

Does “Notice and Choice” Disclosure Regulation Work?

An Empirical Study of Privacy Policies

Florencia Marotta-Wurgler¹

NYU Law School

April, 2015

Abstract: This paper studies online privacy policies for six markets often associated with privacy concerns: dating, social networking, message boards, news and reviews, cloud computing, and gaming. For each of 248 policies in the sample, I track 69 specific terms, including terms pertaining to notice, data sharing, enforcement, security, and other features. In addition to providing a window on modern privacy policies, the evidence calls into question the efficacy of the current “notice and choice” regulatory model. Modern privacy policies are often vague, internally contradictory, offer little protection, or are silent on critical points. While one-third of sample policies claim compliance with a self-regulatory benchmark such as the FTC’s guidelines, only a fraction of the actual terms in these policies actually are consistent with the standard. In general, the analysis of modern privacy policies indicates a need to reevaluate current practices and think about alternatives, such as establishing privacy default rules to fill in incomplete contracts and reduce firms’ incentives to obscure and obfuscate their information practices in their privacy policies.

¹ New York University School of Law. I would like to thank Daniel Svirsky and Robert Taylor for outstanding work on the project, Oren Bar-Gill, Kevin Davis, Chris Hoofnagle, Kirsten Martin, Helen Nissenbaum, Katherine Strandburg, Ira Rubinstein, Jeff Wurgler, Kathryn Zeiler, participants at the Privacy Law Research Scholars Conference, NYU Law Summer Workshop, 2014 Conference of Empirical Legal Studies Conference, University of Houston Law Center Faculty Workshop, Boston University Law and Economics Workshop, members of the Privacy Research Group at New York University for helpful comments and suggestions, and Conference of Empirical Legal Studies 2014 participants. I would also like to thank Amanda Conley, Nicolas Heliotis, Julianne Markel, Isaac Sasson, Luke Smith, Melissa Quartner, Christopher Van Zele, and JingJing Wu for outstanding research assistance.

Introduction

Billions of people use the Internet every day to read the news, check email, connect with friends on social networks, buy groceries, to use a search engine to answer a particular question or find a site or document, and so on. Every keystroke and mouse-click flows into a stream of information on that individual's characteristics, needs, wants, and life. Companies can and often do collect this information for commercial purposes such as constructing user-specific profiles to target content or advertising or to share with third parties.²

In light of the evidence that consumers care about their information privacy and of the potential costs associated with the unknown use or leaks of such information,⁴ policymakers are constantly considering whether the current regulatory model of consumer information protection should be revised and whether bounds should be placed on the collection, use, and security of personal information.⁵ Together with some state laws, consumer information has been protected by a self-regulatory regime articulated and by the Federal Trade Commission (FTC) that is generally referred to as “Notice and Choice” (N&C) and is predominantly based on disclosure.⁷ Although it's been revised a number of times since its inception, the regime essentially asks that companies adopt privacy policies explaining their practices related to the collection, use, sharing, and security of consumer information and that they adopt “Fair Information Practices” (FIPs) promulgated by the FTC through self-regulation.⁸

The goal of disclosure is to encourage firms to “compete on privacy” by allowing consumers to become informed (either by reading policies or relying on third party

² Tal Zarsky, *Transparent Predictions*, Ill L. Rev. 1503 (2013).

⁴ See Section I.A for a detailed account.

⁵ See, e.g., Data Broker Transparency and Accountability Act, S. 2025 (2014); Data Security and Breach Notification Act of 2014, S. Cybersecurity Act of 2013. S. 1976, (2014); 1353, 113th Congress (2013-2014); Personal Data Privacy and Security Act of 2014, H. R. 3990 (2014); Geolocation Privacy and Surveillance Act, H. R. 1312 (2013); Email Privacy Act, H. R. 1852 (2013); Location Privacy Protection Act of 2014, S. 2171 (2014); Eliminate Privacy Notice Confusion Act, H. R. 749 (2013); Alexis Agin Identity Theft Protection Act of 2013, H. R. 2720 (2013).

⁷ See Ben-Shahar and Schneider, *More than you Wanted to Know*, Princeton University Press (2014); Oren Bar-Gill, *Seduction by Contract* (Oxford University Press, 2013.)

⁸ Federal Trade Commission, *Privacy Online: A Report to Congress* 7 (1998), http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf. California law also requires that firms adopt privacy policies giving notice of their privacy practices. See CAL. BUS. & PROF. CODE §§ 22575-22577 (West 2008).

certification seals) and visit firms with desired information protection practices.¹² In theory, disclosure can alleviate market failures that stem from asymmetric information while preserving consumer choice. The reality of disclosure can be more complicated, however, and N&C has been harshly criticized as ineffective.¹³ Indeed, early evidence revealed that for the most part, companies failed to embrace the first set of FTC's fair information practice principles, and a number of industry-wide initiatives—such as seal—closed down after a few years of operation or become subject to industry capture.¹⁴ Further, while privacy policies have been widely adopted, they have been found to be long and hard to read.¹⁵

Despite the early setbacks, current approaches, both at the state and federal level, continue to embrace disclosure-based solutions and self-regulation to protect consumer information privacy. The most recent ones are the 2012 FTC Report to Congress, *Protecting Consumer Privacy in an Era of Rapid Change*, and the 2012 White House's proposed *Consumer Privacy Bill of Rights* (which was recently evolved into the proposed *Consumer Privacy Bill of Rights Act* of 2015).¹⁶ For the most part, both encourage firms to adopt simplified and clear disclosures in their privacy policies to lower the costs of reading and continue to embrace a self-regulatory regime of adoption of fair information practices.

¹² *Id.*

¹³ See, e.g., Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, *Notre Dame L. Rev.*, 87 (3) 2013. Paul Schwartz, *Internet Privacy and the State*, 32 *Conn. L. Rev.* 833 (2000); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 *Stan. L. Rev.* 1193; *Need for Internet Privacy Legislation: Hearing Before the S. comm. On Commerce, Science and Transportation*, 107 Cong. 18-28 (2001) (statement of Professor Fred Cate); Kirsten E. Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Online Privacy*, *First Monday*, Vol. 18, 12-2, 2013. M

¹⁴ See, e.g., Chris Jay Hoofnagle, *Privacy Regulation: A Decade of Disappointment (2005)*, available at <http://epic.org/reports/decadedisappoint.html>. Mary Culnan, *Protecting Privacy Online: Is Self-Regulation Working?* *J. Pub. Pol. and Mtng.*, 19 (1) (2000); See Robert Gellman & Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States (2011)* (summarizing studies suggesting that industry's early self-regulatory initiatives failed) available at <http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf>.

¹⁵ See, e.g., Alicia McDonald and Lorrie Cranor, *The Cost of Reading Privacy Policies*, *J. of Law and Pol. for the Information Society* (2008) (estimating that it would take an average 244 hours per year for each individual to read the privacy policies of each web site visited once a month for a total cost of \$3,534 a year). Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 *Penn. St. L. Rev.* 587 (2007).

¹⁶ FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change*, (2010), available at <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>.

For the standing FTC regime to be effective, two important conditions must be met. First, the privacy policies must communicate company information practices to individuals—or, more likely, intermediaries—in a manner that would enable individuals to make informed choices. Second, companies must follow the FIPs in the most recent FTC guidelines, including the inclusion of some new substantive protections. Of course, consumers must read this information and act on it in a way that improves their wellbeing.

This paper is the first to examine empirically the extent to which the N&C model, as articulated in the most recent FTC guidelines to Congress, has achieved these two main goals. The results should also inform existing debates regarding the desirability of disclosure and self-regulation in consumer markets.

I study the content of the privacy policies of 248 firms from six different online markets where people often share personal and personally identifiable information (albeit to different degrees)—social networks, dating sites, cloud computing, gaming sites, news and reviews, and forum/special interest sites. These are services where consumers actively provide private information and thus more likely to know or care about the companies' information practices. Given their characteristics, these services' privacy policies make for an interesting and potentially revealing sample.

I graded policies on sixty-nine terms related to categories that commonly appear in privacy policies and which are referenced in the FTC guidelines, among others. The categories relate to notice regarding the collection, use and sharing of information, consumer access to data, control of information, data security, data practices, enforcement and opportunities to seek redress, change of terms clauses, and company adoption of substantive privacy protection measures.

To measure firms' compliance with self-regulatory guidelines, I create a set of benchmarks using relevant subsets of the graded terms. I measure the content of each policy against the two most recent information privacy guidelines, those outlined in the FTC 2012 Report to Congress, and those in the 2012 White House Consumer Privacy Bill of Rights, which for the most part complement the FTC guidelines. I account for the possibility that companies are sluggish in updating their policies to comply with the new framework by measuring the extent to which the sample policies comply with the

previous FTC guidelines, outlined in a 2000 FTC Report to Congress. Most firms operate internationally and must comply with other regulations. I account for this by analyzing the extent to which the companies comply with the US-EU Safe Harbor Framework, a self-certification program operated by the Department of Commerce designed for companies who seek to comply with the privacy standards of the European Union. Finally, to get a more comprehensive sense of current information privacy practices, I measure the extent to which the policies comply with three widely regarded fair information practices standards: the original FIPs, as outlined in the influential 1973 Report by the Department of Health, Education, and Welfare, the 1980 OECD Privacy Guidelines, and the 1995 EU Data Directive.¹⁷

The results are revealing. First, it is unlikely that these contracts offer reasonably effective notice. Privacy policies are long; 2,227 words on average. Further, they are often silent on important categories, making it impossible to know how information is collected and used. For example, 40% fail to disclose whether the firms collect content information, such as the subject matter of communications, stored documents, and media, even though consumers are likely sharing that information on the site. Silence is problematic in this context because there are no clear gap-filling default rules, such as those of Article 2 of the UCC. While there is some guidance from judicial opinions and FTC enforcement actions under Section 5 of the FTC Act, these mostly address companies' failure to comply with explicit commitments made in their privacy policies and are thus unlikely to be informative about the meaning of contractual silence.¹⁸

When terms are included, they are written in language that is often vague or ambiguous. For instance, almost all contracts use terms such as "affiliates" or "third parties" when discussing the recipients of shared information, but only 7% define them. Almost all contracts condition their language with words such as "may," or "might," when disclosing their information practices (e.g. "we may share your information with affiliates"). Such phrases appear an average of 20 times per contract. Policies also include contradicting statements and ill-defined actions. These features, when combined,

¹⁷ See U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORTS OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973).

¹⁸ 15 U.S.C. § 45. For a full discussion of the FTC jurisprudence, see Daniel Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014).

make understanding the terms a challenging endeavor. Indeed, coding the terms in this sample often times resulted in disagreement among individuals with legal training, some quite extensive.

An evaluation of compliance with self-regulatory guidelines more generally leads to similar results. The majority of firms tend to comply with 30% to 40% of the requirements of the 2012 FTC guidelines and 20% to 40% of the 2012 White House report, even though preliminary reports have been circulating since 2010. This includes failure to comply with substantive protections that go beyond disclosure. Even firms who claim to adhere to the US-EU Safe Harbor Agreement, which is required for US firms who wish to store data of citizens of EU member countries, do not do so completely. Indeed, over two-thirds of the firms that claim compliance comply with only 10% to 50% of its requirements. Due to limitations in the methodology, such as relying only on the written statements in privacy policies and not actual company behavior, these numbers are suggestive and should be interpreted as offering a rough measurement of compliance. Nevertheless, the results offer a sobering assessment of current regulatory approaches and invite us to consider approaches that move beyond self-regulation.

In sum, the paper makes three contributions. First, it evaluates whether firms have embraced N&C disclosure regulation, as measured by the content of their privacy policies. Second, it offers a snapshot of current information privacy practices from a wide range of firms in six markets where information sharing is pervasive. Finally, it evaluates such practices against a number of meaningful frameworks, such as the original Fair Information Practice Principles.

The evidence suggests that notice and choice disclosure regulation is failing. Policies are long, complex, ambiguous, incomplete, and often silent on important subject matters. These features make it impossible to understand them and for intermediaries to digest them in a consumer friendly manner. A possible way to address it would be to articulate a series of default rules, perhaps based on a version of FIPs, that would reduce companies' incentives to obfuscate their practices to avoid being subject to FTC enforcement actions. There are limits to what can be achieved by disclosure regulation, but given the potential costs of direct regulation, especially in continually evolving

markets, the articulation and implementation of some basic default rules seems likely to be valuable.

While the study offers a rich analysis of the effectiveness of N&C, it has a number of limitations. First, it cannot examine company practices beyond those disclosed in privacy policies. To the extent these differ, this would limit the conclusions of the analysis. Second, the finding that companies have for the most part failed to adhere to the current information privacy framework does not necessarily imply that there is a market failure. Policies might spell onerous practices but might nonetheless be constrained by reputation or fear of litigation or enforcement actions under the FTC's "Unfair and Deceptive Practices" Act. Finally, even if companies complied with all disclosure requirements, it is not clear that compliance will induce consumers to read, understand, and act on the information conveyed by firms. Compliance with substantive protections, however, might increase consumer protection.

The paper proceeds as follows. Section I offers a brief overview of the laws governing consumer information privacy online as well as the literature on valuation of information privacy. Section II provides background on the current literature of privacy policies and self-regulation. Section III explains the sample and methodology. Section IV presents the main analysis. Section VI discusses the implications of the results and concludes.

