November 2006

The FTC and Consumer Privacy in the Coming Decade

Joseph Turow
University of Pennsylvania, jturow@asc.upenn.edu

Chris Jay Hoofnagle
University of California

Deirdre K. Mulligan
University of California

Nathaniel Good
University of California

Jens Grossklags
University of California

Recommended Citation

Turow, J., Hoofnagle, C. J., Mulligan, D. K., Good, N., & Grossklags, J. (2006). The FTC and Consumer Privacy in the Coming Decade. *I/S: A Journal of Law and Policy for the Information Society, 3* (3), 723-749. Retrieved from http://repository.upenn.edu/asc_papers/67

Presented at a Federal Trade Commission Meeting, "Protecting Consumers in the Next Tech-ade."

The FTC and Consumer Privacy in the Coming Decade

Abstract
Large majorities of consumers believe that the term "*privacy policy*" conveys a baseline level of information practices that protect their privacy. In short, "*privacy*," like "*free*" before it, has taken on normative meaning in the marketplace. When consumers see the term "*privacy policy*," they believe that their privacy will be protected in specific ways. In particular, when consumers see the "*privacy policy*" they assume that a web site 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. More frequently, however, privacy policies are used to inform consumers that unless they "opt-out" of certain information sharing, the company will communicate their personal information to other commercial entities.

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 web site in the absence of adherence to these baseline practices can mislead consumers to expect privacy that, in reality, they are not afforded. This is not to suggest that companies are intending 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 marketplace meaning and connotes a particular level of protection to consumers, the Federal Trade Commission should police the use of the term "privacy policy" to assure that companies using the term deliver a set of protections that meet consumers' expectations, and that the term "*privacy policy*" doesn't mislead consumers during marketplace transactions.

Comments
Presented at a Federal Trade Commission Meeting, "Protecting Consumers in the Next Tech-ade."

The FTC and Consumer Privacy

In the Coming Decade

Joseph Turow, Ph.D.
Professor, Annenberg School for Communication
Director, Information & Society Program
Annenberg Public Policy Center
University of Pennsylvania

&

Chris Jay Hoofnagle, JD
Deirdre K. Mulligan, Clinical Professor and Director
Nathaniel Good, Ph.D. Candidate
Jens Grossklags, Ph.D. Candidate

Samuelson Law, Technology and Public Policy Clinic,
U.C. Berkeley Boalt Hall School of Law*

Federal Trade Commission
Tech-ade Workshop
November 8, 2006

* The work of the Samuelson Law, Technology and Public Policy Clinic is generously supported through a generous endowment from Professor Pamela Samuelson and Robert Glushko, PhD. Additional funding is provided by: The Rose Foundation for Communities and the Environment; The Supnick, et al. v. Amazon, Inc. the Alexa Internet Cy Pres Fund, the Household Cy Pres Fund, the Chase Bank Cy Pres Fund, and the National Science Foundation, Team for Research in Ubiquitous Secure Technologies, NSF CCF-0424422.

Major Theme

Large majorities of consumers believe that the term "*privacy policy"* conveys a baseline level of information practices that protect their privacy. In short, "*privacy,*" like "*free*" before it, has taken on normative meaning in the marketplace. When consumers see the term *"privacy policy,"* they believe that their privacy will be protected in specific ways. In particular, when consumers see the *"privacy policy"* they assume that a web site 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. More frequently, however, privacy policies are used to inform consumers that unless they "opt-out" of certain[1] information sharing, the company will communicate their personal information to other commercial entities.

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 web site in the absence of adherence to these baseline practices can mislead consumers to expect privacy that, in reality, they are not afforded. This is not to suggest that companies are intending 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 marketplace meaning and connotes a particular level of protection to consumers, the Federal Trade Commission should police the use of the term "privacy policy" to assure that companies using the term deliver a set of protections that meet consumers' expectations, and that the term *"privacy policy"* doesn't mislead consumers during marketplace transactions.

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

Introduction

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

A core goal of these efforts to date has been to provide information about 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 worked to establish a set of disclosures that responsible companies should provide to consumers in order to facilitate the consumer's 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 web sites? What do consumers think when they see the term "privacy policy?"

