I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

JOSEPH TUROW,[a] CHRIS JAY HOOFNAGLE,[b] DEIRDRE K. MULLIGAN,[c] NATHANIEL GOOD,[d] & JENS GROSSKLAGS[e]

The Federal Trade Commission and Consumer Privacy in the Coming Decade

Abstract:[f] The large majority of consumers believe that the term "privacy policy" describes a baseline level of information practices that protect their privacy. In short,

---

[a] Joseph Turow, Ph.D., is the Robert Lewis Shayon Professor of Communication at the University of Pennsylvania's Annenberg School for Communication, and the director of the Information & Society Program at the University of Pennsylvania's Annenberg Public Policy Center. He is the author of, among other books, *Niche Envy: Marketing Discrimination in the Digital Age* (Cambridge, MA: MIT Press, 2006).

[b] Chris Jay Hoofnagle, J.D., is a senior staff attorney at the Samuelson Law, Technology & Public Policy Clinic, and a senior fellow at the Berkeley Center for Law & Technology of the Boalt Hall School of Law.

[c] Deirdre K. Mulligan, J.D., is the director of the Samuelson Law, Technology & Public Policy Clinic and the Clinical Program at the Boalt Hall School of Law. The work of the Samuelson Clinic is generously supported through an endowment from Professor Pamela Samuelson and Robert Glushko, Ph.D. Additional funding is provided by: The Rose Foundation for Communities and the Environment, the California Consumer Protection Foundation, and the National Science Foundation, Team for Research in Ubiquitous Secure Technologies, NSF CCF-0424422.

[d] Nathaniel Good is a Ph.D. candidate at the School of Information at the University of California, Berkeley.

[e] Jens Grossklags is a Ph.D. candidate at the School of Information at the University of California, Berkeley. His work is supported in part by the National Science Foundation through ITR award ANI-0331659.

[f] This article originally appeared as a paper presented under the same title at the Federal Trade Commission Tech-ade Workshop on November 8, 2006. The version published here contains additional information collected during a 2007 survey.

"privacy," like "free" before it, has taken on a normative meaning in the marketplace. When consumers see the term "privacy policy," they believe that their personal information will be protected in specific ways; in particular, they assume that a website that advertises a privacy policy will not share their personal information. Of course, this is not the case. Privacy policies today come in all different flavors. Some companies make affirmative commitments not to share the personal information of their consumers. In other cases, however, privacy policies simply inform consumers that unless they "opt out" of sharing certain information, the company will communicate their personal information to other commercial entities.[1]

Given that consumers today associate the term "privacy policy" with specific practices that afford a normative level of privacy protection, the use of the term by a website that does not adhere to these baseline practices can mislead consumers to expect privacy that, in reality, does not exist. This is not to suggest that companies intend to mislead consumers, but rather that consumers today associate certain practices with "privacy policy" just as they associate certain terms and conditions with the word "free."

Because the term "privacy policy" has taken on a specific meaning in the marketplace and connotes a particular level of protection to consumers, the Federal Trade Commission ("FTC") should regulate the use of the term "privacy policy" to ensure that companies using the term deliver a set of protections that meet consumers' expectations and that the term "privacy policy" does not mislead consumers during marketplace transactions.

[1] Often consumers are not provided with a means to "opt out" of information sharing.

I. INTRODUCTION

Ten years have passed since the FTC's last comprehensive hearings on the future of consumer protection. In that time, the FTC has pursued a self-regulatory approach to protecting the privacy of personal information, working with industry to deliver market-based approaches ranging from industry best practices, self-regulatory initiatives, advances in technology, and consumer education.

A core goal of these efforts has been to publicize how personal information is handled by companies, in the belief that, if armed with accurate information, consumers will make privacy choices consistent with their personal needs. The FTC has established a set of disclosures that responsible companies should provide to consumers in order to facilitate the consumers' exercise of informed choice about privacy in the marketplace.

Ten years later, it is appropriate to ask what effects these disclosures have had on consumers' experiences in the marketplace. Have improved privacy disclosures allowed consumers to achieve the level of privacy they desire in marketplace transactions? Are consumers more at ease with respect to privacy in marketplace transactions today then they were ten years ago? What is the effect of the existence of "privacy policies" at most of the leading websites? What do consumers think when they see the term "privacy policy"?

This article attempts to answer these questions based on existing peer-reviewed research and consumer surveys conducted in the academic sector. The article examines the strengths and limitations of the notice-based approach to facilitating privacy in the consumer marketplace. Using (1) survey data on consumers' privacy expectations, (2) existing research on whether and in what instances consumers read and comprehend notices, (3) the role information asymmetry and psychological barriers to information processing and risk assessment play in privacy decision-making, and (4) insights about interface design and information presentation, this article identifies several factors that limit the ability of the notice-based approach, operating alone, to meet the varying privacy needs of consumers in the marketplace. It concludes that:

- Without a baseline set of information practices, the term "privacy policy" is confusing to the consumer;

- The lack of common disclosure language undermines consumers' ability to "shop for privacy," thereby undermining businesses' ability to compete on privacy;

- Shortened notices are a promising step toward encouraging a successful privacy marketplace for the consumers who read notices;

- Privacy must be "usable" if it is to serve consumer needs; therefore, incorporating expertise from fields such as human computer interaction and psychology is imperative; and

- If consumers are not able to make informed choices about information privacy and computer security, then it is inevitable that bad actors will undermine consumer privacy and the security of the network infrastructure.