I. Background

A. Consumer Attitudes Towards Information Privacy and Privacy Policies

A number of survey and experimental studies reveal that consumers value information privacy, yet also appear to have difficulty understanding the costs associated with giving away private information.¹⁹ Consumers are reluctant to share information

¹⁹ See, e.g., Aleecia M. McDonald and Lorrie Faith Cranor, *An Empirical Study of How People Perceive Online Behavioral Advertising*, CMU CyLab Working Paper 09-015 (2009) (conducting a series of interviews and finding that when consumers are asked about online advertising, the consumers immediately raise privacy concerns without prompting); Alessandro Acquisti and Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 SECURITY & PRIVACY 26 (2005) (using a survey to find that consumers claim to value privacy highly, for monetary and non-monetary reasons, and that consumers

with third parties in a variety of contexts and believe that the information on their mobile phones is private.²⁰ Laboratory experiments have shown that in some settings consumers are willing to pay to protect their private information from being disclosed.²¹ Yet these results are susceptible to context and framing.²² Another study found that consumers believe that when firms adopt privacy policies their information is more likely to be protected.²³ A concern is that consumers' misperceptions and misunderstanding will dilute firms' incentives to protect private information and may increase the need for regulation.²⁴

B. Consumer Information Privacy Regulation in the United States: A Disclosure Based Approach

would welcome government intervention to protect privacy); Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook in Privacy Enhancing Technologies* in PRIVACY ENHANCING TECHNOLOGY (2006) (finding that Facebook users care a lot about privacy but are unaware of Facebook's privacy policies or hold incorrect beliefs about Facebook's policy); Joseph Turow, Chris Jay Hoofnagle, Deirdre Mulligan, Nathaniel Good, & Jens Grossklags., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 723, 729–32 (2007–08) (collecting survey evidence that consumers worry about online privacy and that consumers believe privacy policies are meant to protect them); Alessandro Acquisti, Leslie John, George Loewenstein., *What is privacy worth*, WORKSHOP ON INFO. SYS. AND ECON. (2009)

²⁰ See e.g., P. G. Leon, B. Ur, Y. Wang, M. Sleeper, R. Balebako, R. Shay, L. Bauer, M. Christodorescu, and L. F. Cranor (finding that 50% a sample of 2,912 survey participants on a medical website would be unwilling to share any information when asked about it, and that factors such as the scope of use and data retention period affected individuals' decision to share personal information with the site.); Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, *Mobile Phones and Privacy*, Jul. 11, 2012, available at <http://ssrn.com/abstract=2103405> (surveying 1,200 individuals and finding that most consider information in their phones to be private and reject information collection by content providers and third party vendors.); Avi Goldfarb & Catherine Tucker, *Shifts in Privacy Concerns*, *American Econ. Rev.* (2010) (examining over three million responses over eight years and finding increased reluctance to share information over time).

²¹ *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 254 (2007).

²² Alessandro Acquisti, Leslie K. John and George Loewenstein, *What is Privacy Worth?* *J. Legal Stud.* 42(2) 249-74 (2103) (showing that privacy valuations are extremely context dependent and concluding that despite this, individuals care about privacy.)

²³ See Chris Jay Hoofnagle & Jennifer King, *What Californians Understand about Privacy Online* (2008) ("In a way, consumers interpret privacy policy as a quality seal that denotes adherence to some set of standards.") available at <http://ssrn.com/abstract=1262130>.

²⁴ *Id.*

With the exception of these specific statutes and some state laws,²⁵ consumer information privacy protection in the United States is primarily based on disclosure and self-governance principles enacted by the FTC.²⁶ In 1997, the FTC created its N&C model encouraging firms to adopt privacy policies outlining their information practices, obtaining consent from consumers for uses of information extending beyond the original collection purpose, and embracing fair information practices through self-regulation.²⁷

The N&C principles stem from the 1973 HEW Fair Information Practice Principles, which outlined eight substantive practices on the collection and use of personal data, including imposing limits on the collection and use of information, requiring entities to articulate purposes for which data is being obtained, requiring consent for uses beyond those purposes, and giving access to individuals' own data, among others.²⁸ The HEW FIPs have been regarded as a gold standard and have become the foundation of all subsequent fair information privacy protection guidelines.²⁹ For example, the European Union's 1995 Data Protection Directive establishes common substantive rules for information privacy regulation based on these principles.³⁰

In addition to the principles of notice and choice, the FTC FIPs have focused on access, security and enforcement. Specifically, "access" requires companies to provide individuals access to their own data and an opportunity to correct mistakes. "Security"

²⁵ While Congress enacted laws regulating information privacy in particular sectors, states, in particular California, have been actively innovating on the information privacy front. For example, California's Data Breach Notification Law of 2002 became a model for other states, most of which followed suit. CAL. CIV. CODE §§ 1798.29, 1798.82. California also enacted the California Privacy Protection Act, which entitles consumers to find out how their personal information is shared by companies for marketing purposes and also encourage companies to allow consumers to opt-out of such sharing. CA Civil Code § 1798.83 (2003). Other states, such as Nebraska and Pennsylvania, enacted laws prohibiting companies from making false or misleading statements in their privacy policies. Nebraska Stat. § 87-302(1); 18 Pa. C.S.A. §4107(a)(1).

²⁶ FTC, Privacy Online: A Report to Congress, available at <http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>.

²⁷ See FTC, Privacy Online, Report to Congress 1998, available at <http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>

²⁸ The eight principles are collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. HEW Principles, *supra* note ____.

²⁹ US Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens, Chapter IV: Recommended Safeguards for Administrative Personal Data Systems (1973), available at <http://epic.org/privacy/hew1973report/default.html>. The Fair Information Principles include limits on companies' use of personal information, data collection, and disclosure of such information. They also require that collection and use of information be relevant and accurate; that individuals are given notice, access, and the right to correct information; transparent processing systems; and security measures to protect such information.

³⁰ See Paul Schwartz, The EU-US Privacy Collision: A Turn to Institutions and Procedures. 126 Harv. L. Rev. 1966 (2013).

requires that entities take reasonable steps to adequately protect the information collected. “Enforcement” requires the adoption of a mechanism capable of providing sanctions for non-compliance. To complement the self-regulatory framework, the FTC began enforcing Section 5 (“Unfair and Deceptive Practices Act”) against companies who violated the commitments made in their own privacy policies.³¹ The FTC has since brought numerous enforcement actions for privacy policy violations against firms like Sears, Facebook, Google, and Microsoft.³²

While the threat of an FTC enforcement action for privacy policy violations would possibly reduce firms’ incentive to adopt privacy policies, (especially if consumers were not attentive to these practices), adoption became widespread. This is partly due to California’s enactment of the Online Privacy Protection Act, which requires operators of commercial websites that collect personally identifiable information of California residents to post a privacy policy in a conspicuous manner and to abide by it. In addition, the US-EU Safe Harbor Framework requires companies wishing to transfer personal data of European Union (EU) citizens to non-EU locations to abide by certain requirements, including having a privacy policy.³³

Despite widespread adoption of privacy policies, early studies found weak compliance with notice and choice.³⁴ A 2010 FTC preliminary report to Congress summarized part of this research: “The Notice and Choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand.”³⁵ This should not be surprising, as other forms of disclosure regulation have been found to be similarly unsatisfactory.³⁶

In reaction to this, the FTC urged Congress to enact legislation setting forth a basic level of privacy protection for commercial web sites that collect personally

³¹ See note 18 *supra*.

³² For a review of FTC enforcement actions, see Solove & Hartzog, *supra* note 18.

³³ Cal. Bus. & Prof. Code §§ 22575-22579. The policy must also comply with a number of requirements, such as identifying the categories of personally identifiable information collected and post an effective date of the policy, among others.

³⁴ For a review of the failure of codes of conduct and privacy seals, see Robert Gellman and Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, (Oct. 14, 2011) available at <http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf>.

³⁵ FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 16

³⁶ See Omri Ben-Shahar & Carl Schneider, *supra* note 7 (for a thorough review of the failures of mandated disclosure); Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI’s “Principles of the Law of Software Contracts,”* 78 U. Chi. L. Rev. 165 (2011).

identifiable consumer information. Yet in its most recent report to Congress in 2012, *Protecting Consumer Privacy in an Era of Rapid Change*, the FTC insisted on disclosure by urging firms to make their disclosures clear and conspicuous, without conflicting or internally contradictory language. In addition, it recommended that firms offer a summary of their information practices, called “layered notice,” at the top of their privacy policy.³⁷ The report also included substantive recommendations, such as asking firms to adopt “privacy by design;” that is, take business decisions that are mindful of consumer privacy throughout their business operations.³⁸ Privacy by design requires firms to limit data collection and retention, adopt reasonable security and data accuracy measures, and implement data management procedures.³⁹

Also in 2012, due to increased awareness to consumer information privacy, the Obama administration released a report, *Consumer Data Privacy in a Networked World*, where it urged for the adoption of legislation that would create baseline privacy protection standards. However, it also encouraged self-regulation through the adoption of voluntary codes embracing the FTC FIPs and a disclosure-based approach.⁴⁰

While a number of privacy bills were introduced in Congress in the wake of the report, none made it into law.⁴¹ A number of new bills wait in Congress and several state legislatures, fates pending.⁴²

II. Prior Literature

As noted earlier, privacy policies have been at the center of N&C model of consumer protection. They have been found to be long and at a linguistic complexity

³⁷ See, FTC “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers,” Report to Congress 2012, [hereinafter FTC 2012 Report] available at <http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy>.

³⁸ Id.

³⁹ The report also recommended the implementation of a “Do Not Track” mechanism allowing consumers to control the collection of their data. Id.

⁴⁰ FTC 2012 Report, White House Consumer Privacy Bill of Rights.

⁴¹ See, e.g., Sen. Leahy Personal Data Privacy Act of 2009 (S. 1490); Sen. Feinstein, Data Breach Notification Act of 2009 (S. 139); Kerry-McCain, The Commercial Privacy Bill of Rights of 2011 (S. 799), Franken-Blumenthal, The Location Privacy Protection Act of 2011 (S. 1223).

⁴² CITE

typically requiring at least two years of college to fully grasp.⁴³ Indeed, it has been estimated that it would take individuals about 201 hours a year to read all the privacy policies of the sites they visited.⁴⁴ It is thus not surprising that people don't read them.⁴⁵ Privacy notices themselves have also been found to confuse consumers.⁴⁶

Early evidence suggests that companies have also failed to adopt FIPs. In a report entitled *Privacy Online: Fair Information Practices in the Electronic Marketplace* in 2000, the FTC reported the findings from a study of 100 privacy policies that about 20% to 40% complied with FIPs. It also found that 40% to 60% complied with just the notice and choice principles, as did 60% of the most popular firms. The report employed a generous notion of compliance (i.e., the notice requirement would be met if the privacy policy disclosed at least some information collected from the individual, not all of it). It also found that firms did not adhere to voluntary codes, such as privacy seal certification programs, as much as originally desired.

A 1999 study by EPIC tracked ten terms in the 100 most popular sites and found weak compliance with current FTC guidelines.⁴⁷ The most recent study evaluating the standardized privacy policies of thousands of financial institutions using a machine learning approach and found that very few comply with the requirement of the Gramm-Leach-Bliley Act, a statute mandating particular disclosure of financial information by specific financial institutions.⁴⁸

This study builds on and improves this literature in a number of ways. First, it offers the first empirical analysis examining compliance with the most recent FTC guidelines. Second, it contrasts compliance with other relevant privacy guidelines. Third,

⁴³ C. Jense & C Potts, Privacy Policies as Decision-Making Tools: an Evaluation of Online Privacy Notices. SIGCHI. 2004. Xinguang Sheng and Lorrie Faith Cranor, *Evaluation of the Effect of U.S. Financial Privacy Legislation Through the Analysis of Privacy Policies*, 2 INFO. SCI. J. OF L AND POL'Y 943 (2005)..

⁴⁴ McDonald and Cranor, The Cost of Reading Privacy Policies (estimating that it would take individuals about 201 hours a year to read all the privacy policies of the sites they visited) (2008).

⁴⁵ Privacy Leadership Initiative. Privacy Notices Research Final Results, November 2001, Available at: <http://www.und.erstandingprivacy.org/content/library/datasum.pdf>.

⁴⁶ Chris Jay Hoofnagle & Jennifer Urban, Alan Westin's Privacy Homo Economicus, 49 Wake Forest L. Rev. 261 (2014); Turow, J. Feldman, L., and Meltzer, K. Open to Exploitation: American Shoppers Online and Offline. The Annenberg Public Policy Center. 2005. <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>.

⁴⁷ See Surfer Beware III, available at <https://epic.org/reports/surfer-beware3.html> an discussed in Chris Hoofnagle (2005) <http://epic.org/reports/decadedisappoint.html>.

⁴⁸ Cranor et al, Examining Thousands of Privacy Polices of Financial Institutions. [CITE].

it develops a methodology creating replicable benchmarks against which to measure compliance. Fourth, it analyzes and compares privacy practices and compliance within and across six different and important markets that haven't been analyzed systematically before. Finally, the analysis covers a comprehensive set of terms that give the fullest picture to date on the content of privacy policies.

III. An Empirical Analysis of Privacy Policies

Absent information about the relative costs and benefits of information collection and sharing as well as consumer and firm behavior in regards to information privacy online, it is not possible to establish whether the market for personal information online is working well or requires some form of intervention. We can, however, evaluate whether current approaches to protect consumer information online are being complied with.

These are: the 2012 FTC Report to Congress and on the 2012 White House proposed Consumer Privacy Bill of Rights. These reports have been available as early as 2010, thus giving firms time to adopt the new principles. Yet firms might be sluggish in updating their policies, so I account for this possibility by measuring compliance against an earlier standard, the FTC Guidelines from its 2000 report to Congress. In addition, a number of companies operating beyond the United States might have to comply with other self-regulatory standards. For this reason, I also track the extent to which firms comply with the provisions of the US-EU Safe Harbor. This should offer a more comprehensive account of compliance with self-regulatory standards.