This short paper attempts to answer these questions based on existing peer reviewed research and consumer surveys conducted in the academic sector. The paper examines the strengths and limitations of the notice-based approach to facilitating privacy in the consumer marketplace. Based on survey data on consumers' privacy expectations, existing research on whether and in what instances consumers read and comprehend notices, the role information asymmetry and well know psychological barriers to information processing and risk assessment by individuals play in privacy decision-making, and insights from the field of human computer interaction about interface design and information presentation, this paper 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:

- in the absence of a baseline set of information practices the use of the term "privacy policy" creates consumer confusion;

- the lack of common language for disclosures undermines that ability of consumers to "shop for privacy" and therefore undermines the ability of businesses to compete on privacy;
- short notices are a promising step toward lowering the barriers to a successful marketplace for privacy for the consumers who read notices;
- privacy must be "usable" if it is to serve consumer needs and therefore including experts from fields such as human computer interaction and psychology is imperative; and finally,
- if consumers are not able to make informed choices about the privacy and security aspects of their computers it makes it easy, and in fact inevitable, that bad actors will take advantage of this to undermine consumer privacy and the security of the network infrastructure by turning consumers' machines against them and us.

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

Requiring businesses that use the term privacy policy to provide some baseline privacy protections that meet established consumer expectations;

Developing a set of required disclosures and terms to facilitate comparison shopping for privacy and to facilitate competition among firms for privacy practices;

Pushing for short notices to limit the transaction costs associated with reading long, indecipherable end user license agreements (EULAs); and,

Including information from other disciplines, including usability and human computer interaction, in the design of future initiatives aimed at usable privacy and security.

These refinements and initiatives will ensure that Tech-ade 2016 will see progress on privacy protection. It is crucial that we evaluate the effect of the FTC's initiatives, assess and rechart the course, and establish benchmarks for evaluating consumer privacy in the marketplace for the next Tech-ade.

The FTC's Approach to Consumer Privacy

Just over ten years ago, the FTC conducted its last forward-looking proceeding analyzing the future of consumer protection in a high tech economy. In a report from that proceeding, FTC staff 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."

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.[3] 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 (FIPS)—notice, choice, access and security—as the framework for self-regulatory and regulatory initiatives. The Commission's approach omitted several important data protection principles including the concepts of "data minimization," requiring companies to minimize the amount of personal information collected to that which is necessary for a transaction, and "purpose specification," requiring 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 repurpose information without consumer consent. After adopting its limited set of FIPS, the FTC highlighted the

---

[2] Federal Trade Comission, *Anticipating The 21st Century: Consumer Protection Policy In The New High-Tech, Global Marketplace* 46 (May 1996).

[3] Marcia Hofmann, *Federal Trade Commission Enforcement, in* PROSKAUER ON PRIVACY (Practicing Law Institute, forthcoming 2006).

importance of notice/awareness 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 conditions collection of information from children under 13 years old upon first obtaining parental consent. 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 and the Privacy Act of 1974, that embraced a full set of "Fair Information Practices" (FIPs) to protect personal information. Rearticulated in the Organization for Economic Cooperation and Development Guidelines (OECD), which were endorsed by all 30 OECD nations, including the United States.

OECD FIPs versus FTC Principles

OECD	FTC
• Collection Limitation	
• Data Quality	
• Purpose Specification	
• **Use Limitation**	>>Choice/Consent
• **Security Safeguards**	>>Integrity/Security
• **Openness**	>>Notice/Awareness
• **Individual Participation**	>>Access/Participation
• **Accountability**	**>>** Enforcement/Redress

Most ecommerce 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 develop new technologies. Finally, we need to educate consumers so that they can take steps to protect themselves.[4]

At this important juncture, it makes sense to evaluate its strengths and weaknesses. Before the FTC decides what approaches to pursue during the next decade, we suggest that they

[4] Deborah Platt Majoras, Address at the Anti-Spyware Coalition (Feb. 9, 2006), available at http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf.

critically reflect on research that explores the effectiveness of the FTC's approach during the last decade.