At this ten-year interval, it is important to consider the effect of the FTC's approach to privacy. Research provides important information about the strengths and limitations of the FTC's work to date. The FTC should use this information to refine and adjust its policy to reflect what we know today about consumer expectations and actions in the marketplace. In addition, this article's conclusions, listed above, suggest several additional interventions in the marketplace:

- Require businesses that advertise a "privacy policy" to provide some baseline privacy protections that meet established consumer expectations;

- Standardize disclosures and terminology to facilitate comparison shopping by consumers and competition among firms based on privacy practices;

- Shorten notices to reduce the transaction costs associated with reading long, indecipherable End User License Agreements ("EULAs"); and,

- Include information from other disciplines, including usability and human computer interaction, in future privacy and security initiatives.

II. THE FTC'S APPROACH TO CONSUMER PRIVACY

Just over ten years ago, the FTC conducted its last forward-looking proceeding in which it analyzed the future of consumer protection in a high-tech economy. In a report from that proceeding, the FTC concluded that the essential elements of a balanced consumer protection program are:

- Coordinated law enforcement by state and federal agencies against fraud and deception;
- Industry self-regulation and private initiatives to protect consumers; and
- Consumer education through the combined efforts of government, business, and consumer groups.[2]

The report continues:

> The hearing record is replete with examples of private initiatives: industry self-regulation programs and plans to develop and expand such programs, technology-based consumer protections and self-help opportunities, and commitments to undertake new consumer education programs. These and other initiatives will be crucial in providing consumer protection in the new marketplace.[3]

Over the past ten years, the FTC has pursued these three goals. It has brought an impressive array of actions under the agency's authority to prosecute unfair or deceptive trade practices.[4] It has fostered self-regulatory programs and it continues to operate multilingual consumer outreach both online and offline.

The FTC established five Fair Information Practice Principles ("FIPPS")—notice, choice, access, security and accountability—as the

---

[2] Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (hearing report, May 1996): 46 (formatting added). Also available online at http://www.ftc.gov/opp/global/report/gc_v2.pdf.

[3] Ibid.

[4] Marcia Hoffman, "Federal Trade Commission Enforcement of Privacy," in *Proskauer on Privacy* (New York: Practicing Law Institute, 2006).

framework for self-regulatory and regulatory initiatives. The Commission's approach omitted several important data protection principles that were recognized by the Organization for Economic Cooperation and Development Guidelines ("OECD"), including the concepts of "data minimization," which requires companies to restrict the amount of personal information collected to only that which is necessary for a transaction, and "purpose specification," which requires companies to have a clear and legitimate purpose for data collection.

The absence of these two principles has led firms to collect extraneous information and to repurpose information without consumer consent. After adopting its limited set of FIPPS, the FTC highlighted the importance of notice and security. The agency did intervene to set standards for children's privacy that are stronger than the norm; the Children's Online Privacy Protection Act ("COPPA") requires prior parental consent before personal information can be collected from children under the age of thirteen.[5] In general, though, the agency put substantial resources behind encouraging adaptation of notice, and the development of "short notices." The market-based approach to privacy in the electronic commerce sphere adopted by the FTC was a departure from a tradition of privacy laws, such as the Fair Credit Reporting Act of 1970 ("FCRA") and the Privacy Act of 1974, which embraced a full set of FIPPS to protect personal information.

Most e-commerce sites today have privacy policies, but whether these policies provide privacy protection remains an open question. The FTC has not evaluated the basic assumption of the market-based model to privacy protection: that with good information consumers will make good choices. Echoing the recommendations from the 1995 hearings, Chairman Majoras seeks to employ the same techniques used to protect privacy during the last decade:

> First, we must study and evaluate new technologies so that we are as prepared as possible to deal with harmful, collateral developments. Second, we need to bring appropriate law enforcement actions to reaffirm that fundamental principles of FTC law apply in the context of new technologies. Third, we must look to industry to implement self-regulatory regimes and, more importantly, to

---

[5] *Children's Online Privacy Protection Act of 1998*, Public Law 105-277, codified at *U.S. Code* 15 (2000), §§ 6501 *et seq.*

> develop new technologies. Finally, we need to educate consumers so that they can take steps to protect themselves.[6]

At this important juncture, it makes sense to evaluate the strengths and weaknesses of these techniques. Before the FTC decides what approaches to pursue during the next decade, we suggest that the agency critically reflect on research that explores the effectiveness of the self-regulatory system.

The FTC has held close the assumption that introducing additional information about companies' data practices into the marketplace through self-regulatory systems, combined with consumer self-help, will allow consumers to adequately protect their privacy as they see fit. But research shows that consumers continue to have high levels of concern for privacy of personal information. It also reveals that the EULAs and privacy policies used to convey this information to consumers are not effective—they are rarely read and are in many instances unreadable. More importantly, consumers appear to believe that the term "privacy policy" conveys a specific level of privacy protection. Confusion exists among consumers concerning what rights they have and can exercise over personal information. Interestingly, while the FTC has pursued self-regulatory solutions to consumer privacy, the large majority of consumers believe incorrectly that laws protect their personal information from secondary use.

III. RESEARCH DEMONSTRATES THE LIMITS OF THE DISCLOSURE-BASED APPROACH

A. CONSUMERS CARE DEEPLY ABOUT PRIVACY

Surveys conducted by the Annenberg Public Policy Center show that Americans care deeply about the privacy of their personal information and that despite the FTC's ten-year commitment to self-regulation, they are nevertheless concerned about information collection.[7] A 2003 Annenberg survey found that 70% of advanced

---

[6] Deborah Platt Majoras, "Finding the Solutions to Fight Spyware: The FTC's Three Enforcement Principles," (remarks, Anti-Spyware Coalition, Washington, D.C., February 9, 2006): 3, http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf.