Finally, I measure the extent to which privacy policies comply with three sets of information practice principles that have been set as models for subsequent regimes: the 1977 HEW FIPs, the 1980 OECD Guidelines, and the 1995 EU Data Directive. In the absence of clear default rules, this analysis should help us understand current privacy practices against well-established standards.

A. Methodology and Sample

The sample firms are in six online markets where consumers tend to share personal and sensitive information: dating, social networks, message and special interest, cloud computing, news and reviews, and gaming. Not all markets are the same, of course. Individuals might share more information on dating and social network sites than on gaming and reviews sites. Sharing is also qualitatively different across markets; compare a social network with a cloud computing service. I chose firms in markets where information sharing is salient and potentially extensive because consumers might be more likely to become aware of and care about the privacy policies of the firms with which they interact. With the exception of some games and news sites, the services offered by the sample firms are essentially generated by information shared by users of the sites. This also makes the privacy policy relatively more important. To the (unlikely) extent that consumers shop for firms with good privacy policies, we are more likely to find it here, where consumers are aware that they are sharing personal information and, in some cases, lots of it.

The sample includes 248 firms that conduct business in the United States. They are fairly diverse, and a small minority has greater markets abroad. They include giants like Facebook and Google, as well as dozens of smaller firms (such as veggiedate.com). An initial sample of 150 firms came from companies that were listed in Wikipedia in 2009, 2010, and 2011, as at the time of collection it contained a fairly extensive list for our sample categories.⁴⁹ In 2010, we obtained 36 additional dating sites from the website www.100bestdatingsites.com, by selecting those active sites that catered to individuals in the United States. We obtained 55 additional bulletin board sites from <http://rankings.big-boards.com/>. We have no reason to believe that the firms obtained for the sample will create a substantial bias in the analysis of their privacy policies. The first half of Table 1 reports the summary statistics for each market. Of the 248 privacy policies, 40 are dating sites, 89 are social networks, 50 are special interest/message boards, 18 are news and reviews sites, 28 are cloud computing, and 23 are gaming sites.

B. Firm Characteristics

⁴⁹ The list was originally available at http://en.wikipedia.org/wiki/List_of_social_networking_websites.

Table 1 summarizes the company characteristics that we measure, which might affect the content of privacy policies. About 5% of sample firms are not for profit, a characteristic that might decrease their interest in sharing personal information. Another relevant company characteristic is whether the product or service is offered for free or on a subscription basis, as those firms who earn money from subscriptions might have a decreased need to rely on personal information for revenue. About 40% of sample firms offer at least a portion of their services for a fee, but there are differences across markets. A little over 90% of dating sites, 54% of cloud computing sites, and 57% of gaming sites are on a subscription basis. The remaining markets do not offer subscriptions but premium access, or offer the ability to purchase items for a price. These include 16% of social networks, 3% of message boards, and 28% of news and reviews sites. This last number is partly driven by firms like Amazon.com, who have review forums but also sell merchandise. There are very few firms that offer more than one product or service, so classification is generally easy.

Another relevant category is whether the information collection is especially sensitive. Two percent of the sample companies offer services we labeled “discreet,” because they relate to activities that are generally perceived as highly private. For example, the dating site AshleyMadison.com is for individuals already in a relationship who are looking for an affair. Individuals might care more about privacy in these contexts and thus perhaps pay more attention to privacy policies, which in turn might induce firms to offer better terms. Finally, I track the Alexa Rank from alexa.com, a website that creates rankings on web sites based on the number of monthly visitors and use these rankings as a proxy for company size.⁵⁰ A lower number indicates a more popular site; the mean Alexa rank is 979,193 and the standard deviation is 3,646,845, indicating a large range in the amount of traffic our sample companies get.

IV. Evaluating the Effectiveness of Notice and Choice Regulation

⁵⁰ Alexa.com. Alexa rankings offer just approximate estimates of web traffic because they rely on the metrics provided by those users who install the Alexa Toolbar, which might not be representative of all internet users. Still, there is no reason to believe that the sample we use is particularly biased. Rankings might not be precise, but they are approximate enough to reveal a wide range of company sizes.

A. Contract Characteristics and Notice

This sub section examines whether particular contract characteristics, such as the length of the contract and whether the company adheres to a privacy certification seal, are likely to provide effective notice. These can be found in the second half of Table 1. While the sample firms' data were collected over years, the privacy policies used in this study were all collected in June 2013, thus offering a snapshot of privacy practices as of that time. The first variable, "Year Last Updated," measures the last reported date when the privacy policy was updated. 192 firms include this information in the contract, so we report the "last update" for this subset. On average, contracts in force in June 2013 were last updated in 2010 (median 2011). Cloud computing firms had the most recently updated contracts, perhaps because this is a newer market. Dating sites' policies were on average last updated in 2008. Figure 1 offers a more detailed look by tabulating the number of contracts that were last updated in a particular year. It shows that most had been revised within two years of when we collected them (June 2013). Contracts appear to be revised fairly frequently (based on unreported analysis; this cannot be documented directly by this cross-sectional analysis) which is not surprising given the ever-changing landscape of these markets and the self-regulation initiatives.

While there has been a recent push to standardize and shorten contracts (e.g., being considered in California⁵¹), existing guidelines prescribe no limit to contract length. The average length in our sample is 2,227 words long, approximately the average length of End User Software License Agreements.⁵² The average reader reads about 250 words per minute, so it would take an individual about 10 minutes to read the average privacy policy. Gaming and social networks have the longest contracts, with an average around 2,500 words. Special interest and message board sites have an average of 1,709 words, perhaps because many consumers have the possibility of creating anonymous profiles and offering little personal information. Figure 2 shows that the majority of the sample

⁵¹ See, e.g., AB 242 (proposing to amend California Online Privacy Protection Act to "require the privacy policy of a commercial Web site or online service to be no more than 100 words, be written in clear and concise language, be written at no greater than an 8th grade reading level.)

⁵² Marotta-Wurgler, What's in a Standard Form Contract? An Empirical Analysis of Software License Agreements. *J. Emp. L. Studies* (2007).

policies are between 1,800 and 3,000 words. There is a long right tail. A number of policies are over 4,000 words long, and some are almost 10,000 words long.

Figure 3 combines these variables and shows the average number of words by the year of last update. In 2004, contracts were about 1,200 words on average. Recently updated contracts tended to be longer, with an average of about 2,000 words in 2010, to 2,600 words in 2011, to about 3,300 words for the most recently updated contracts. If the goal is to lower reading costs, the current trend is alarming. Firms revise their contracts by including additional terms or increasing the length of existing ones that increase the cost of reading.⁵³

The cost of reading could be reduced, though, if firms adopt certification seals that signal to consumers the quality of privacy policies without the need of reading them. One of the self-regulatory efforts has been to encourage firms to adopt codes of conduct in the form of privacy seals to adhere to particular frameworks. I track whether a particular firm affirms in its privacy policy that it adheres to a particular privacy seal, such as TRUSTe, or to a particular framework, such as the US-EU Safe Harbor. In this sample, 31% of the companies claim to adhere to a privacy seal or self-harbor agreement. There are wide differences across markets. The highest fraction of seal adherents comes from the cloud computing market, where 68% of firms claim to do so. Companies in this market might feel more pressure to do this because consumers' potential losses associated with the loss or leaking of uploaded information are large and because these companies may have larger businesses as clients, who might insist on certain security measures. In contrast, only 17% of review sites and 18% of special interest message boards adhere to a certification program, perhaps because the nature of the information shared and the possibility of remaining anonymous. With the exception of cloud computing, adherence to seals might probably be too low to confer the benefits associated with it, as consumers might encounter them too infrequently to associate a particular type of contract quality with each. Moreover, it is not clear whether firms actually adhere to the privacy practices of these certification programs.

⁵³ This is consistent with the findings of paper finding that EULAs have grown an average of 30% in length over a seven year period. See Florencia Marotta-Wurgler & Robert Taylor, *Set in Stone? Change and Innovation in Consumer Standard Form Contracts*, N.Y.U L. Rev (2013).

Table 2 explores this further by listing the certification programs that appear in the sample privacy policies. Of the 78 firms claiming to adhere to a benchmark or seal, 58 claim to adhere to the US-EU Safe Harbor and 25 to the US-Swiss Safe Harbor. Firms that want to have a presence in the EU and Switzerland need to comply with the Data Directive's heightened standard. Sample companies claim to adhere to 14 other certification programs in the EU and Australia (such as United Kingdom Information Commissioner's Office and the Australian Best Practice Guidelines for Online Behavioral Advertising). Section V explores the extent to which companies comply with the requirements of the EU-US Safe Harbor. Twenty-one firms include a TRUSTe seal, and 6 firms include different seals, such as PRIVO (specializing in the Children's Online Privacy Protection Act) and Code Blue Security. If seals such as TRUSTe's were supposed to reduce search and reading costs and standardize privacy practices by having firms embrace them widely, this presents further evidence that doesn't appear to be working well. This is consistent with previous evidence from FTC studies reporting low take-up rates of privacy seals.⁵⁴

B. Correlations

Are there particular firm features that are associated with contract characteristics? This section explores the relationship (in the form of correlations) between contract and company characteristics. One would expect that larger firms, who have higher traffic and are likely to gather more information, would have higher incentives to innovate by finding new ways of using data, and thus would modify and update their privacy policies more frequently. The results in Table 3 support this view. It shows that companies with lower Alexa rankings (i.e., higher traffic) are more likely to have updated their policies recently. Higher traffic is also associated with longer contracts and an increased likelihood of certification, a likely cause of the presence of in-house counsel. Larger companies are also more likely to have a larger client base and thus adhere to safe harbor agreements. However, one might have instead imagined that smaller, less known firms would be willing to invest in a third party seal to increase consumer trust. Yet there is no

⁵⁴ CITE

evidence supporting this position, perhaps because consumers don't pay much attention to seals anyway so it might not be worth the expense.

C. Notice and Choice: A Closer Look at Privacy Policies

For notice to be effective, the terms in the policies must be clear and privacy practices must be spelled out completely, especially since there are no default rules that can fill in gaps in the face of contractual silence. This sub-section evaluates the quality of notice in the privacy policies themselves by measuring the extent to which they comply with the disclosure mandates of various guidelines. It also evaluates the extent to which policies are clear by measuring the extent to which they are internally contradicting and include open-ended clauses. We also counted the number of times the contract included words such as "may" or "might," or "from time to time," which might dilute some of their statements.

This and the subsequent analyses are done by tracking 69 terms that appear in eight fair information practice principles, described in Subsection D, such as the 1973 FIPs, the FTC FIPs, and the 2012 proposed White House Consumer Privacy Bill of Rights that related to notice, choice, access, security, and redress, among others. In addition, I track terms that had been identified as important by the FTC in its enforcement actions, previous studies examining privacy policies, and by commentators and industry participants. These include terms giving the firm the right to revise the contract, or giving the company the right to disclose use information to the government, or whether the contract includes dispute resolution clauses such as choice law, forum, and class action waivers.

All contracts were read and graded by hand. Each contract was assigned to a team of eight law students, which was divided in pairs. To increase grading accuracy, each member of a pair read the entire contract and graded a specific portion of it independently. Each contract was thus graded twice. The team of students and I would meet periodically to discuss any discrepancies in grading and decide on the proper classification. As the number of contracts graded, the number of discrepancies among graders decreased, but did not disappear. In fact, discussions over particular terms were

usually long. This is because these contracts include ambiguous clauses and often times give rights that cannot be exercised. For example, a common practice is to tell consumers that they are given a choice as to how their personal information can be shared, but then do not explain how that choice can be exercised and do not offer the choice outside the contract. Other times firms would state that their information would not be shared, only to list several lines below that it might be shared with third parties, or might be shared with user consent—but it was never clear whether choice was opt-in or opt-out, or even a choice. The legal interpretation of these clauses is complex, as many are arguably deceptive, and thus not enforceable. Also, if the statement such as “we do not share your information” is considered a warranty, then a company cannot later disclaim it in the same document.

These issues aside, we graded the contracts in a strict sense. Choices that were not made clear were not counted as choices and statements that were later retracted were not counted as affirmations of fact (even though courts would most likely interpret such retraction as against the drafter, we did not code them as choices because we wanted to document company practices).

All 69 terms are listed in Table 4. The first column lists the particular terms that we track. The second column explains how each term was scored. Notice and choice (as well as other guidelines) require that companies disclosure information practices specifically and explain, among others, what type of information, if any, is being collected, how it is collected, and with whom it is shared. To measure compliance, we track the extent to which policies are silent on each of these required areas of disclosure. To measure compliance with the choice requirement, we noted whether choices offered, were opt-in or opt-out.

The first 26 terms relate to the principle of notice, whose objective is inform individuals about the information practices of the firms to allow consumers to make informed choices. The first couple of terms describe the extent to which notice of the policy is prominent (as encouraged by the FTC⁵⁵) show that about 90% of companies make their privacy policies available on their main page, but only 18% require users to expressly agree to them. While it has become customary for individuals to visit sites

⁵⁵ CITE

without having to explicitly agree to any terms (otherwise it would be too burdensome to surf online), even firms that require users to register and sign up, such as social networks (20%) and dating sites (25%), do not generally require users to explicitly agree to their privacy policies. This is probably because users are asked to agree to Terms of Use, which incorporate Privacy Policies by reference. To the extent that privacy policies are relatively important in sites such as social networks and dating sites, current contracting practices make it harder for consumers to become informed. This distinction might not matter. Clickwraps (contracts where consumers are asked to click on “I agree”) tend to be ignored, anyway—at least when it comes to software contracts—.