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 end user license agreements 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 FTC has pursued self-regulatory solutions to consumer privacy, large majorities of consumers believe incorrectly that laws protect their personal information from secondary use.

Research Demonstrates the Limits of the Disclosure-Based Approach

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. A 2003 Annenberg survey found that 70% of respondents agreed or agreed strongly with the statement that, "I am nervous about websites having information about me."[5] In 2005, the same response was reported by 79% of respondents. Individuals also believe that they are put at risk as a result of information collection. Only 17% agreed with the proposition that "What companies know about me won't hurt me."

[5] 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, carried out from January 30 to March 21, 2003, ICR interviewed by phone a nationally representative sample of 1,200 adults who were using the internet at home. For the 2005 survey, carried out from February 8 to March 14, 2005, ICR interviewed by phone a nationally representative sample of 1,200 adults who said they used the internet in the past month. See, Joseph Turow, *Americans and Online Privacy* (Philadelphia: Annenberg Public Policy Center, 2003) and Joseph Turow, Lauren Feldman and Kimberly Meltzer, *Open to Exploitation*, (Philadelphia: Annenberg Public Policy Center, 2005). Both reports can be found at http://www.appcpenn.org.

A high level of concern is also reported concerning both commercial and government collection of personal information. In 2003, 92% reported concern that marketers were "collecting information about your household members' activities without your knowledge or consent." Similarly 83% were concerned that the government was "collecting information about your household members' activities without your knowledge or consent." Respondents also believe that they should be in control of marketing communications. For instance, 94% reported that web sites should ask for permission before sending ads.

Consumers fundamentally misunderstand the "privacy policy" label

Supporters of privacy self-regulation suggest that Americans' high levels of concern can be alleviated when they begin to examine their options for releasing personal data. Professor Alan Westin, for example, has written that most Americans take an informed cost-benefit tack in relation to their information online and offline. "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."[6] This description of most Americans as aware of their online privacy options supported the line by internet industry players that an accurate privacy policy on every site would create a world of optimal consumer privacy as each individual shopped with their mouse for privacy that matched their personal needs.

Unfortunately that doesn't appear to be happening. One could assume from this that consumers don't 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 being by assuring the consumer that the site cares about his or her privacy, but then in the following paragraphs (often pages) proceed, in technical language, to inform consumers about "affiliate" sharing, required disclosures, distinctions between personally identifiable information (pii) and aggregate data, noting that the policy doesn't control other sites or content

[6] Alan F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59:2 (20003) 431-453.

that may be included or accessed from the site, and finally caution that the privacy policy can change at any time (sometimes telling consumers that the site will inform them when that happens).

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 they will share it with affiliates and outside firms, and how. Most Americans believe, logically, that the phrase *privacy policy* signifies that *their information will be kept private*. For 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." 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.

Consumers misunderstand online data collection

But 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 don't register, however they do not understand that data flows behind their screens invisibly connect seemingly unrelated bits about them. The survey's interviewers asked respondents to name a site they valued and then went on to ask their reaction to what is actually a common scenario of the way sites track, extract and share information to make money from advertising. 85% of the surveyed adults who go online at home stated that they did not agree to accept the use of their data, collected and aggregated across visits to multiple sites, for click stream advertising—even by a "valued" site. When offered a choice to get content from a valued site with such a policy or pay for the site and not have it collect information, 54% of adults who go online at home said that they would rather find the information offline than exercise either option presented.

Among the 85% who did not accept the practice, one in two (52%) had earlier said they gave or would likely give the valued site their real name and email address. 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 given up these data had also agreed that the mere presence of a web site privacy policy means that it won't share data with other firms. Bringing these two results together suggests that at least one of every three of the 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.

