with other websites and companies without my permission' is false."[53] This study confirms this ongoing ignorance. Turow also found that most Americans, even those with the capacity to do so, do not weigh costs and benefits when deciding to give up their data; rather, they are resigned to it.[54] And those resigned to their inability to control their data make risky privacy choices and allow marketers to use consumer data with impunity.[55] However, the data presented in this Essay suggests that greater education about privacy policies and their implications could have an ameliorative effect on the deterioration of consumer confidence and trust in the use of data.

That said, this study is subject to certain limitations. A sample set of approximately 500 respondents is adequate but still relatively small. Additional research is necessary to replicate this study on a larger scale. Furthermore, knowledge of privacy law could be measured in different ways. For ease of statistical analysis, anyone who marked a false statement as "True" was considered to lack knowledge of the legal implications of privacy policies. Only those who marked either one or both true statements as "True," without any others, were categorized as knowledgeable. Although this strategy accurately reflects knowledge on a dichotomous scale, it misses nuance and partial accuracy.

CONCLUSION

The design of privacy policies affects users' ability to comprehend the substance of those policies. Design can make information more readable and understandable; it also can obscure, confuse, and manipulate. Design is not neutral. This Essay adds to the scholarship of the relationship between notice design and user comprehension by showing that greater awareness of the legal implications of privacy policies is associated with more discerning approaches to interpreting those policies. In particular, those internet users who correctly identified certain facts about the law of notice-and-choice were statistically more likely to identify privacy policies that offered stronger privacy protections in spite of manipulative design strategies. This suggests that in addition to mandating improvements in notice readability and design, policymakers should commit themselves to educating the public about privacy law basics and the legal implications of privacy notices.

53 *Id.* at 4.
54 *Id.*
55 *Id.* at 5.