Still, the reduced notice of the contract might decrease the probability that it will be read. The FTC’s 2012 recommendation that privacy policies include short, or “layered” notices, summarizing the most important terms of the policies, doesn’t appear to have picked up yet, as only 22% of contracts include one. These numbers are being driven by the privacy policies in cloud computing, where almost half of them include layered notices. In contrast, only 10% of dating sites and special interest boards include them. Procedural notice is thus somewhat lacking, at least as compared to the standards created by the FTC.

The next series of terms report the extent to which firms disclose which types of data they collect. The overwhelming majority report they collect contact, computer (IP address, etc.) and interactive (browsing behavior, search history, etc.) information. About half collect financial information, most likely to process the transactions consumers complete in their sites. Forty-three percent collect content information, including personal communication, stored documents, and media, and 28% collect sensitive information, such as race, religion, sexual orientation, social security numbers, etc.). The nature of the information that is possibly collected by these sites increases the probability that consumers might care about the information collected. A smaller percentage of firms explicitly state that they do not collect contact (3%), computer (2%), interactive (12%), financial (2%), and content (16%) information. A notable exception is that 40% of firms explicitly state that they do not collect sensitive information, perhaps due to the influence of the EU Data Privacy directive, which treats sensitive information differently. Note that these practices vary widely by market. Only 5% of dating sites deny collection of such

information, whereas 50% of social networks do. Roughly about one third of times, however, privacy policies do not disclose whether they collect these classes of personal information or not, making it hard to put consumers on notice of their private information practices.

Failure to disclose a particular practice is hard to understand because it is unclear whether firms are allowed to engage in particular behaviors if they don't disclose them. Until very recently, the FTC has only gone after firms that violated explicit statements in their privacy policies, leaving room to conclude that undisclosed information practices are allowed unless they are unfair and deceptive in other ways. In a recent case, however, the FTC stated that a company that suffered two data breaches had a duty to provide reasonable security measures.⁵⁶ At least with respect to data security, there appears to be a background rule requiring firms to offer reasonable protection.⁵⁷

The data also show that 93% of firms claim to use cookies; 2% explicitly state that they do not do this, and 5% do not disclose whether they do. We next measure whether firms commit to use data for stated, context-specific purposes, as recommended by most guidelines, including the 2012 FTC Principles and Consumer Bill of Rights.⁵⁸ Only 26% claim to use personal information for internal business purposes, but, again, the results vary by market. Whereas only 15% of dating sites commit to use the information exclusively for internal business purposes (i.e., administering the transaction, communicating with the user, etc), 42% of special interest and message boards commit to do so. One of the reasons explaining these differences is that dating sites sit on a treasure trove of personal information, making it more costly not to exploit. It could also be that message boards want members to be candid and thus encourage this with relatively stronger privacy protections. Of course, this assumes individuals are informed about privacy practices. Similarly, only about 25% commit to using personal information for context-specific purposes; that is, uses that user would expect given the nature of the site.

Next are terms notifying users about the company's practices regarding the sharing of personal information. Sixty four percent allow third parties to track user

⁵⁶ See Wyndham case.

⁵⁷ See Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014)

⁵⁸ For a detailed account of the role of context, See Helen Nissenbaum, *PRIVACY IN CONTEXT*. See also Katherine Strandburg.

behavior and only 1% explicitly states they do not allow third party tracking. The rest do not disclose this. Only 10% identifies recipients of sold or shared data and only 7% defines words such as “affiliates” or “third parties,” if it uses them. Fifty percent claim to share personal information with affiliates and 72% claim to do so with third parties. These numbers are higher to dating (78%), special interest (82%), cloud computing (79%), and gaming (85%). Note the conflict in the “special interest and message board” category: 42% claim to use the information internal business purposes, yet 82% share the information with third parties. Note that this definition excludes contractors, which are parties to whom information is disclosed to, say, process payments and other aspects of regular business. This is an example of the internal contradictions mentioned earlier.

A number of terms measure the extent to which companies have contracts with third parties limiting the use the shared information or imposing data security commitments. Because consumers cannot monitor the behavior of third parties with respect to their personal information, the companies that share such information are arguably in a better position to create safeguards that internalize consumer preferences (assuming such preferences embrace imposing limits on third party use of their information). Only 13% of sample firms claim that affiliates and subsidiaries with which they share information, and 20% of contractors, are bound by their privacy policy. These results vary markets. In the dating site market, only 8% of contractors are bound by the same privacy policy, as compared to cloud computing, where 25% are. Only 4% of third parties are bound by the same privacy policy, and only 2% of firms claim to perform due diligence on the legitimacy of third parties that have access to the data. Nine percent of all companies (and 15% of dating sites) have contracts with third parties limiting how the disclosed data can be used. And only 7% include links to the privacy policies of the third parties with whom they share information. A number of information practice guidelines have encouraged firms give consumers choice in regards to the sharing of their personal information. Twenty six percent of all firms give consumers the option to opt-in to share information, a mechanism that is generally regarded as consumer-friendly, and 7% have offer an opt-out mechanism. The remainder don’t give the option or not disclose. Note that we can measure only what the contract says, not what the company does.

A feature that has been prominent in all consumer contracts, including privacy policies, has been “change of terms” clauses. These are terms that give a right to firms to change the contract terms unilaterally. Some contract revisions are desirable, as modifications can potentially benefit both companies and consumers alike. Yet, other modifications might be used to extract more benefits to firms, at the expense of consumers. These clauses have been viewed with suspicion because they might induce consumers to enter into welfare reducing contracts.⁵⁹ This is one of the reasons why the CARD Act of 2009 prohibited firms to unilaterally change interest rates in the fine print. Consumer welfare can also be affected by changes in the fine print that alter the companies’ information privacy policies, especially once consumers invest time and information in a particular site, such as a social network or dating site. Several guidelines have noted the increased prevalence of these terms and have encouraged firms to seek express assent to these material change provisions.

Of the total sample, 86% of firms have “change of terms” clauses. All of cloud computing and gaming sites have them, eliminating the choice of opting for a firm without them. Only 36% will notify consumers in a meaningful way whenever the policy get revised in a material way: 9% will email consumers notifying them of the changes, and 20% promises to post a prominent link in their homepage with the revised policy. Seven percent claim that changes to the terms are retroactive. Ten percent will ask consumers for explicit consent before revising a contract, but the numbers vary by market. While 43% of cloud computing firms ask for explicit consent to revisions, only 5% of dating and not one gaming site seeks for explicit assent. The table reports other terms related to the principle of notice, such as whether the firm explains its data procedures if the company is sold or ceases to exist (only 8% do).

We also measure the extent to which users are given control of their information, such as whether they can access and correct their information. We find that 61% of firms give users the ability to adjust their privacy settings. About 50% of dating sites allow users to do this, 66% of social networks, and 71% of news and reviews sites. The variation might be driven by differences in the inherent services offered. Seventy percent of sample firms allow users to access and correct personal information (and 3% give only

⁵⁹ See Oren Bar-Gill and Kevin Davis, *Empty Promises*, S. Cal. L. Rev. (2010).

access). This high percentage is likely not representative of the whole population of privacy policies. Most of the firms in markets selected for this study allow users enter and revise their information on an ongoing basis due to the nature of the services offered. Almost 60% offer consumers the ability to delete or anonymize their information (mostly be allowing them to delete their accounts). Only 2% of firms offer consumers a choice as to what happens to their personal information if the company is sold or goes bankrupt, and only 17% promise that the buyer of the firm (and data) is bound to abide to the same privacy policy.

Another set of terms report on company measures to protect data accuracy and security. Thirty one percent of firms state that they adopt reasonable procedures to ensure data accuracy, and only 2% guarantee it. As would be expected, most firms will reserve the right to disclose personal information to comply with, protect a crime, or defend its own rights. Two percent state that they will disclose personal information to the government upon request. In terms of implementing substantive privacy protections, 46% state they have protections incorporated into operating procedures, such as limiting the number of employees with access to the data. This is true for 64% of cloud computing and 65% of gaming sites. Finally, 45% of sample firms (and 86% of cloud computing sites) identify means of technological security, such as encryption. Only 6% of sites state a period for data retention and only 1% promises to destroy the personal data when the user terminates the account. In terms of compliance with privacy by design measures, as outlines in the FTC 2012 report, only 13% of companies state that they conduct periodic compliance reviews of data and security measures (a result mostly driven by cloud computing firms, where 43% claim to do so). Also, only 5% of sample firms (and 29% of cloud computing firms) contain self-reporting measures in case of privacy violations.

The final class of terms relates to enforcement and dispute resolution. The vast majority, or 95%, includes contact information where consumers can reach out with privacy questions or concerns. Most firms include dispute resolution clauses, which are not surprising, as they are open to being sued in multiple locations. Almost 80% include a choice of forum clause, and 85% include a choice of law clause. Twenty three percent include arbitration clauses and about 20% include class action waivers.

Finally, a word on language. Sixty four percent of the sample firms use mitigation phrases, such as “occasionally and “from time to time,” making it hard for consumers or intermediaries to understand the nature of the obligation. The average contract uses almost two mitigation phrases. Almost all contracts, or 97% uses hedge words, such as “may or “might,” in relationship to the companies’ obligations. The average number of hedge words is 20 per contract, ranging from an average of 14 for review sites to 27 for gaming sites. The presence of these words in conjunction with change of terms clauses, make it especially likely for even seasoned contract readers to get a clear understanding of a company’s information privacy practices.

This problem is compounded in instances where privacy policies make claims that directly contradict one another. It is possible that an enlightened fact finder can wade through the layers of hedges and open-ended promises described above to glean the real meaning of a privacy policy. However, when a privacy policy makes one statement and then makes a directly contradictory statement, there is no way to discern the intent of the agreement. One such contradiction occurs when a privacy policy claims that it does not share a user’s personally identifiable information (PII) with third parties, but then allows third parties to place advertisements that track the website’s users. Of the 248 privacy policies, 56 claim that they do not share PII with third parties. Of these 56, 18 of these firms allow third parties to track users’ behavior. Our terms allow us to track a similar contradiction. Forty-seven firms claim that they only use PII for internal business purposes, such as effecting a transaction or improving the website. Of these 47, 21 allow third party advertisers to track and collect users’ behavior.

In addition, 45 firms require users to explicitly assent to a privacy policy at sign-up. Of these, 36 of the policies allow the firm to make material changes to the policy without the user’s assent. While this is not a direct contradiction, the second term essentially renders the first protection meaningless: users get ample notice and the opportunity to consent to a policy that can be changed without their notice and consent.

Taken together, these measures of language in the privacy policies show that in spite of FTC suggestions, privacy policies are generally dense, unreadable, vague, open-ended, and in some cases, self-contradicting.

D. Comparing Policies to Benchmarks

We now turn to evaluate the extent to which the policies comply with existing and past benchmarks. They include the most recent guidelines (the 2012 FTC Privacy Report, and the 2012 White House Consumer Privacy Bill of Rights), an international guidelines (2000 US-EU Safe Harbor for companies doing business in the EU), the older guideline (the 2000 FTC FIPs), and the three widely regarded standards to measure the average “quality” of these contracts (1973 FIPs, the 1980 OECD Guidelines, the 1995 EU Data Directive). We use a number of fair information principle guidelines as benchmarks, and these in particular, for several reasons.

First, absent clear default rules, these guidelines offer a second best approach to compare the sample privacy policies against existing benchmarks. Second, we use a number of influential guidelines in the US and the EU across time to give the sample firms a greater opportunity to comply with at least one of these. As seen from Table 1, not all firms update their policies regularly or in response to new guidelines. Third, we focus in the US and EU guidelines due to the nature of our sample, which include firms that are mostly US based or have significant business in the EU. While we don’t expect that US firms will comply with the EU Data Directive (they don’t have to), we are interested in seeing the extent to which compliance varies across guidelines that place different emphasis on different aspects of information privacy.

As Schwartz (2010) explains, differences between the US and EU approaches are both a matter of kind as well as a matter of degree. While all guidelines embrace the 1973 FIPs, the EU places greater weight on principles such as data collection limits, data quality, and notice, access, and correction, and additional protection given to sensitive data. As explained above, the US has focused more on notice and choice and reduced the FIPs to five, and ultimately four fair information principles: notice, choice, access, and security. Because companies operate world wide, we look at the extent to which companies comply with EU-US and US-Swiss Safe Harbors, which is required of companies that wish to transfer data outside of the EU.

Table 5 lists the same terms that appear in Table 4, but selects only those terms that are relevant for each of the seven guidelines (or law, in case of the EU Data

Directive) and measures the percentage of firms comply with that particular terms. Consider, for example, the FTC FIPs 2000. The terms that comprise this particular benchmark appear on the fifth column on Table 5. For the Notice principle, we see that firms must disclose whether they collect particular types of personal information. These are terms N5 (for “notice”) to N10 in the table, in addition to other terms, as shown in the table. The table shows that a total of 35 of the 69 terms comprise the five principles outlines in the 2000 FTC FIPs. We can also see the extent to which each term that comprises each benchmark complies with the stated requirement. Going back to term N5 to N10, we see that all firms comply in disclosing whether they collect contact information, 88% comply in disclosing whether computer information is collected, 83% comply in disclosing whether interactive information is collected, 70% comply in disclosing whether interactive information is collected, 59% comply in disclosing whether financial information is collected, 68% comply in disclosing whether sensitive information is collected, and all firms comply in disclosing whether geolocation information is collected. The table does this for all principles for all seven benchmarks.

Because the terms that we measure do not always fit the principles of all guidelines well and because some terms included in the principles are arguably missing, the results should be interpreted only as approximations. Still, they offer an informative comparison on the extent to which firms roughly abide by these principles as well as differences in compliance across principles.