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 over consumer information in the marketplace. Table 1 lists true-or-false statements that the 2005 Annenberg survey presented to its representative national sample. The answers indicate a low level of understanding of consumer rights and redress in the marketplace. High proportions of consumers believe they have certain privacy rights—notably consistent with those provided under FIPS—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 (N=1,500)*

	%T	%F	DK
Most online merchants give me the opportunity to see the information they gather about me. *47% didn't know the right answer*	23	**53**	25
Most online merchants allow me the opportunity to erase information they have gathered about me *50% didn't 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% didn't 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% didn't know the right answer*	**38**	29	33
Correctly knows the name of a credit reporting agency *66% didn't 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% didn't know the right answer*	37	**32**	31
It is legal for an **offline** store to charge different people different prices at the same time of day. *71% didn't know the right answer*	**29**	42	29

Bold numbers indicate the correct answer. Sums greater than 100% result from rounding error. DK=Don't Know

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"),[7] researchers at U.C. Berkeley's Samuelson Clinic have examined the utility of short notices and variations on notice timing in communicating about privacy and security (among other) consequences of software installation.[8] The installation of downloadable software almost always involves the provision and "click"-through to privacy notices and end user license agreements (EULA). Notices are usually presented in a separate screen during installation and, 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 and privacy, as well as 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 end user license agreements suggest that they are largely ineffective means to communicate with consumers. EULAs, terms-of-service agreements (ToS), and some privacy policies present complex legal information. Research shows that complexity of notices hampers users' ability to understand such agreements. For example, Jensen and Potts

---

[7] 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, the 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.

[8] See, for example, Nathan Good, Rachna Dhamija, Jens Grossklags, Steven Aronovitz, David Thaw, Deirdre Mulligan and Joseph Konstan (2005) "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware," *in Proceedings Of The Symposium On Usable Privacy And Security*. *Also, see*: Nathan Good, Jens Grossklags, Deirdre Mulligan and Joe Konstan (2006) *Noticing Notice: A large-scale experiment on the timing of software license agreements* (working paper available from authors of this report).

studied a sample of 64 privacy policies from high traffic and health care web sites.[9] They found that the formats of policies, their location on the web site and their legal content severely limit users' ability to make informed decisions based on them. Additionally, Masson and Waldron showed that simplifying legal contracts (for example, by using easier words and replacing obscure terms with common versions) could not achieve very high degrees of comprehension. This is because "non-experts have difficulty understanding complex legal concepts that sometimes conflict with prior knowledge and beliefs."[10]

Vila et al. raise the question of whether users will ever bother to read or believe privacy policies at all.[11] They claim that because the cost of lying 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 them or pay attention to them at all. Actually, 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 that "I look to see if a website has a privacy policy before answering any questions." Anecdotal evidence does, however, support the impression that people don't read the policies. One software provider included a $1000 cash prize offer in the EULA that was displayed during each software installation. It took four months and 3,000 downloads of the software for someone to notice the clause and claim the prize.

Among 222 study participants, the Samuelson Clinic found that only 1.4% reported reading EULAs often and thoroughly when they encounter them. 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.

Short and layered notices have been 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 programs activities, this is termed "regret."

---

[9] Jensen, C., and C. Potts, *Privacy policies as decision-making tools: An evaluation on online privacy notices*, *in CHI 2004 Connect: Conference Proceedings*: April 24-29, 2004.

[10] Masson, M. E. J., & Waldron, M. A., *Comprehension of legal contracts by non-experts: Effectiveness of plain language redrafting,* Applied Cognitive Psychology, 8, 67-85 (1994).

[11] Vila, T., Greenstadt, R., and Molnar, D., *Why we can't be bothered reading privacy policies - models of privacy economics as a lemons market, in* Proceedings of the Fifth International Conference Electronic Commerce, pp. 403-407 (2005).

Subjects were shown the program EULA or the EULA and a short notice high lighting core aspects of performance, privacy and security, when downloading and installing programs. 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 had received the short notices during the study were less likely to fewer reverse their earlier decision to install software. However, overall, many users after reading the short notice during the exit interview expressed regret about their installation decisions across all treatments (EULA, and EULA plus short notice).

Overall regret was high. Importantly, however, regret was lower in the case of the short notices.

Other forces also prevent consumers from successful privacy protection

Beyond the issues of whether consumers read and comprehend privacy policies, individuals' ability to make market-place 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 may seem unpredictable, even random. Sometimes risks only become known 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 (2005) report, for example, that 73% of respondents in their survey underestimated the risk of becoming a victim of identity theft.[12]

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

[12] Acquisti, A., and Grossklags, J., *Privacy and Rationality in Individual Decision Making*, IEEE Security & Privacy, 3(1): 26-33 (2005).