[7] Unless otherwise noted, the public polling data presented are from two national surveys created by Professor Turow and carried out by the firm ICR/International Communication Research of Media, Pennsylvania. For the 2003 survey, *infra* note 8, ICR interviewed by phone a nationally representative sample of 1,200 adults who were using the Internet at home.

users agreed or agreed strongly with the statement, "I am nervous about websites having information about me."[8] In 2005, the same response was reported by 79% of respondents.[9] Individuals also believe that they are put at risk as a result of information collection. Only 17% agreed with the proposition, "What companies know about me won't hurt me."[10]

A high level of concern is also reported about both commercial and government collection of personal information. In 2003, 92% reported that they would be concerned if marketers were "collecting information about your household members' activities without your knowledge or consent."[11] Similarly 83% would be concerned if the government was "collecting information about your household members' activities without your knowledge or consent."[12] (52% believed the federal government was doing that.[13]) Respondents also believe that they should be in control of marketing communications. For instance, 94% reported that websites should ask for permission before sending ads.[14]

B. CONSUMERS FUNDAMENTALLY MISUNDERSTAND THE "PRIVACY POLICY" LABEL

Supporters of privacy self-regulation suggest that Americans' high levels of concern will be alleviated when they begin to examine their options for releasing personal data. Professor Alan Westin, for

---

For the 2005 survey, *infra* note 9, ICR interviewed by phone a nationally representative sample of 1,200 adults who said they used the Internet in the past month.

[8] Joseph Turow, *Americans and Online Privacy: The System is Broken* (Philadelphia: Annenberg Public Policy Center, June 2003): 16. Also available online at http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.

[9] Joseph Turow, Lauren Feldman and Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline* (Philadelphia: Annenberg Public Policy Center, June 2005): 4. Also available online at http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/Turow_APPC_Report_WEB_FINAL.pdf.

[10] Ibid.

[11] Turow, *Americans and Online Privacy*, 19–20.

[12] Ibid.

[13] Ibid., 19.

[14] Ibid., 28.

example, has written that most Americans take an informed cost-benefit tack in relation to their information online and offline.[15] "They examined the benefits to them or society of the data collection and use, wanted to know the privacy risks and how organizations proposed to control those, and then decided whether to trust the organization or seek legal oversight."[16] This characterization of most Americans as being aware of their online privacy options supports the viewpoint of Internet industry players that posting an accurate privacy policy on every site would create a world of optimal consumer privacy in which each individual shopped with his or her mouse for privacy that matched his or her personal needs.

Unfortunately that does not appear to be happening. One could assume from this that consumers do not care, the argument being that companies give individuals information and they ignore it or fail to value the privacy choices it offers. However, research tells a far more complex story about why privacy disclosures alone have failed to alleviate the privacy concerns of individuals.

The push for privacy disclosures has resulted in a world of legalistically phrased privacy policies that begin by assuring the consumer that the site cares about his or her privacy, but then proceeds to confuse the consumer with technical language about "affiliate" and "non-affiliate" sharing, required disclosures, distinctions between personally identifiable information ("PII") and aggregate data, inapplicability with regard to other sites, or content that may be included or accessed from the site, and finish with the caveat that the privacy policy can change at any time, with or without notice.[17]

Both the 2003 and 2005 Annenberg surveys revealed, however, that American adults do not know that privacy policies merely tell people how the site will use their information: whether or not, and how, they will share it with affiliates and outside firms.[18] Most

---

[15] A. F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59, no.2 (2003): 445.

[16] Ibid.

[17] For example, of 64 website privacy policies that were reviewed between 2001 and 2003, Jensen and Potts found that eight (13%) offered no mention of how changes to the policy would be conveyed to the user, twelve policies (19%) offered to notify users through email and a posting on the policy page, and 44 policies (69%) required users to check the policy page periodically. C. Jensen and C. Potts, "Privacy Policies as Decision-making Tools: An Evaluation on Online Privacy Notices," in *CHI 2004 Connect: Conference Proceedings* (New York: ACM Press, 2004), 471–78.

[18] Turow, *Americans and Online Privacy*, 3; Turow, Feldman and Meltzer, *Open to Exploitation*, 3.

Americans believe, logically, that the phrase "privacy policy" signifies that *their information will be kept private*. In the 2003 survey, 57% of the nationally representative sample of 1,200 adults who were using the Internet at home agreed or agreed strongly with the statement, "When a web site has a privacy policy, I know that the site will not share my information with other websites or companies."[19] In the 2005 survey, questioners asked 1,200 nationally representative adults who said they had used the Internet in the past month whether that statement is true or false; 59% answered it is true.[20]

C. CONSUMERS MISUNDERSTAND ONLINE DATA COLLECTION

The misunderstandings do not stop with the label. The 2003 survey found that 59% of adults who use the Internet at home know that websites collect information about them even if they do not register;[21] however, they do not understand that data-flows behind their screens connect seemingly unrelated bits about them.[22] The survey's interviewers asked respondents to name a site they valued and then went on to ask their reaction to click-stream advertising,[23] which is actually a common way that sites track, extract and share information to make money from advertising. Of the surveyed adults who go online at home, 85% stated that they did not agree to the collection and aggregation of their data across multiple sites for purposes of click-stream advertising, even by a "valued" site.[24] When offered a choice of using a valued site for free and letting information be collected, or paying for the site and not letting information be collected, 54% of adults who go online at home said that they would rather find the information offline than exercise either option presented.[25]

---

[19] Turow, *Americans and Online Privacy*, 3.

[20] Turow, Feldman and Meltzer, *Open to Exploitation,* 20.

[21] Turow, *Americans and Online Privacy*, 3.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Ibid.