These results can be better seen in Table 6, which reports the number of contracts that comply with each of the guidelines, laws, and safe harbor agreements. The first column lists the fraction of terms within that set of guidelines that comply with the requirements or recommendations set forth therein. The remaining columns list all guidelines. For example, the HEW FIPs of 1973 is comprised of 24 out of the 69 terms that we track. The results show that 13 out of the 248 privacy policies in our sample (or 5%) comply with 70 to 80 percent of the terms comprising this benchmark. No contract complies with a higher percentage. Indeed, 121 (or 48%) comply with only 50 to 60 percent of such terms. As for compliance with OECD guidelines, which comprise 34 of the 69 terms that we track, we see that firm compliance is even lower. Only 12 of the

sample firms comply within a range of 60 to 70 percent of the requirements of these guidelines, and the bulk of firms (107) comply with 40 to 50 percent of the requirements.

This might be surprising, as the FIPs and OECD guidelines have more stringent requirements than those later adopted by the FTC. One might conclude that firms have focused on complying with the later, and perhaps more relevant, FTC guidelines. Indeed, 6 firms comply with 70 to 80 percent of the 35 terms comprising the FTC 2000 guidelines, a fraction higher than the previous guidelines. One hundred and thirty-two, however, complied with only 60 to 70 percent of the terms. While some commentators claim that self-regulation became more effective over time because more firms adopted privacy policies, the results here show that firms have become less likely to comply with the FTC recommendations regarding the information disclosure in privacy policies as well as some privacy information practices over time. Only 11 firms complied with 60 to 70 percent of the terms that make up the guidelines set by the FTC 2012 privacy report; 86 complied with 30 to 40 percent, 26 with 20 to 30 percent, and 2 with just one 10 to 20 percent of terms. One might conjecture that firms did not have enough time to adapt, given that contracts were obtained in June 2013. This seems unlikely, though. The FTC had a preliminary report as early as 2010, and such report was widely discussed in the media. Firms appear to have had time to adapt, especially given how frequently they update contracts⁶⁰

Compliance with the White House Bill of Rights is even scarcer. In this case 19 firms complied with 50 to 60 percent of terms and one firm complying with 0 to 10 percent of the terms. In conclusion, to the extent that this methodology is able to give a general flavor of compliance, the results suggest that the guidelines had only modest influence in the contracting behavior of online firms in the sample markets.

Compare the US-EU Safe Harbor, which has more teeth, because it requires firms that adhere to it to comply with their guidelines. The results show that even with the threat of sanctions, companies don't abide to the Safe Harbor as strongly as expected. The numbers in brackets show the compliance fraction for firms that claim to adhere to the US-EU Safe Harbor. Only 12 firms comply with 50 to 60 percent of terms that comprise the safe harbor, 16 comply with 30 to 40 percent, 14 with 20 to 30 percent, and

⁶⁰ See Florencia Marotta-Wurgler, *They Dynamics of Privacy* (working paper).

10 with 10 to 20 percent. To the extent that the benchmarks constructed in this paper reflect the actual requirements. All of the companies that adhere to the Safe Harbor, which include large firms, are thus violating parts of it. It appears that even stricter standards are not enough to encourage firms to adopt them.

V. Conclusion and Implications

This paper conducts the most comprehensive large-sample analysis of online privacy policies to date. I review 248 privacy policies for services where privacy concerns are especially significant, including social networking and cloud computing. I study the incidence of 69 terms pertaining to notice, data sharing, enforcement, security, and other features and I contrast them with various legal guidelines. The analysis uncovers a number of new facts about privacy policies to help inform both academic and regulatory discussions.

What does the evidence imply for the efficacy of the standard N&C regulatory model? The general assessment is not favorable. Policies are long, complex, ambiguous, incomplete, and often silent on important subject matter. Moreover, the substance of the rights that are explicitly reserved are sometimes fairly concerning. Policies that claim compliance with various regulatory benchmarks inevitably omit or contradict features of those benchmarks. Policies are often silent on a number of important terms, and if they are not, they can be vague and internally contradictory. These features make it almost impossible for intermediaries to simplify the terms in a way that consumers can understand. It's just very hard to get a clear meaning from them. A possible solution for this problem would be to require standardization of particular disclosures, very much like a menu.⁶¹

On the policy side, the analysis suggests that an articulation of default rules for privacy policies would be an important advance. Intentional vagueness or obfuscation on the part of sellers would be reduced, and onerous or unusual terms would be easier to detect. There are limits to what can be achieved by any disclosure-based regulatory approach, but given the potential costs of direct regulation, especially in a case of

⁶¹ Ayres (cite).

emergent contracts like privacy policies with minimal case law, to support the current regime with clear default rules.

Table 1. Summary Statistics

	Sample N contracts	All N = 248	Dating N = 40	Social Networks N = 89	Special Interest Message Board N = 50	News and Reviews N = 18	Cloud Computing N = 28	Gaming N = 23
Nonprofit (0 - 1)	n (nonmissing)	248	40	89	50	18	28	23
	mean	0.05	0.07	0.04	0.1	0	0	0
	median	0	0	0	0	0	0	0
	SD	0.22	0.27	0.21	0.3	0	0	0
Paid Service (0 - 1)	n	248	40	89	50	18	28	23
	mean	0.4	0.93	0.16	0.3	0.28	0.54	0.57
	median	0	1	0	0	0	1	1
	SD	0.49	0.27	0.37	0.46	0.46	0.51	0.51
Discreet Service (0 - 1)	n	248	40	89	50	18	28	23
	mean	0.02	0.1	0	0.02	0	0	0
	median	0	0	0	0	0	0	0
	SD	0.14	0.3	0	0.14	0	0	0
Alexa Rank	n	244	39	86	50	18	28	23
	mean	979,193	1,540,000	1,100,000	851,474	1,550,000	171,891	376,604
	median	9,184	53,349	15,077	9,192	4,440	195	2,229
	SD	3,646,845	3,761,570	4,638,454	2,593,809	4,939,170	820,000	1,593,272
Year Last Updated	n	192	38	68	31	12	26	17
	mean	2010	2008	2011	2010	2011	2012	2011
	median	2011	2009	2011	2011	2011	2012	2011
	SD	2.7	3.7	2.2	2.5	1.9	0.8	2.1
Number of Words	n	248	40	89	50	18	28	23
	mean	2,227	2,008	2,469	1,797	2,315	2,166	2,608
	median	2,168	2,212	2,168	1,830	2,278	2,168	2,569
	SD	1,408	1,196	1,702	1,028	1,166	911	1,675
Certification is Claimed (0 - 1)	n	248	40	89	50	18	28	23
	mean	0.31	0.28	0.33	0.18	0.17	0.68	0.3
	median	0	0	0	0	0	1	0
	SD	0.47	0.45	0.47	0.39	0.38	0.48	0.47

Table 2. Certifications Claimed. Sample of 248 privacy policies; some claim multiple certifications.

	N Policies
US-EU Safe Harbor	58
US-Swiss Safe Harbor	25
TRUSTe	21
Australian Best Practice Guidelines for Online Behavioural Advertising	4
Data Protection Directive 95/46/EC	2
Entertainment Software Rating Board Certification (ESRB)	2
IAB Europe EU Framework for Online Behavioural Advertising	2
Thawte Certificate (n.l.e.)	2
UK Information Commissioner's Office (ICO)	2
UK Internet Advertising Bureau Good Practice Principles	2
Code Blue Security	1
German Laws on Privacy and Data Protection	1
Giodo (Polish Chief Inspectorate for the Protection of Personal Data)	1
Habeas Web Seal	1
PCI Security Standard	1
PRIVO (specializing in COPPA compliance)	1
None Claimed	170
One Claimed	44
Two Claimed	22
Three Claimed	10
Four Claimed	2

Table 3. Correlations. Correlations of service and contract characteristics.

Sample: All N Contracts = 248	Nonprofit	Paid Service	Discreet Service	Log Alexa Rank	Year Last Updated	Number of Words	Certification is Claimed
Nonprofit	1 n = 248						
Paid Service	-0.107 n = 248	1 n = 248					
Discreet Service	0.101 n = 248	0.176** n = 248	1 n = 248				
Log Alexa Rank	0.101 n = 244	0.0788 n = 244	-0.0442 n = 244	1 n = 244			
Year Last Updated	-0.0165 n = 192	-0.117 n = 192	0.007 n = 192	-0.383*** n = 189	1 n = 192		
Number of Words	-0.0565 n = 248	0.0503 n = 248	-0.015 n = 248	-0.274*** n = 244	0.395*** n = 192	1 n = 248	
Certification is Claimed	-0.0718 n = 248	0.033 n = 248	0.0264 n = 248	-0.279*** n = 244	0.434*** n = 192	0.402*** n = 248	1 n = 248

Note: n = n (nonmissing) for both variables

* p<0.05, ** p<0.01, *** p<0.001

Table 4. Content of Privacy Policies. Content of privacy policy terms by categories: Notice, Sharing, User Control, Security, Data Practices, Enforcement, Privacy by Design, and Language.

		All N = 241	Dating N = 40	Social Networks N = 88	Special Interest Message Board N = 48	News and Reviews N = 17	Cloud Computing N = 28	Gaming N = 20
Notice								
N1. Policy is accessible through a direct link from the homepage	yes	0.88	0.93	0.9	0.83	0.94	0.79	0.85
	no	0.12	0.08	0.09	0.17	0.06	0.18	0.15
	n.a.	0.01		0.01			0.04	
N2. Users asked to manifest consent when signing up via clickwrap	yes	0.18	0.25	0.2	0.17	0.24	0.93	0.2
	no	0.8	0.75	0.78	0.83	0.76	0.07	0.8
	n.a.	0.01		0.01				
N3. Layered or short notice is presented	yes	0.22	0.1	0.19	0.1	0.35	0.46	0.35
	no	0.78	0.9	0.81	0.9	0.65	0.54	0.65
N4. Contact data is collected and stored	yes	0.97	0.98	0.99	0.92	1	1	0.95
	no	0.03	0.03	0.01	0.08			0.05
N5. Computer data is collected and stored (e.g., IP address, browser type, OS)	yes	0.86	0.68	0.88	0.9	0.94	0.93	0.95
	no	0.02	0.33	0.05	0.02	0.06	0.07	0.05
	undisclosed	0.11		0.08	0.08			
N6. Interactive data is collected and stored (e.g., browsing behavior or search history)	yes	0.71	0.6	0.74	0.75	0.76	0.64	0.8
	no	0.12	0.05	0.13	0.06	0.12	0.25	0.15
	undisclosed	0.17	0.35	0.14	0.19	0.12	0.11	0.05
N7. Financial information is collected and stored (e.g., account status or history, credit)	yes	0.48	0.68	0.4	0.4	0.35	0.64	0.5
	no	0.2	0.08	0.16	0.27	0.41	0.29	0.2
	n.a.	0.03		0.07	0.04			
	undisclosed	0.29	0.25	0.38	0.29	0.24	0.07	0.3
N8. Content is collected and stored (e.g., personal communications, stored documents, media)	yes	0.43	0.43	0.47	0.46	0.41	0.36	0.3
	no	0.16	0.05	0.16	0.19	0.18	0.32	0.05
	undisclosed	0.41	0.53	0.38	0.35	0.41	0.32	0.65
N9. Sensitive information is collected and stored (e.g., race, medical info, religion, sexual orientation, income, SSN)	yes	0.28	0.7	0.25	0.17	0.29	0.11	0.1
	no	0.4	0.05	0.49	0.44	0.47	0.61	0.25
	undisclosed	0.32	0.25	0.26	0.4	0.24	0.29	0.65
N10. Geolocation information is collected and stored (not just IP address)	yes	0.15	0.08	0.2	0.13	0.06	0.25	0.1
	no	0.5	0.63	0.42	0.44	0.71	0.32	0.85
	n.a.	0.34	0.3	0.38	0.44	0.24	0.43	0.05
N11. Cookies used	yes	0.93	0.88	0.94	0.9	0.88	1	1
	no	0.02	0.05	0.02		0.06		
	undisclosed	0.05	0.08	0.03	0.1	0.06		
N12. PII used internally only for business purposes (e.g., administering transaction, communication with user, research, internal database compilation, servicing site)	yes	0.26	0.15	0.27	0.42	0.24	0.18	0.2
	no	0.74	0.85	0.73	0.58	0.76	0.82	0.8