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.

Even if individuals have access to complete information about their privacy risks and modes of protection, they might not be able to process vast amounts of 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, ecommerce, and evolving business practices.

Consumers are limited in their attempts to protect their information

Evidence abounds that consumers 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.[13] Fully 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. 65% had declined to register at an e-commerce site because of privacy concerns. Among individuals described as the "privacy unconcerned" 47% reported that they took 4 of 7 identified privacy-protecting behaviors, while 65% of "privacy pragmatists" had taken these actions.

These results are echoed by a small-scale survey of 222 people who participated in experimental research of Acquisti and Grossklags.[14] They found that at least 75 percent 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. However, they also found that usage of specific technologies was consistently low across the sample population. For example, 67% never encrypted their emails, 82% never put a credit alert on their credit report, and 82% never removed their phone numbers from public directories.

---

[13] Privacy & American Business, *New National Survey On Consumer Privacy Attitudes To Be Released At Privacy & American Business Landmark Conference,* (June 10, 2004), available at http://Www.Marketwire.Com/Mw/Release_Html_B1?Release_Id=68484.

[14] Acquisti, A., and Grossklags, J., *Privacy and Rationality in Individual Decision Making*, *IEEE Security & Privacy*, 3(1): 26-33 (2005).

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 67% do not know the name of a credit agency and 76% do not correctly respond "false" to the statement that "The Federal Trade Commission will correct errors in credit reports if it is shown proof of the errors." Rather than laziness, these findings suggest that while people would like to protect their privacy, and do at the most basic levels, large proportions do not have the knowledge that will allow them to move beyond the very basics of privacy-protective behavior.

In the online environment, the complexity of privacy-protection activities increases, and so the likelihood that Americans carry them out decreases substantially. The 2003 Annenberg survey asked American adults who use the internet at home if they carried out certain activities in relation to controlling their information online. Fully 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 don't register. The percentage applied other privacy tools drops steeply from there, 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."

To gauge how experienced individuals are with the range of these practices, we gave them scores based on the number they reported performed. Four points went to people who said they have carried out all of these activities, three to those who have done three of them, and so on. We found that fully 25% had not carried out any of these information-controlling activities (we called them *highly inexperienced*). 31% had carried out one task (*inexperienced*). 25% were in the middle with two of the four (*neither experienced nor inexperienced*), only 11% fell into the *experienced* slot, and an even smaller 8% claimed to be *highly experienced*—having at least some skill at carrying out four of the four information-controlling activities.

For those who want to encourage more citizens to control their information online, an obvious path is to cultivate internet users who are experienced with privacy-protecting technologies. At present only 19% of adults who go online from home fall into either the *highly experienced* or *experienced* categories. The rest—from *neither experienced nor inexperienced*

through *highly inexperienced*—are both much less knowledgeable and much less active about controlling their online data.

Unfortunately, we could not find out what characteristics or activities foretell whether or not a person will be more or less experienced in this regard. We used a statistical technique called optimal scaling regression. It helped us explore whether a variety of background characteristics that we expected would encourage concern with online privacy would, in fact, predict a higher score on privacy-tool experience. In addition to demographic characteristics such as age, income, race, education, and gender, and region of the country, we were interested in whether having a child aged six to seventeen who uses the internet leads someone to learn more privacy tools. We also thought that incidence of internet use and self-reported ability to navigate the web might pay important roles in leading a person to be privacy-tool experienced.[15] It turned out that among all the variables, only the time spent online (specifically, weekly versus daily and spending more than one hour on the internet) could be seen to impact involvement with privacy tools. Our statistical technique indicated, however, that even these variables predicted only 7% of the factors that drive experience with them. Overall, our model accounted for just 11% of the variance and so explains little about why certain individuals learn a number of ways to control their information online and others do not.