Among the 85% who did not accept the data-collection practice, one in two (52%) had earlier said that they gave or would likely give the valued site their real name and email address.[26] Yet those bits of information are what a site needs to begin creating a stream of data about them—the very flow, personally identifiable or not, that they refused to allow in response to the scenario. Moreover, 63% of the people who said they had provided this data had also agreed that the mere presence of a website privacy policy means that the website will not share data with other firms.[27] Bringing these two results together suggests that at least one out of every three respondents who refused to barter their information either do not understand or do not think through the privacy outcomes of basic data-collection activities on the Internet.

Similarly, other fundamental processes involved in online interactions are not very well understood by the consumer. In a related survey, Acquisti and Grossklags show that individuals are often unable to name obvious parties, beyond the merchant and the consumer, that have access to consumer data during and after an online credit card transaction, such as the credit card company.[28] These findings help uncover the important distinction between knowledge about commercial practices that is active and actionable, and knowledge that is passive or completely lacking. Most consumers have some passive knowledge about the roles played by credit card companies, other third parties, and technical processes, but it is doubtful that this knowledge is always available to them when they are actively making decisions.

D. CONSUMERS MISUNDERSTAND MANY RULES ABOUT PRIVACY IN THE MARKETPLACE

These misconceptions about information privacy and data practices are, however, merely the tip of an iceberg of consumer confusion concerning their rights and merchants' rights to consumer information

---

[26] Ibid.

[27] Ibid., 23.

[28] When 119 university staff and students were confronted with the open-ended question: "You completed a credit-card purchase with an online merchant. Besides you and the merchant Web site, who else has data about parts of your transaction?" 34.5 percent of the sample answered "nobody," 21.9 percent answered "my credit card company or bank," and 19.3 percent answered "hackers or distributors of spyware." A. Acquisti and J. Grossklags, *Privacy and Rationality in Individual Decision Making*, *IEEE Sec. & Privacy* 3, no. 1 (2005): 26–33.

in the marketplace. Table 1 lists true-or-false statements that the 2005 Annenberg survey presented to its representative national sample.[29] The answers indicate a low level of understanding of consumer rights and redress in the marketplace. A high proportion of consumers believe they have certain privacy rights—notably consistent with those provided under FIPPS—when they do not. Others simply have no idea what rights they have.

Table 1: True/false responses to statements about rules of profiling, behavioral targeting, price discrimination and recourse in the marketplace. (1,500 persons sampled)

	%T	%F	%DK
Most online merchants give me the opportunity to see the information they gather about me. *47% did not know the right answer*	23	**53**	25
Most online merchants allow me the opportunity to erase information they have gathered about me. *50% did not know the right answer*	19	**50**	30
A website is allowed to share information about me with affiliates without telling me the names of the affiliates. *49% did not know the right answer*	**51**	29	20
It is legal for an online store to charge different people different prices at the same time of day. *62% did not know the right answer*	**38**	29	33
Respondent correctly identifies the name of a credit-reporting agency. *66% did not know the right answer*	**34**	66	--
By law, a site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices. *68% did not know the right answer*	37	**32**	31

[29] Turow, Feldman and Meltzer, *Open to Exploitation*, 15.

Table 1: (continued)			
It is legal for an offline store to charge different people different prices at the same time of day. *71% did not know the right answer*	**29**	42	29
Bold numbers indicate the correct answer. Sums greater than 100% result from rounding errors. DK=Don't Know			

A 2007 Golden Bear telephone survey of Californians reinforces the idea of consumer misunderstanding about online marketplace privacy policies and rules.[30] This survey focused on people who have actually purchased items on the Internet and, as such, would presumably be more informed than participants in the Annenberg studies, who were adults who used the Internet for any reason. Moreover, the statements about rules and privacy policies in the Golden Bear survey were more varied than those in the Annenberg study.

Despite their presumably greater stake in commerce and privacy than the Annenberg respondents, the Golden Bear respondents followed the same pattern; almost 70% of the respondents knew that sites are allowed to keep records of their addresses and purchase histories. The respondents' knowledge was much worse, however, with respect to the other statements about privacy policies and marketplace rules, as Table 2 shows. Note that when presented with a privacy-policy statement that was similar to the one in the Annenberg study—if a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies—the percentage of respondents who answered incorrectly was very similar, 55% in Golden Bear compared to 59% in Annenberg.

[30] The 2007 Golden Bear Omnibus Survey was a random-digit telephone survey of 1,186 English- and Spanish-speaking adults in California. It was conducted by the University of California's Survey Research Center using Computer-Assisted Telephone Interviewing (CATI) to landline and wireless phones from April 30, 2007, to September 2, 2007. It was funded by the Survey Research Center. The privacy questions were funded by the Samuelson Clinic.

Table 2: True/false responses to statements about rules of the online marketplace.

	%T	%F	%DK
If a website has a privacy policy, it means that the site cannot keep records of your address and purchase history. (188 persons sampled) *30.9% did not know the right answer*	19.7	**69.1**	11.2
If a website has a privacy policy, it means that the site cannot give information about your address and purchases to the government. (208 persons sampled) *45.2% did not know the right answer*	36.1	**54.8**	9.1
If a website has a privacy policy, it means that the site cannot use information to analyze your online activities. (205 persons sampled) *47.8% did not know the right answer*	37.1	**52.2**	10.7
If a website has a privacy policy, it means that the site cannot buy information about you from other sources to analyze your online activities. (251 persons sampled) *50.6% did not know the right answer*	39.8	**49.4**	10.8
If a website has a privacy policy, it means that the site cannot share information about your address and purchases with affiliated companies that are owned by the website. (207 persons sampled) *55% did not know the right answer*	47.8	**44.9**	7.2
If a website has a privacy policy, it means that you have the right to require the website to tell you what other businesses purchased your personal information. (208 persons sampled) *60.1% did not know the right answer*	51.9	**39.9**	8.2