N13. PII used only for stated, context-specific purposes (e.g., user would expect that this data would be shared for service to function)	yes	0.25	0.3	0.26	0.19	0.24	0.21	0.3
	no	0.75	0.7	0.74	0.81	0.76	0.79	0.7
N14. Non-PII used internally only for business purposes	yes	0.19	0.13	0.22	0.17	0.29	0.29	0.05
	no	0.81	0.88	0.78	0.83	0.71	0.71	0.95
N15. Non-PII used only for stated, context-specific purposes	yes	0.08	0.13	0.1	0.04	0.12	0.04	0.05
	no	0.92	0.88	0.9	0.96	0.88	0.96	0.95
N16. User's profile, picture, or other information may be used in advertising	yes	0.04	0.1	0.03			0.07	
	no	0.91	0.73	0.9	1	1	0.93	1
	opt-in/opt-out	0.05	0.18	0.07				
N17. Third parties may place advertisements that track user behavior	yes	0.64	0.55	0.63	0.69	0.53	0.71	0.8
	no	0.1	0.18	0.1	0.04	0.24	0.07	0.05
	undisclosed	0.25	0.28	0.27	0.27	0.24	0.21	0.15
N18. Recipients of shared or sold data are identified	yes	0.1	0.05	0.08	0.19	0.06	0.11	0.05
	no	0.9	0.95	0.92	0.81	0.94	0.89	0.95
N19. Words such as "affiliates" or "third parties" are defined, if used	yes	0.07	0.05	0.09	0.04	0.06	0.04	0.2
	no	0.82	0.8	0.81	0.85	0.82	0.86	0.8
	n.a.	0.1	0.15	0.1	0.1	0.12	0.11	
N20. Change of Terms (COT) provision explicitly or implicitly allowing changes to policy	yes	0.86	0.88	0.82	0.79	0.82	1	1
	no	0.14	0.13	0.18	0.21	0.18		
N21. Company alerts user to material changes to the policy (simply posting new policy constitutes no notice)	yes	0.36	0.38	0.36	0.27	0.47	0.25	0.55
	no	0.51	0.5	0.47	0.52	0.41	0.75	0.45
	n.a.	0.11	0.13	0.11	0.19	0.12		
	undisclosed	0.02		0.06	0.02			
N22. Manner in which company gives notice of changes to policy	email or other prominent link on homepage	0.09	0.1	0.08	0.06	0.24	0.07	0.1
	at our discretion	0.2	0.23	0.2	0.19	0.12	0.11	0.4
	none	0.21	0.23	0.19	0.15	0.24	0.39	0.15
	n.a.	0.36	0.33	0.35	0.4	0.29	0.43	0.35
	undisclosed	0.11	0.13	0.11	0.19	0.12		
		0.02		0.06	0.02			
N23. User must explicitly assent to material changes	yes	0.1	0.05	0.08	0.02	0.06	0.43	
	no	0.8	0.83	0.81	0.79	0.82	0.57	1
	n.a.	0.11	0.13	0.11	0.19	0.12		
N24. Material changes are retroactive	yes	0.07	0.03	0.13	0.02	0.06	0.07	
	no	0.93	0.98	0.88	0.98	0.94	0.93	1
N25. Provides notice of data procedures if company is sold or otherwise ceases to exist	yes	0.08	0.08	0.1	0.04	0.06	0.11	0.05
	no	0.92	0.93	0.9	0.96	0.94	0.89	0.95
N26. Policy is dated	yes	0.78	0.95	0.76	0.63	0.65	0.96	0.7
	no	0.22	0.05	0.24	0.38	0.35	0.04	0.3
Sharing								
SH1. Affiliates and subsidiaries are bound by the same privacy policy	yes	0.13	0.23	0.11	0.08	0.06	0.25	0.8
	no	0.51	0.43	0.57	0.5	0.47	0.32	0.2
	n.a.	0.36	0.35	0.32	0.42	0.47	0.43	
SH2. Contractors (e.g., payment process companies) are bound by the same privacy policy	yes	0.2	0.08	0.25	0.23	0.24	0.25	0.1
	no	0.61	0.73	0.58	0.48	0.59	0.61	0.85
	n.a.	0.19	0.2	0.17	0.29	0.18	0.14	0.05

SH3. Third parties are bound by the same privacy policy	yes	0.04	0.03	0.07	0.06			
	no	0.76	0.78	0.75	0.63	0.76	0.82	0.95
	n.a.	0.2	0.2	0.18	0.31	0.24	0.18	0.05
SH4. Company shares non-PII with affiliates	yes	0.51	0.43	0.58	0.44	0.35	0.54	0.7
	no	0.49	0.58	0.42	0.56	0.65	0.46	0.3
SH5. Company shares PII information with affiliates	yes	0.5	0.45	0.52	0.44	0.47	0.5	0.7
	no	0.5	0.55	0.48	0.56	0.53	0.5	0.3
SH6. Company shares PII information with third parties	yes	0.72	0.78	0.7	0.58	0.82	0.79	0.85
	no	0.28	0.23	0.3	0.42	0.18	0.21	0.15
SH7. Company shares non-PII data with third parties	yes	0.77	0.7	0.8	0.67	0.76	0.82	0.95
	no	0.23	0.3	0.2	0.33	0.24	0.18	0.05
SH8. Company reports performing due diligence to ensure legitimacy of third parties that have access to data	yes	0.02		0.02	0.04	0.12		
	no	0.98	1	0.98	0.96	0.88	1	1
SH9. Company has contract with third parties establishing how disclosed data can be used	yes	0.09	0.15	0.09	0.08	0.06	0.04	0.05
	no	0.75	0.68	0.76	0.69	0.76	0.82	0.9
	n.a.	0.16	0.18	0.15	0.23	0.18	0.14	0.05
SH10. Provides links to privacy policies of 3rd parties	yes	0.07	0.08	0.03	0.13	0.12	0.04	0.05
	no	0.8	0.75	0.85	0.71	0.71	0.82	0.9
	n.a.	0.14	0.18	0.11	0.17	0.18	0.14	0.05
SH11. Consent mechanism for sharing/selling PII or sensitive information (except for typical internal business purposes)	opt-in	0.26	0.25	0.23	0.21	0.24	0.5	0.25
	opt-out	0.07	0.08	0.03	0.06	0.24	0.04	0.1
	mandatory	0.37	0.38	0.47	0.27	0.29	0.36	0.3
	n.a.	0.3	0.3	0.27	0.46	0.24	0.11	0.35
SH12. Consent mechanism for sharing/selling non-PII or sensitive information to non-service providers (except for typical internal business purposes)	opt-in	0.02	0.05	0.01	0.04			
	opt-out	0.07	0.05	0.06	0.04	0.12	0.07	0.15
	mandatory	0.7	0.65	0.75	0.69	0.59	0.64	0.8
	n.a.	0.21	0.25	0.18	0.23	0.29	0.29	0.05
User Control								
UC1. User can adjust privacy settings	yes	0.61	0.5	0.66	0.52	0.71	0.68	0.6
	no	0.39	0.5	0.34	0.48	0.29	0.32	0.4
UC2. User allowed to access and correct personal data collected	no	0.27	0.18	0.23	0.46	0.35	0.21	0.25
	can access and correct	0.7	0.8	0.73	0.54	0.59	0.75	0.75
	can access	0.03	0.03	0.05		0.06	0.04	
UC3. User can request that information be deleted or anonymized	yes	0.57	0.68	0.59	0.42	0.59	0.61	0.6
	no	0.43	0.33	0.41	0.58	0.41	0.39	0.4
UC4. Ownership rights of user data	user owns, licenses to entity	0.71	0.7	0.69	0.71	0.65	0.75	0.85
	user owns, add'l protection vs. lic.	0.03		0.02	0.04		0.11	
	company owns	0.02	0.03	0.02			0.04	0.05
	undisclosed	0.24	0.28	0.26	0.25	0.35	0.11	0.1
UC5. Destiny of data when company no longer exists	sold, PP remains in force	0.17	0.18	0.22	0.13	0.06	0.18	0.1
	sold with company/o.w. disclosed	0.77	0.75	0.66	0.85	0.88	0.82	0.9
	undisclosed	0.07	0.08	0.13	0.02	0.06		
UC6. User given a choice of what happens to data if company is sold or otherwise ceases to exist	yes	0.02	0.03	0.03	0.04			
	no	0.98	0.98	0.97	0.96	1	1	1

Security

SEC1. Guarantees data accuracy	yes	0.02		0.02		0.12		
	no	0.98	1	0.98	1	0.88	1	1
SEC2. Company adopts reasonable procedures to ensure accuracy	yes	0.31	0.18	0.28	0.25	0.24	0.68	0.35
	no	0.69	0.83	0.72	0.75	0.76	0.32	0.65
SEC3. Company reserves right to disclose protected information to comply with the law or prevent a crime	yes	0.85	0.85	0.84	0.73	0.94	0.96	0.9
	no	0.15	0.15	0.16	0.27	0.06	0.04	0.1
SEC4. Company reserves right to disclose protected information to protect own rights	yes	0.7	0.68	0.68	0.6	0.76	0.86	0.8
	no	0.3	0.33	0.32	0.4	0.24	0.14	0.2
SEC5. User will be given notice of government requests for information about the user	yes	0.02	0.03	0.01		0.06	0.04	
	no	0.98	0.98	0.99	1	0.94	0.96	1
SEC6. User will be notified of any data breach	yes	0.02	0.03	0.02	0.04	0.06		
	no	0.98	0.98	0.98	0.96	0.94	1	1
SEC7. Describes substantive privacy and security protections incorporated into operating procedures (e.g., limiting number of employees with access to data)	yes	0.46	0.38	0.45	0.33	0.47	0.64	0.65
	no	0.54	0.63	0.55	0.67	0.53	0.36	0.35
SEC8. Identifies means of technological security (e.g., encryption)	yes	0.45	0.53	0.44	0.35	0.29	0.86	0.15
	no	0.55	0.48	0.56	0.65	0.71	0.14	0.85

Data Practices

DP1. States time limit for data retention (including when account is closed)	yes	0.06	0.03	0.11	0.04		0.07	
	no	0.94	0.98	0.89	0.96	1	0.93	1
DP2. Policy for personal data when account is closed	destroyed or anonymized	0.1	0.08	0.15	0.08	0.06	0.04	0.05
	retained as if service continues	0.1	0.03	0.16	0.08	0.06	0.11	0.05
	retained but modified	0.2	0.35	0.16	0.1	0.29	0.11	0.3
	undisclosed	0.61	0.55	0.53	0.73	0.59	0.75	0.6
DP3. Has a procedure for safely disposing of unused data	yes	0.01		0.02	0.02			
	no	0.99	1	0.98	0.98	1	1	1

Enforcement

E1. Provides contact information for privacy concerns or complaints	yes	0.95	0.93	0.95	0.94	1	1	0.9
	no	0.05	0.08	0.05	0.06			0.1
E2. Forum selection clause	yes	0.77	0.78	0.77	0.69	0.76	0.79	0.95
	no	0.23	0.23	0.23	0.31	0.24	0.21	0.05
E3. Choice of law clause	yes	0.85	0.88	0.86	0.79	0.82	0.89	0.9
	no	0.15	0.13	0.14	0.21	0.18	0.11	0.1
E4. Arbitration clause	yes	0.23	0.33	0.17	0.23	0.29	0.25	0.25
	no	0.74	0.65	0.8	0.77	0.59	0.75	0.75
	consumer may choose	0.02	0.03	0.03		0.12		
E5. Class action waiver	yes	0.19	0.3	0.13	0.17	0.29	0.21	0.15
	no	0.81	0.7	0.88	0.83	0.71	0.79	0.85
E6. Disclaims liability for failure of security measures	yes	0.59	0.53	0.63	0.63	0.65	0.39	0.7
	no	0.41	0.48	0.38	0.38	0.35	0.61	0.3

E7. Provides link to FTC's Consumer Complaint Form and/or its telephone number	yes	0.08	0.1	0.06	0.1	0.12	0.07	0.05
	no	0.92	0.9	0.94	0.9	0.88	0.93	0.95
E8. Claims privacy seal, certification, or consistency with an industry oversight organization's practice	yes	0.32	0.28	0.33	0.17	0.18	0.68	0.35
	no	0.68	0.73	0.67	0.83	0.82	0.32	0.65
Privacy By Design								
PBD1. Requires periodic complicate review of structural and technological data security measures	yes	0.13	0.03	0.16	0.02	0.06	0.43	0.15
	no	0.87	0.98	0.84	0.98	0.94	0.57	0.85
PBD2. Contains self-reporting measures in case of privacy violation (to a privacy seal organization, third-party consultant)	yes	0.05		0.02	0.02		0.29	
	no	0.95	1	0.98	0.98	1	0.71	1
Language								
L1. Uses mitigation phrases (e.g., "from time to time," "occasionally") relating to company's obligations	yes	0.64	0.65	0.6	0.69	0.47	0.68	0.75
	no	0.36	0.35	0.4	0.31	0.53	0.32	0.25
L2. Number of mitigation phrases, if used	mean	1.78	1.79	1.82	1.71	2	1.47	2.07
L3. Uses hedge words (e.g., "may," "might," "at our sole discretion") relating to company's obligations	yes	0.97	0.98	0.97	0.96	0.94	1	1
	no	0.03	0.03	0.03	0.04	0.06		
L4. Number of hedges, if used	mean	20	19	21	14	23	25	27

Table 5. Guidelines and Compliance. We calculate the fraction of policies compliant with guideline- and term-specific requirements. The footnote describes the definition of compliance in special cases.