What the FTC Must Confront in the Next Decade

Americans' continuing concerns and confusions about information privacy

Research indicates that American consumers care deeply about information privacy and worry that its 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 market place transactions. Most fundamentally, research indicates that a large majority of American adults believe that a

[15] In our model, *incidence of internet use* involved three variables—years on the internet (prior to 1997 to present—2003), use/non-use of the internet at home during the past month, daily vs. weekly use of the internet, and spending minutes vs. hours online. Linear relationships were tests for age and income. Curvilinear relationship was also tested for age.

"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 two years apart (in 2003 and 2005) revealed virtually the same percentage of Americans—almost 60%--believing that "when a website has a privacy policy, that means it will not share information about them with other websites or companies." In the 2005 survey, where the statement was presented in true/false form, 59% incorrectly said the statement was true and an additional 16% said they didn't know if it were true or false.

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. It also 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—full and understandable—information about data practices that affect their privacy. More significantly, even if full and understandable information is provided in a short format, consumers will 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, will limit the number of consumers who read and act on such privacy notices. If a website carries a privacy policy which states that it will reveal users' data to affiliates or other companies without the users' permission, consumers privacy is undermined.

The current notice-based approach has consequences for the security of the network itself.

Consumers' basic misunderstanding of the purpose of privacy policies is the leading edge of an iceberg of confusions that we have described. 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 with negative affects on 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. In doing so, they will lower the security protections of the entire network, not just their own computers.

A case in point is the recent wide-scale installation of a "rootkit" by purchasers of music CDs. In attempting to protect the 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 open millions of computers to control by others. This allows bad actors to create "botnets," zombie networks of consumers' computers, which can be remotely directed to engage in denial of service attacks and other malicious acts.

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. And yet while many websites begin their privacy policies with statements that "your privacy is important to us," very many of them disclose further down that they collect quite a bit of the information from their sites' users and often do share them with affiliates or marketers or other entities. Note, too, that information-sharing agreements with third parties generally need not by law 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 actual policy may or may not state what is happening to their information.

Given consumers expectations, the use of the term privacy policy absent some baseline privacy protections ought to be considered deceptive. The Commission evaluates deceptive marketing communications to consumers based upon whether the representation is "likely to mislead reasonable consumers under the circumstances. The test is whether the consumer's interpretation or reaction is reasonable."[16] The FTC's guidance specifies that communications should be judged upon "the basis of the net general impression conveyed…" The Policy Statement on Deception advances four model questions for evaluating a representation: How

[16] FTC, Policy Statement on Deception (Oct. 14, 1983).

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?

Given consumer expectations, the use of the label *privacy policy* by web sites that share information about their users without user permission is deceptive. First, surveys demonstrate that reasonable consumers believe that the mere presence of privacy policies mean that substantive protections are in place to prevent the sharing of their information. Web sites 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, it 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 Used in cases where sites share information without consumer consent, therefore, 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.”

2. Privacy mechanisms should be vetted by usability and other experts.

Currently, notices are written to satisfy lawyers, leaving consumers behind. 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, usability and other experts need a seat at the table. Such experts need to have a hand in crafting privacy-protecting mechanisms. Consumers would benefit from having experts in usability and psychology at the table when notices and other privacy mechanisms are designed. Research at the Samuelson Clinic and elsewhere is beginning to untangle 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 Techade hearings, Chairman Majoras asked:

> "What 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?"[17]

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.[18] Without benchmarks, self-regulation, and regulation for that matter, has no clear metric for assessing 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.

The next decade will bring new technologies that will be able to extract far more information from and about Americans than was previously possible.[19] These technologies will raise new and complex privacy issues. The FTC should base its activities during the next decade 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 in the marketplace. Providing consumers with more information about data practices has not led to greater consumer confidence or a rich market place 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 straight forward information available that facilitates privacy choices.

---

[17] Deborah Platt Majoras, Address at the Anti-Spyware Coalition (Feb. 9, 2006), available at http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf.

[18] FTC, Public Workshop on Consumer Privacy on the Global Information Infrastructure Fn. 156 (Dec. 2006).

[19] See, for example, Joseph Turow, *Niche Envy: Marketing Discrimination in the Digital Age*. Cambridge, MA: MIT Press, 2006.