Table 2: (continued)	**%T**	**%F**	**%DK**
If a website has a privacy policy, it means that you have the right to obtain help from the website, if information you provided to it was used for identity theft. (198 persons sampled) *64.1% did not know the right answer*	49.5	**35.9**	14.6
If a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies. (231 persons sampled) *64.5% did not know the right answer*	55.4	**35.5**	9.1
If a website has a privacy policy, it means that you have the right to sue the website for damages if it violates your privacy. (230 persons sampled) *65.6% did not know the right answer*	53	**34.3**	12.6
If a website has a privacy policy, it means that you have the right to access your personal information stored on the site and correct it. (222 persons sampled) *72.1% did not know the right answer*	56.8	**27.9**	15.3
If a website has a privacy policy, it means that you have the right to be notified if the website has a security breach that leaks information about you to others. (215 persons sampled) *75.4 did not know the right answer*	64.7	**24.7**	10.7
If a website has a privacy policy, it means that you have the right to require the company to delete your personal information upon your request. (213 persons sampled) *77% did not know the right answer*	68.1	**23**	8.9
Bold numbers indicate the correct answer. Sums greater than 100% result from rounding errors. DK=Don't Know.			

E. PRIVACY NOTICES ALONE ARE INSUFFICIENT

Despite self-regulatory efforts, there remains substantial confusion among consumers about information privacy. Much of the FTC's attention has focused on the development of improved disclosures. Surveys, user studies, and focus groups do support the agency's belief that users would welcome well-crafted, short notices in the hope that they will ease comprehension of privacy policies.

In research supported by the National Science Foundation Science and Technology Center, Team for Research in Ubiquitous Secure Technologies ("TRUST"),[31] researchers at U.C. Berkeley's Samuelson Clinic have examined the utility of short notices and variations on notice timing in communicating about privacy, security, and other consequences of software installation.[32] The installation of downloadable software almost always involves the click-through to privacy notices and EULAs. Notices are usually presented in a separate screen during installation and are reasonably accessible to the user. Users are involved in a main task of evaluating and deciding whether to install a piece of software. Given that information about security, privacy, and functionality are disclosed during the installation process, this is a natural context in which to explore the utility of such notices and disclosures.

Recent studies involving EULAs suggest that they are largely ineffective as a means of communicating with consumers. EULAs, terms-of-service agreements ("ToS"), and privacy policies present complex legal information. Research shows that notices' complexity

---

[31] This work was generously supported by the NSF Science and Technology Center, Team for Research in Ubiquitous Secure Technologies ("TRUST"), NSF CCF-0424422. Computer trustworthiness continues to increase in importance as a pressing scientific, economic, and social problem. As a consequence, there is an acute need for developing a much deeper understanding of the scientific foundations of cyber security and critical infrastructure systems, as well as their implications for economic and public policy. In response to this need, TRUST is devoted to the development of a new science and technology that will radically transform the ability of organizations (software vendors, operators, local and federal agencies) to design, build, and operate trustworthy information systems for our critical infrastructure. The Center brings together a team with a proven track record in relevant areas of computer security, systems modeling and analysis, software technology, economics, and social sciences. See http://trust.eecs.berkeley.edu/ for details of all of TRUST's research.

[32] For detailed results of the studies, see Nathaniel Good and others, "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware," in *Proceedings of the Symposium on Usable Privacy and Security* (New York: ACM Press, 2005), 43–52; Nathaniel Good and others, "Noticing Notice: A Large-scale Experiment on the Timing of Software License Agreements" in *Proceedings of CHI 2007* (New York: ACM Press, 2007), 607–16.

hampers users' ability to understand such agreements. For example, Jensen and Potts studied a sample of 64 privacy policies from high-traffic and healthcare websites.[33] They found that the policies' formats, locations on the websites, and legal content severely limit users' ability to make informed decisions based on them.[34]

In another study that produced similar results, Grossklags and Good evaluated the notice practices of 50 popular downloadable programs.[35] The location and presentation of the notices differed from vendor to vendor, which would make it more difficult for consumers to find relevant information. These notices were often difficult to understand or even read. The average EULA was over 2500 words long and would require approximately thirteen minutes for a consumer of average reading skill to parse, according to accepted reading metrics. Font sizes were often too small to be read easily and notices were displayed in comparatively small windows, for example, showing only one percent of the complete notice text at a time.

Research indicates that simplifying the notices has a limited effect. Masson and Waldron showed that simplifying the language of legal contracts, for example, by using easier words and replacing obscure terms with common ones, could not achieve very high degrees of comprehension.[36] This is because "non-experts have difficulty understanding complex legal concepts that sometimes conflict with prior knowledge and beliefs."[37]

Vila and others ask whether users will ever bother to read or believe privacy policies at all.[38] They claim that because the cost of

---

[33] Jensen and Potts, "Privacy Policies as Decision-making Tools: An Evaluation on Online Privacy Notices."

[34] Ibid.

[35] Jens Grossklags and Nathan Good, "Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers," in *Lecture Notes in Computer Science* (Berlin: Springer, 2008), 341–55. Originally presented at Useable Security (USEC'07), February 15–16, 2007. Also available online at http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags07-USEC.pdf.

[36] M.E.J. Masson and M.A. Waldron, "Comprehension of Legal Contracts by Non-experts: Effectiveness of Plain Language Redrafting," *Applied Cognitive Psychology* 8 (1994): 67–85.

[37] Ibid.