Notice		FTC FIPs 1977	OECD 1980	EU Data Directive 1995	European Safe Harbor 2000	FTC FIPs 2000	FTC Privacy Report 2012	White House Privacy Bill of Rights 2012
N1. Policy is accessible through a direct link from the homepage	yes no n.a.	0.88 0.12 0.01	.	.	.	yes ¹ (0.88 comply)	yes ¹ (0.88 comply)	.
N2. Users asked to manifest consent when signing up via clickwrap	yes no n.a.	0.18 0.8 0.01	yes ¹ (0.18 comply)	yes ¹ (0.18 comply)	.	yes ¹ (0.18 comply)	yes ¹ (0.18 comply)	.
N3. Layered or short notice is presented	yes no	0.22 0.78	yes (0.22 comply)
N4. Contact data is collected and stored	yes no	0.97 0.03	must disclose (1 comply)	must disclose (1 comply)	must disclose (1 comply)	must disclose (1 comply)	.	.
N5. Computer data is collected and stored (e.g., IP address, browser type, OS)	yes no undisclosed	0.86 0.02 0.11	must disclose ³ (0.88-1 comply)	must disclose ³ (0.88-1 comply)	must disclose ³ (0.88-1 comply)	must disclose ³ (0.88-1 comply)	.	.
N6. Interactive data is collected and stored (e.g., browsing behavior or search history)	yes no undisclosed	0.71 0.12 0.17	must disclose ³ (0.83-1 comply)	must disclose ³ (0.83-1 comply)	must disclose ³ (0.83-1 comply)	must disclose ³ (0.83-1 comply)	.	.
N7. Financial information is collected and stored (e.g., account status or history, credit)	yes no n.a. undisclosed	0.48 0.2 0.03 0.29	must disclose ² (0.70-1 comply)	must disclose ² (0.70-1 comply)	must disclose ² (0.70-1 comply)	must disclose ² (0.70-1 comply)	must disclose ² (0.70-1 comply)	.
N8. Content is collected and stored (e.g., personal communications, stored documents, media)	yes no undisclosed	0.43 0.16 0.41	must disclose ³ (0.59-1 comply)	must disclose ³ (0.59-1 comply)	must disclose ³ (0.59-1 comply)	must disclose ³ (0.59-1 comply)	.	.
N9. Sensitive information is collected and stored (e.g., race, medical info, religion, sexual orientation, income, SSN)	yes no undisclosed	0.28 0.4 0.32	must disclose ³ (0.68-1 comply)	must disclose ³ (0.68-1 comply)	!#\$%&'#(&')*\$ +,-./0	must disclose ³ (0.68-1 comply)	must disclose ³ (0.68-1 comply)	.
N10. Geolocation information is collected and stored (not just IP address)	yes no n.a.	0.15 0.5 0.34	must disclose (1 comply)	must disclose (1 comply)	must disclose (1 comply)	must disclose (1 comply)	must disclose (1 comply)	.
N11. Cookies used	yes no undisclosed	0.93 0.02 0.05	.	.	.	must disclose ³ (0.95-1 comply)	.	.
N12. PII used internally only for business purposes (e.g., administering transaction, communication with user, research, internal database compilation, servicing site)	yes no	0.26 0.74	yes (.26 comply)	yes (.26 comply)	yes (.26 comply)	yes (.26 comply)	yes (.26 comply)	yes (.26 comply)
N13. PII used only for stated, context-specific purposes (e.g., user would expect that this data would be shared for service to function)	yes no	0.25 0.75	yes (.25 comply)	yes (.25 comply)	yes (.25 comply)	yes (.25 comply)	yes (.25 comply)	yes (.25 comply)
N14. Non-PII used internally only for business purposes	yes no	0.19 0.81
N15. Non-PII used only for stated, context-specific purposes	yes no	0.08 0.92

N16. User's profile, picture, or other information may be used in advertising	yes no opt-in/opt-out	0.04 0.91 0.05	.	.	no or user's option (0.96 comply)	.	(no or) user's option (0.96 comply)	.	no (0.91 comply)
N17. Third parties may place advertisements that track user behavior	yes no undisclosed	0.64 0.1 0.25	.	must disclose ³ (0.74-1 comply)	no ⁴ (0.1-0.35 comply)	.	no ⁴ (0.1-0.35 comply)	no ⁴ (0.1-0.35 comply)	must disclose ³ (0.74-1 comply)
N18. Recipients of shared or sold data are identified	yes no	0.1 0.9	yes (0.1 comply)	yes (0.1 comply)	yes (0.1 comply)	yes (0.1 comply)	yes (0.1 comply)	.	.
N19. Words such as "affiliates" or "third parties" are defined, if used	yes no n.a.	0.07 0.82 0.1	.	yes ¹ (0.08 comply)	yes ¹ (0.08 comply)	yes ¹ (0.08 comply)	yes ¹ (0.08 comply)	.	yes ¹ (0.08 comply)
N20. Change of Terms (COT) provision explicitly or implicitly allowing changes to policy	yes no	0.86 0.14	.	no (0.14 comply)
N21. Company alerts user to material changes to the policy (simply posting new policy constitutes no notice)	yes no n.a. undisclosed	0.36 0.51 0.11 0.02	.	yes ⁵ (.40-.43 comply)	.	.	.	yes ⁵ (.40-.43 comply)	.
N22. Manner in which company gives notice of changes to policy	email or other prominent link on homepage at our discretion none n.a. undisclosed	0.09 0.2 0.21 0.36 0.11 0.02
N23. User must explicitly assent to material changes	yes no n.a.	0.1 0.8 0.11	yes ¹ (0.11 comply)	yes ¹ (0.11 comply)	.	yes ¹ (0.11 comply)	.	yes ¹ (0.11 comply)	.
N24. Material changes are retroactive	yes no	0.07 0.93	no (0.93 comply)
N25. Provides notice of data procedures if company is sold or otherwise ceases to exist	yes no	0.08 0.92	yes (0.08 comply)	yes (0.08 comply)	yes (0.08 comply)
N26. Policy is dated	yes no	0.78 0.22
Sharing									
SH1. Affiliates and subsidiaries are bound by the same privacy policy	yes no n.a.	0.13 0.51 0.36	.	.	.	yes ¹ (0.20 comply)	.	yes ¹ (0.20 comply)	yes ¹ (0.20 comply)
SH2. Contractors (e.g., payment process companies) are bound by the same privacy policy	yes no n.a.	0.2 0.61 0.19	.	.	yes ¹ (0.25 comply)	yes ¹ (0.25 comply)	.	yes ¹ (0.25 comply)	yes ¹ (0.25 comply)
SH3. Third parties are bound by the same privacy policy	yes no n.a.	0.04 0.76 0.2	.	.	yes ¹ (0.05 comply)	yes ¹ (0.05 comply)	.	yes ¹ (0.05 comply)	yes ¹ (0.05 comply)
SH4. Company shares non-PII with affiliates	yes no	0.51 0.49
SH5. Company shares PII information with affiliates	yes no	0.5 0.5	.	.	must disclose (1 comply)	.	must disclose (1 comply)	no (0.5 comply)	no (0.5 comply)

SH6. Company shares PII information with third parties	yes no	0.72 0.28	must disclose (1 comply)	.	must disclose (1 comply)	.	must disclose (1 comply)	no (0.28 comply)	no (0.28 comply)
SH7. Company shares non-PII data with third parties	yes no	0.77 0.23
SH8. Company reports performing due diligence to ensure legitimacy of third parties that have access to data	yes no	0.02 0.98	.	yes (0.02 comply)	yes (0.02 comply)	.	.	.	yes (0.02 comply)
SH9. Company has contract with third parties establishing how disclosed data can be used	yes no n.a.	0.09 0.75 0.16	.	yes ¹ (0.11 comply)	.	yes ¹ (0.11 comply)	.	.	yes ¹ (0.11 comply)
SH10. Provides links to privacy policies of 3rd parties	yes no n.a.	0.07 0.8 0.14
SH11. Consent mechanism for sharing/selling PII or sensitive information (except for typical internal business purposes)	opt-in opt-out mandatory n.a.	0.26 0.07 0.37 0.3	opt-in ⁶ (0.37 comply)	opt-in ⁶ (0.37 comply)	opt-in ⁶ (0.37 comply)	user's option ² (0.47 comply)	user's option ² (0.47 comply)	opt-in ⁶ (0.37 comply)	user's option ² (0.47 comply)
SH12. Consent mechanism for sharing/selling non-PII or sensitive information to non-service providers (except for typical internal business purposes)	opt-in opt-out mandatory n.a.	0.02 0.07 0.7 0.21
User Control									
UC1. User can adjust privacy settings	yes no	0.61 0.39	.	yes (0.61 comply)	.	.	yes (0.61 comply)	.	yes (0.61 comply)
UC2. User allowed to access and correct personal data collected	no can access and correct can access	0.27 0.7 0.03	can access and correct (0.7 comply)	can access and correct (0.7 comply)	can access and correct (and third parties notified) (0.7 comply)	can access and correct (and third parties notified) (0.7 comply)	can access and correct (0.7 comply)	can access (0.73 comply)	can access and correct (0.7 comply)
UC3. User can request that information be deleted or anonymized	yes no	0.57 0.43	yes (0.57 comply)	yes (0.57 comply)	.	.	yes (0.57 comply)	yes (0.57 comply)	yes (0.57 comply)
UC4. Ownership rights of user data	user owns, licenses to entity user owns, add'l protection vs. lic. company owns undisclosed	0.71 0.03 0.02 0.24
UC5. Destiny of data when company no longer exists	sold, PP remains in force sold with company/o.w. disclosed undisclosed	0.17 0.77 0.07
UC6. User given a choice of what happens to data if company is sold or otherwise ceases to exist	yes no	0.02 0.98	yes (0.02 comply)	yes (0.02 comply)	.	.	yes (0.02 comply)	.	.
Security									
SEC1. Guarantees data accuracy	yes no	0.02 0.98	yes (0.02 comply)	yes (0.02 comply)	yes (0.02 comply)	yes (0.02 comply)	yes (0.02 comply)	yes (0.02 comply)	yes (0.02 comply)
SEC2. Company adopts reasonable procedures to ensure accuracy	yes no	0.31 0.69	yes (0.31 comply)	yes (0.31 comply)	yes (0.31 comply)	yes (0.31 comply)	yes (0.31 comply)	yes (0.31 comply)	yes (0.31 comply)

SEC3. Company reserves right to disclose protected information to comply with the law or prevent a crime	yes no	0.85 0.15	yes (0.85 comply)	yes (0.85 comply)
SEC4. Company reserves right to disclose protected information to protect own rights	yes no	0.7 0.3	yes (0.7 comply)	.	yes (0.7 comply)
SEC5. User will be given notice of government requests for information about the user	yes no	0.02 0.98	yes (0.02 comply)	.	yes (0.02 comply)
SEC6. User will be notified of any data breach	yes no	0.02 0.98
SEC7. Describes substantive privacy and security protections incorporated into operating procedures (e.g., limiting number of employees with access to data)	yes no	0.46 0.54	yes (0.46 comply)	yes (0.46 comply)	yes (0.46 comply)	yes (0.46 comply)	yes (0.46 comply)	yes (0.46 comply)	yes (0.46 comply)
SEC8. Identifies means of technological security (e.g., encryption)	yes no	0.45 0.55	yes (0.45 comply)	yes (0.45 comply)	yes (0.45 comply)	yes (0.45 comply)	yes (0.45 comply)	yes (0.45 comply)	yes (0.45 comply)
Data Practices									
DP1. States time limit for data retention (including when account is closed)	yes no	0.06 0.94	.	.	yes (0.06 comply)	.	yes (0.06 comply)	yes (0.06 comply)	yes (0.06 comply)
DP2. Policy for personal data when account is closed	destroyed or anonymized retained as if service continues retained but modified undisclosed	0.1 0.1 0.2 0.61	must disclose (0.4 comply)
DP3. Has a procedure for safely disposing of unused data	yes no	0.01 0.99	.	yes (0.01 comply)	yes (0.01 comply)	yes (0.01 comply)	yes (0.01 comply)	yes (0.01 comply)	yes (0.01 comply)
Enforcement									
E1. Provides contact information for privacy concerns or complaints	yes no	0.95 0.05	.	yes (0.95 comply)	yes (0.95 comply)	yes (0.95 comply)	yes (0.95 comply)	.	.
E2. Forum selection clause	yes no	0.77 0.23
E3. Choice of law clause	yes no	0.85 0.15
E4. Arbitration clause	yes no consumer may choose	0.23 0.74 0.02
E5. Class action waiver	yes no	0.19 0.81
E6. Disclaims liability for failure of security measures	yes no	0.59 0.41	.	no (0.41 comply)	.	.	.	no (0.41 comply)	.
E7. Provides link to FTC's Consumer Complaint Form and/or its telephone number	yes no	0.08 0.92	.	.	.	yes (0.08 comply)	.	.	.
E8. Claims privacy seal, certification, or consistency with an industry oversight organization's practice	yes no	0.32 0.68	.	yes (0.32 comply)	.	yes (0.32 comply)	yes (0.32 comply)	.	.
Privacy By Design									
PBD1. Requires periodic compicance review of structural and technological data security measures	yes no	0.13 0.87	yes (0.13 comply)	yes (0.13 comply)	yes (0.13 comply)	yes (0.13 comply)	yes (0.13 comply)	yes (0.13 comply)	yes (0.13 comply)

PBD2. Contains self-reporting measures in case of privacy violation (to a privacy seal organization, third-party consultant)	yes	0.05	.	yes	yes	yes	yes	.	yes
	no	0.95		(0.05 comply)	(0.05 comply)	(0.05 comply)	(0.05 comply)		(0.05 comply)

Language

L1. Uses mitigation phrases (e.g., "from time to time," "occasionally") relating to company's obligations	yes	0.64
	no	0.36							
L2. Number of mitigation phrases, if used	mean	1.78
L3. Uses hedge words (e.g., "may," "might," "at our sole discretion") relating to company's obligations	yes	0.97
	no	0.03							
L4. Number of hedges, if used	mean	20

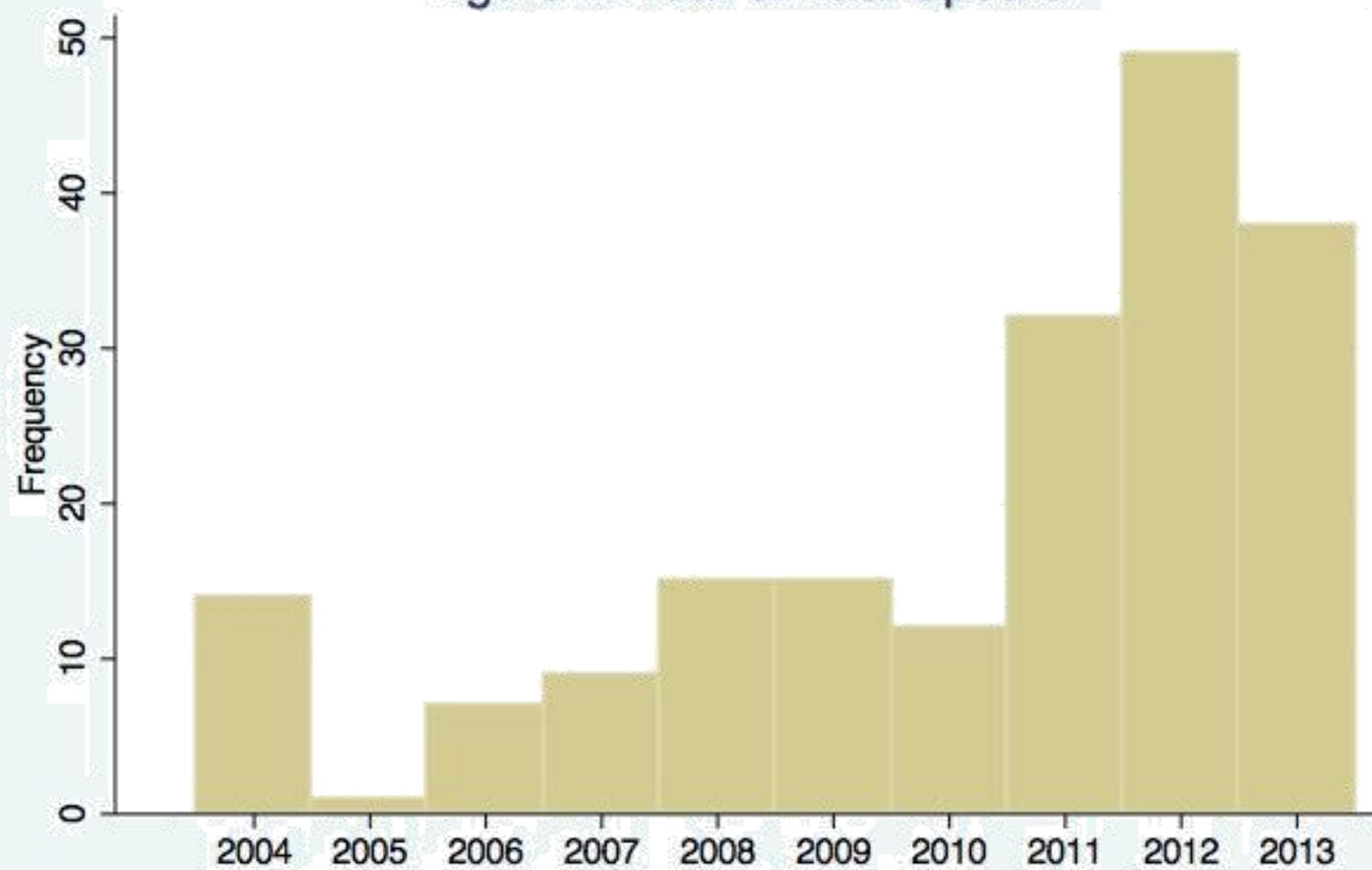
Special definitions of compliance:

1. yes/(yes+no)
2. (opt-in+opt-out)/(opt-in+opt-out+mandatory)
3. yes+no (lower bound) to yes+no+undisclosed (upper bound) depending on assumptions about undisclosed behavior and legal treatment of undisclosed vs. no
4. no (lower bound) + no+undisclosed (upper bound) depending on assumptions about undisclosed behavior and legal treatment of undisclosed vs. no
5. yes/(yes+no+undisclosed) (lower bound) to (yes+undisclosed)/(yes+no+undisclosed) (upper bound) depending on assumptions about undisclosed behavior and legal treatment of undisclosed vs. no
6. opt-in/(opt-in+opt-out+mandatory)

Table 6. Compliance with Guidelines. For example, the HEW FIPs 1973 guidelines involve 24 terms that we track; 13 out of 248 privacy policies comply with between 70% and 79.9% of these terms. In brackets, we examine 58 policies that claim compliance with the European Safe Harbor 2000 guidelines. Results are adjusted to account for policies for which a given term is not applicable.

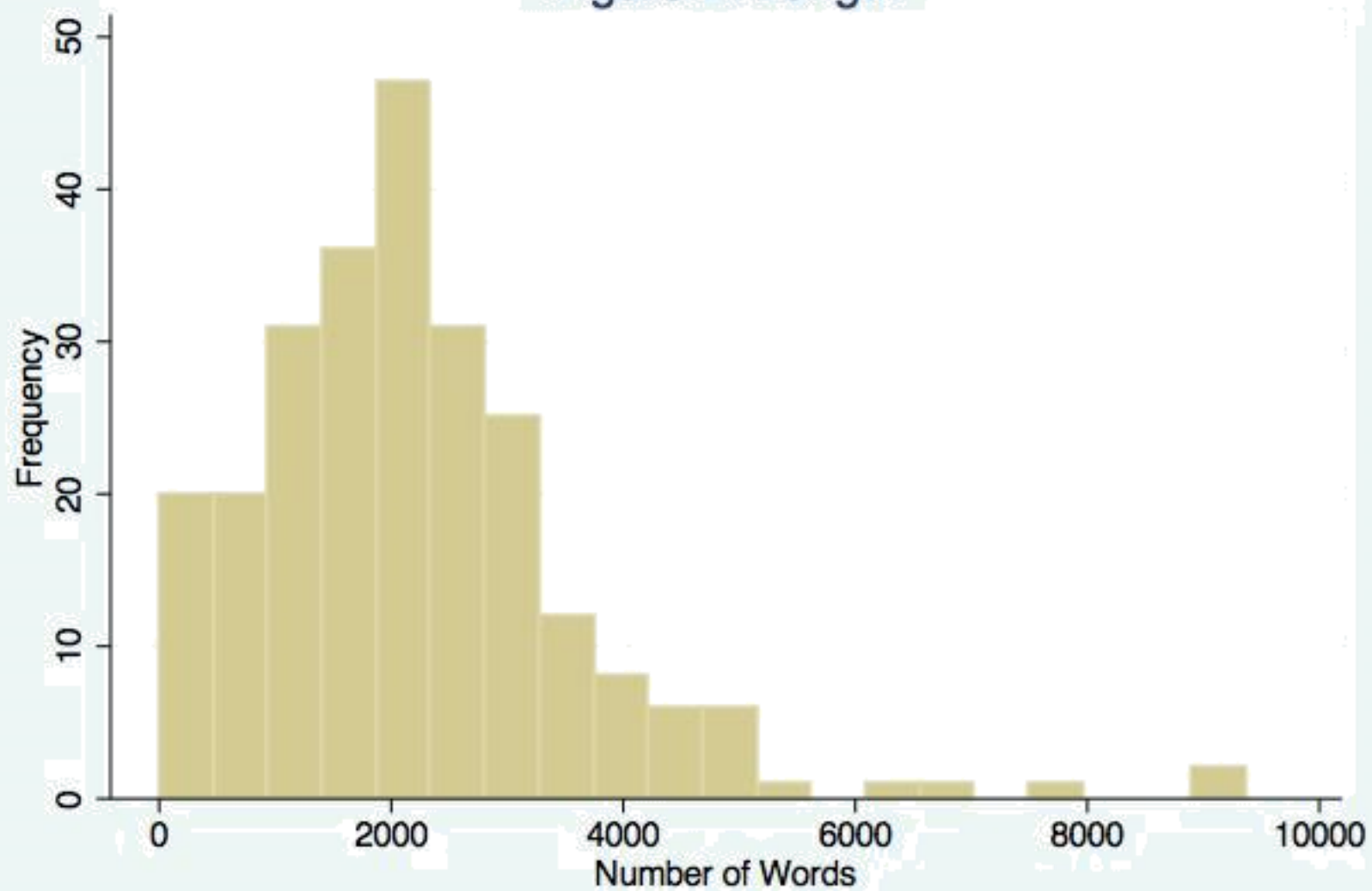
Number of Contracts (N = 248)							
	HEW FIPs 1973	OECD 1980	EU Data Directive 1995	European Safe Harbor 2000	FTC FIPs 2000	FTC Privacy Report 2012	White House Privacy Bill of Rights 2012
Fraction of Terms (24 total terms) Complied With	(34 total terms)	(29 total terms)	(19 total terms)	(35 total terms)	(27 total terms)	(30 total terms)	
[0.9, 1.0]
[0.8, 0.9)
[0.7, 0.8)	13	.	.	.	6	.	.
[0.6, 0.7)	41	12	11	.	44	11	.
[0.5, 0.6)	121	47	89	12[12]	132	44	19
[0.4, 0.5)	61	107	115	8[6]	58	79	50
[0.3, 0.4)	12	79	33	33[16]	8	86	93
[0.2, 0.3)	.	3	.	77[14]	.	26	68
[0.1, 0.2)	.	.	.	80[10]	.	2	17
[0.0, 0.1)	.	.	.	38[.]	.	.	1

Figure 1. Year of Last Update



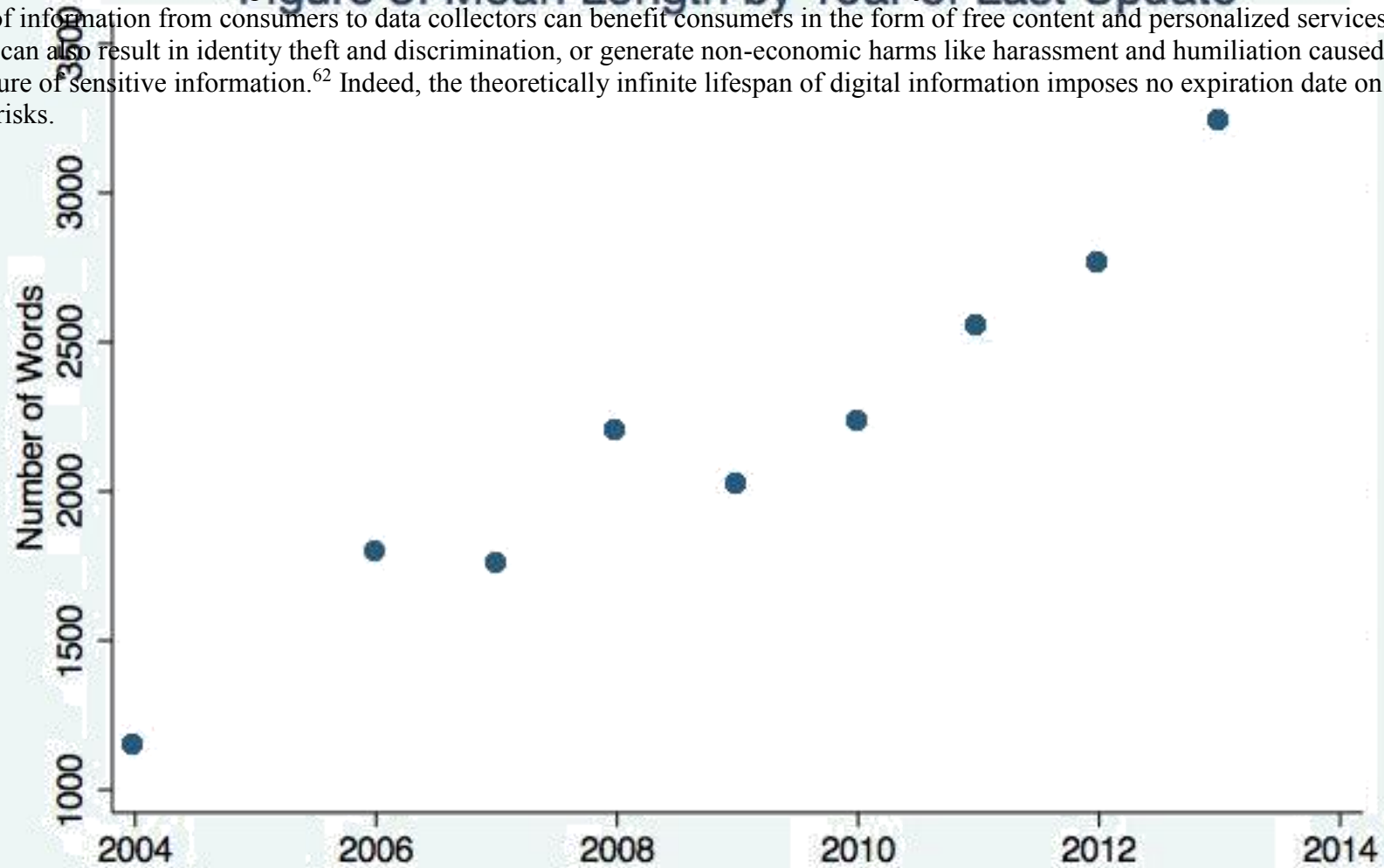
Note: N = 187 of 241 policies are dated

Figure 2. Length



Deleted TEXT

The extent to which online operators should be free to undertake these activities is a subject of heated debate. Free and unrestricted flow of information from consumers to data collectors can benefit consumers in the form of free content and personalized services. But it can also result in identity theft and discrimination, or generate non-economic harms like harassment and humiliation caused by exposure of sensitive information.⁶² Indeed, the theoretically infinite lifespan of digital information imposes no expiration date on these risks.



Note: The 2005 contract (N = 1) is grouped with 2006 contracts.

⁶² Alessandro Acquisti, *The Economics and Behavioral Economics of Privacy with PROVA CONTRACTS, AND THE PUBLIC GOOD* (Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum, Eds.) (Cambridge U. Press 2014), (Calo, 2011), Nissenbaum, Romanosky and Acquisti 2009.