[38] T. Vila, R. Greenstadt and D. Molnar, "Why We Can't be Bothered Reading Privacy Policies - Models of Privacy Economics as a Lemons Market," in *Proceedings of the Fifth International Conference on Electronic Commerce* (Pittsburg: ICEC, 2005), 403–07. Also available online at http://www.eecs.harvard.edu/~greenie/econprivacy.pdf.

misrepresentation in a privacy policy is low and that some of the privacy policies are not trustworthy, users do not feel it is worth their time to read or pay attention to them.[39] In contrast, results from the 2003 Annenberg survey suggest that relatively high proportions of adults with the Internet at home trust privacy policies; 71% agreed or agreed strongly, "I look to see if a website has a privacy policy before answering any questions."[40] Anecdotal evidence does, however, support the impression that people do not read the policies. One software provider included a $1000 cash prize offer in a EULA that was displayed during every software installation. It took four months and 3,000 downloads of the software for someone to notice the clause and claim the prize.[41]

Among 222 study participants, the Samuelson Clinic found that only 1.4% reported reading EULAs often and thoroughly, 66.2% admit to rarely reading or browsing the contents of EULAs, and 7.7% indicated that they have not noticed these agreements in the past or have never read them.[42]

Short and layered notices are one method that has been proposed to overcome these problems. The Samuelson Clinic has performed a controlled study of short notices and timing of notices. The study examined whether consumers were happy with their installation decisions after they were fully informed of the program's activities; this is termed "regret." When downloading and installing programs, subjects were shown either the EULA by itself or the EULA and a short notice highlighting core aspects of performance, privacy and security.

During the post-experimental survey, all study participants were shown the short notices. When asked whether they would install the programs they chose to install during the experiment, participants who received the short notices during the study were less likely to reverse their earlier decision to install software. However, many users, both those who originally received the short notice and those who did not, expressed regret about their installation decisions after reading the short notice during the exit interview. Overall, the incidence of regret

---

[39] Ibid.

[40] Turow, *Americans and Online Privacy*, 18.

[41] Larry Magid, It Pays To Read License Agreements, http://www.pcpitstop.com/spycheck/eula.asp (accessed January 22, 2008).

[42] See 2007 Golden Bear Omnibus Survey.

was high. Importantly, however, the incidence of regret was lower when short notices were received before program installation.

F. OTHER FORCES ALSO PREVENT CONSUMERS FROM SUCCESSFUL PRIVACY PROTECTION

Beyond the issues of whether consumers read and comprehend privacy policies, individuals' ability to make marketplace privacy decisions that reflect their needs is hampered by several factors. Incomplete information is a major difficulty. Even when they read privacy notices and EULAs, consumers have trouble evaluating the consequences of disclosing the bundles of information that companies say they are taking. Consumers have difficulty assessing and valuing certain privacy risks, which makes their decisions seem unpredictable, even random. Sometimes risks become known only after a security breach or privacy invasion.

Moreover, while many consumers are certainly aware of many privacy risks, they may not be well informed about the magnitude of these risks in certain circumstances. Acquisti and Grossklags report, for example, that 73% of respondents in their survey underestimated the risk of becoming a victim of identity theft.[43]

> Adding to the problem of incomplete information is the challenge of grasping the abilities of technologists to take seemingly innocuous items of information and link them in new, unexpected ways. For example, when asked, "Imagine that somebody does not know you but knows your date of birth, sex, and zip code. What do you think the probability is that this person can uniquely identify you based on those data?," 68.6% answered that the probability was 50% or less (and 45.5% of respondents believed that probability to be less than 25%). According to Carnegie Mellon University researcher Latanya Sweeney, however, 87% of the US population may be uniquely identified personally through a 5-digit zip code, birth date, and sex. To expect individuals to foresee such possibilities is unreasonable.[44]

---

[43] Acquisti and Grossklags, *Privacy and Rationality*.

[44] Ibid., 24.

Even if individuals have access to complete information about privacy risks and modes of protection, they might not be able to process enough data to formulate a rational privacy-sensitive decision. Human beings' rationality is bounded, which limits our ability to acquire and then apply information. Furthermore, consumers are busy and experience many demands on their attention. They cannot be expected to be familiar with all the vagaries of technologies, e-commerce, and evolving business practices.

G. CONSUMERS ARE LIMITED IN THEIR ATTEMPTS TO PROTECT THEIR INFORMATION

Evidence abounds that consumers do try to protect their privacy. Survey results released in June 2004 by Privacy & American Business found that two-thirds of Americans have taken some steps to protect their privacy.[45] In fact, 87% indicated that they had asked a company to remove their information from a marketing database; 60% decided not to patronize a store because of doubts about the company's privacy protections; and 65% had declined to register at an e-commerce site because of privacy concerns.[46] Among individuals that Westin has described as the "privacy unconcerned," 47% reported that they engaged in four out of seven identified privacy-protecting behaviors, while 65% of the "privacy pragmatists" had engaged in these behaviors.[47]

Situational characteristics can reduce consumers' efforts to protect their information. For example, Spiekermann, Grossklags, and Berendt observed 171 study participants while they shopped online, specifically when they interacted with an anthropomorphic sales advisor. By answering questions posed by the advisor, study participants could receive recommendations about products. The advisor also asked questions that were highly intrusive of privacy or that requested irrelevant information. Participants could simply have refused to respond to these questions, thereby protecting themselves against potential threats. However, regardless of the strength of the participants' self-reported privacy preferences, their actual responses

---

[45] Privacy & American Business, "New National Survey on Consumer Privacy Attitudes to be Released at Privacy & American Business Landmark Conference," news release, June 10, 2004.

[46] Ibid.

[47] Westin, "Social and Political Dimensions of Privacy," 445.

to the advisor revealed much more information than their self-reported preferences predicted, even among the "privacy-concerned" individuals. These results demonstrate the power of interactive marketing techniques to lead even privacy-motivated consumers to behave in ways that appear contradictory to their stated preferences.[48] The similarity between the behavior of the "unconcerned" participants and the behavior of participants who claim to be highly concerned about privacy suggests that Westin's dichotomy may be less useful than previously thought in capturing the nuances of consumers' attitudes on privacy.

Further evidence that we need a more differentiated understanding of protection behaviors is provided by Acquisti and Grossklags.[49] They found that at least 75% of the consumers did adopt at least one strategy or technology, or otherwise took some action, to protect their privacy, such as interrupting purchases before entering personal information or providing incorrect information in website forms.[50] However, they also found that use of specific technologies was consistently low across the sample population.[51] For example, 67% of respondents never encrypted their email, 82% never put a credit alert on their credit report, and 82% never removed their phone numbers from public directories.[52]

Other findings suggest that while people would like to protect their privacy, and try to at the most basic levels, a large proportion of these people do not have the knowledge necessary to move beyond the very basics of privacy-protective behavior. Before concluding that people do not put a credit alert on their credit report because they are lazy or uncaring, recall the Annenberg survey finding that 66% do not know the name of a credit agency and 76% do not correctly respond "false" to the statement, "the Federal Trade Commission will correct errors in credit reports if it is shown proof of the errors."

---

[48] S. Spiekermann, J. Grossklags and B. Berendt, "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior," in *Proceedings of the 3rd ACM Conference on Electronic Commerce*, (New York: ACM Press, 2001), 38–47. Also available online at http://people.ischool.berkeley.edu/~jensg/research/paper/grossklags_e-Privacy.pdf.

[49] Acquisti and Grossklags, *Privacy and Rationality in Individual Decision Making*, 26–33.

[50] Ibid.

[51] Ibid.

[52] Ibid.

In the online environment, the complexity of privacy-protecting actions increases, and thus the likelihood that Americans perform them decreases substantially. The 2003 Annenberg survey asked American adults who use the Internet at home if they performed certain activities in relation to controlling their information online; 65% said that the have erased unwanted cookies at least once. This finding is consistent with the finding that a clear majority of the sample—59%—was aware of what cookies do; people know that when they go online, sites collect information on them even if they do not register. The percentage applying other privacy tools drops steeply, however. Only 43% said that they have used filters to block unwanted email, 23% said they have used software that looks for spyware, and 17% said they have used anonymizers—"software that hides your computer's identity from websites that they visit."

IV. WHAT THE FTC MUST CONFRONT IN THE NEXT DECADE

A. AMERICANS' CONTINUING CONCERNS AND CONFUSIONS ABOUT INFORMATION PRIVACY

Research indicates that American consumers care deeply about information privacy and worry that it is not well protected. It also reveals that great majorities of American consumers do not grasp basic facts about companies' data collection practices, do not know the laws that govern data protection, do not read or comprehend the notices that are supposed to explain data practices and afford privacy choices, and are confronted with many social and psychological factors that undermine their ability to protect their privacy during marketplace transactions.

Most fundamentally, research indicates that a large majority of American adults believe that the existence of a "privacy policy" on a website indicates some level of substantive privacy protection for their personal information. The finding is not an aberration. Two major national surveys performed two years apart, in 2003 and 2005, revealed virtually the same percentage of Americans—almost 60%—believed that "when a website has a privacy policy, that means it will not share information about them with other websites or companies."[53] In the 2005 survey, where the statement was presented in true/false

[53] Turow, *Americans and Online Privacy*, 4; Turow, Feldman and Meltzer, *Open to Exploitation*, 20.

form, 59% incorrectly said the statement was true and an additional 16% said they did not know if it was true or false.[54]

Because American consumers mistakenly believe that a "privacy policy" indicates a level of substantive privacy protection, they do not read them. The failure to read privacy policies leaves consumers unaware of data practices such as data-mining and allows a wide range of practices that are inconsistent with consumer expectations to avoid consumer scrutiny.

Under the Federal Trade Commission's notice and choice regime, the operating assumption is that people will make good choices if they are provided with good information. Our studies have found that Americans do not have good, i.e., full and understandable, information about data practices that affect their privacy.[55] More significantly, even if full and understandable information is provided in a short format, consumers retain the belief that the mere invocation of the term "privacy policy" creates a baseline set of protections for their information. That belief, along with other cognitive biases, limits the number of consumers who read and act on such privacy notices. If a website contains a privacy policy that states it will reveal users' data to affiliates or other companies without the users' permission, then the privacy of consumers who stop reading once they see that a privacy policy exists is undermined.

B. THE CURRENT NOTICE-BASED APPROACH HAS CONSEQUENCES FOR THE SECURITY OF THE NETWORK ITSELF

Consumers' basic misunderstanding of the purpose of privacy policies is one of many misconceptions that contribute to confusion in the online marketplace. When consumers do not read, or read but cannot understand, privacy notices and EULAs on websites and software, they may unwittingly install malicious programs that exploit consumer machines to the detriment of the entire Internet. Unless "privacy policies" provide some baseline privacy protections, the notice-based privacy regime will continue to unintentionally lead consumers to "consent" to invasive program installations and other practices. By doing so, they lower the security protections of the entire network, not just their own computers.

---

[54] Turow, Feldman and Meltzer, *Open to Exploitation*, 15.

[55] See Turow, *Americans and Online Privacy*; Turow, Feldman and Meltzer, *Open to Exploitation*.

One case in point is the 2005 wide-scale installation of a "rootkit" by purchasers of music CDs.[56] In an attempt to control the distribution of songs on the CD, Sony bundled a program that ran silently in the background and opened many computers to security vulnerabilities. Similarly, spyware, even if "consensually" installed pursuant to a EULA, can allow millions of computers to be controlled by others. This allows bad actors to create "botnets," e.g. zombie networks of consumers' computers, which can be remotely directed to engage in denial-of-service attacks and other malicious acts.

C. THE NEED TO ADOPT THREE POLICIES TO SUPPORT INFORMATION PRIVACY

To advance privacy, the Federal Trade Commission should take the following three steps:

1. THE FTC SHOULD POLICE THE TERM "PRIVACY POLICY"

Two national surveys by the Annenberg Public Policy Center revealed that to a majority of American consumers, "privacy policy" carries a particular meaning: that a website will not disclose personal information to others without the consumer's permission. While many websites begin their privacy policies with the claim that "your privacy is important to us," many of these same policies disclose further down that the websites collect quite a bit of the information from their users and often do share the information with affiliates, marketers, or other entities. Note, too, that information-sharing agreements with third parties generally are under no legal requirement to be disclosed; there is no other source for this omitted information. The result is a situation where consumers assume that the privacy policy label indicates that the site will not share data, whereas the opposite may be true and the policy may or may not state what is done with the information.

Given consumers' expectations, the use of the term "privacy policy" absent some baseline privacy protections, ought to be considered deceptive. The Commission evaluates potentially deceptive marketing communications to consumers based upon

---

[56] Deirdre K. Mulligan and Aaron K. Perzanowski, "The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident," *Berkeley Technology Law Journal* 22 (2007): 1157.

whether the representation is "likely to mislead reasonable consumers under the circumstances. The test is whether the consumers' interpretation or reaction is reasonable."[57] The FTC's guidance specifies that communications should be judged upon "the basis of the net general impression conveyed . . . ."[58] The Policy Statement on Deception advances five model questions for evaluating a representation: how clear is the representation, how conspicuous is any qualifying information, how important is the omitted information, do other sources for the omitted information exist, and how familiar is the public with the product or service?[59]

Given consumer expectations, the use of the label "privacy policy" by websites that share information about their users without user permission is deceptive. First, surveys demonstrate that reasonable consumers believe that the mere presence of a privacy policy means that substantive protections are in place to prevent the sharing of their information. Websites' top-level assertions about privacy are often very clear; sites abound with privacy seals and claims that "your privacy is important to us." As such, "privacy" is used as a marketing tool, a type of quality representation that consumers find meaning in and rely upon. Qualifying information, by contrast, is buried within privacy policies in the fine print. As we have shown, this qualifying information is often not understandable and often goes unread by consumers who presume that the policies extend many rights, and thus are not necessary to read.[60] In cases where sites share information without consumer consent, therefore, the use of the term "privacy policy" is deceptive under FTC guidelines.

The Federal Trade Commission should rule, then, that websites using the label "privacy policy" are deceptive unless those sites promise not to share information about their users without their permission. While sites that engage in such sharing without user permission should be required to make disclosures, they should not be allowed to refer to such disclosures as "privacy policies."

---

[57] James C. Miller III, *FTC Policy Statement on Deception* (October 14, 1983). Also available online at http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[58] Ibid.

[59] Ibid.

[60] See Turow, *Americans and Online Privacy*; Turow, Feldman and Meltzer, *Open to Exploitation*.

2. PRIVACY MECHANISMS SHOULD BE VETTED BY USABILITY AND OTHER EXPERTS

Currently, notices are written to satisfy lawyers. The notices do not help consumers make privacy choices that reflect their privacy interests. If the FTC wants consumers to make smart decisions on privacy, then experts in usability and other areas need a seat at the table. Such experts need to help craft privacy-protecting mechanisms. Consumers would benefit from the involvement of experts in usability and psychology in designing notices and other privacy mechanisms. Research at the Samuelson Clinic and elsewhere is beginning to identify the features that can improve the chances that consumers read, comprehend and act upon privacy notices in a manner consistent with their needs and expectations. The FTC needs to avail itself of that research and the expertise behind it.

3. THE FTC SHOULD SET BENCHMARKS FOR SELF-REGULATION

In announcing the 2006 Tech-ade hearings, Chairman Majoras asked:

> [W]hat have we learned over the past decade? How can we apply those lessons to what we do know, and what we cannot know, as we look to the future? And how can we best protect consumers in a marketplace that now knows no bounds, that is virtual, 24-7, and truly global?[61]

The FTC would be better equipped to evaluate what it has learned about self-regulation if it had adopted a reasonable recommendation offered by Privacy Rights Clearinghouse Executive Director Beth Givens in 1996—that the agency set performance benchmarks for self-regulation.[62] Without benchmarks, self-regulation and regulation, for that matter, have no clear metrics for measuring success. Accordingly, we recommend that the FTC define clear benchmarks for its privacy initiatives—educational, regulatory and self-regulatory—and evaluate its approach against those benchmarks between now and 2016.

---

[61] See Majoras, Anti-Spyware Coalition.

[62] FTC, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, n. 156 (Dec. 2006).

V. CONCLUSION

The next decade will bring new technologies that will be able to extract far more information from and about Americans than was previously possible.[63] These technologies will raise new and complex privacy issues. The FTC should plan its activities for the next decade based on a reasoned assessment of its policy initiatives over the last ten years. While some progress has been made, it is clear that consumers remain unable to fully effectuate their privacy rights in the marketplace. Providing consumers with more information about data practices has not led to greater consumer confidence or to a rich marketplace of privacy options for consumers. It is clear that if the FTC continues to pursue a market-based approach, additional interventions are necessary to ensure that consumers are not misled and have straightforward information available that facilitates privacy choices.

---

[63] Turow, *supra* note 1.