



# PRIVACY & SECURITY LAW



## REPORT

Reproduced with permission from Privacy & Security Law Report, 9PVLR42, 10/25/2010. Copyright © 2010 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### **Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States**



BY CHRISTOPHER WOLF

*Christopher Wolf, Practice Leader, Hogan Lovells Privacy and Information Management Practice and Founder/Co-Chair of the Future of Privacy Forum (FPF). Special thanks to Bret Cohen, an attorney in the Privacy and Information Management Practice at Hogan Lovells for his assistance in the preparation of this article.*

*This article is adapted from a paper prepared for presentation at the 32d Annual International Conference of Privacy and Data Protection Commissioners in Jerusalem, Israel Oct. 27 and 28, 2010.*

**M**odern democracies are committed to the protection of personal data. There are various approaches to achieving protection, ranging from the comprehensive regulatory approach of the European Union, to the harms-based Asia-Pacific Economic Cooperation (APEC) framework, to the sectoral and geographic approach of the United States, which relies heavily on Federal Trade Commission (FTC) enforcement against unfair or deceptive consumer practices and the combination of federal and state laws. The U.S. framework frequently is criticized for the absence of a comprehensive privacy law. Indeed that perceived deficiency has resulted in a persistent finding by the European Union that the United States lacks “adequate protection” for personal data, requiring legal workarounds for the cross-border transfer of personal data from the European Union to the United States. At the same time, there is global recognition of a need to re-examine privacy governance to cope with the implications of new technologies, and to protect generations of technology users.

Without debating the primacy of one approach to the protection of privacy over another, it nevertheless is useful to look beyond labels and common perceptions to examine the effective aspects of the U.S. regime. This paper discusses the effectiveness of enforcement by the FTC under its jurisdiction to police unfair and deceptive practices,<sup>1</sup> and the experience in individual states as incubators of new privacy and data security laws that have nationwide effects. It also highlights privacy-enhancing practices and technologies adopted by businesses aware of the advantages of self-regulation over

prescriptive rules and the need to self-regulate and innovate to avoid restrictive regulation.

As documented in research by Professors Kenneth Bamberger and Deirdre Mulligan of the University of California at Berkeley, *Privacy on the Books and on the Ground*,<sup>2</sup> despite the gaps in statutory privacy law coverage, privacy law as enforced in the United States by the FTC has been successful in establishing rules of conduct for businesses handling personal data and in preventing violations of individual privacy.<sup>3</sup> Indeed, as FTC enforcement has evolved and has resulted in highly publicized consent decrees, the FTC has been increasingly specific about what privacy and data security practices are required to protect personal data, in effect setting clear baseline privacy protections.<sup>4</sup> This has created a “common law of consent decrees,” producing a set of data protection rules for businesses to follow.

The authors of the *Privacy on the Books and on the Ground* study also found that the possibility (or threat) of enforcement has prompted businesses to develop privacy-enhancing technologies and business practices. Thus, discretionary enforcement by the federal regulator has served as a powerful impetus for the enhancement of privacy protections in the United States.

## I. The American Approach

Jurisdiction to prescribe and enforce privacy rules in the United States is shared by the federal and state governments. At the federal level, privacy laws have arisen in response to the increasing use of technology to collect, use, share, and retain personal information, with emphasis where there is the greatest potential for harm from misuse. For this reason, Congress has legislated extensively to protect financial and health information, and information collected from children. Federal law also empowers the independent FTC to enforce violations of the broad statutory proscription against “unfair” or “deceptive” acts or practices. That power has been used to bring enforcement actions against companies that fail to provide privacy protections promised in privacy policies and that fail to utilize reasonable data security practices in a manner deemed to be “unfair” to consumers because of the demonstrable harm caused.

<sup>1</sup> 45 U.S.C. § 5 (Section 5 of the FTC Act) (unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are unlawful).

<sup>2</sup> See Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. (forthcoming Jan. 2011), available at <http://ssrn.com/abstract=1568385> (draft of June 29, 2010). For a digest of the article, see [http://futureofprivacy.org/wp-content/uploads/2010/09/Privacy%20Papers%20for%20Policy%20Makers\\_FULL%20BK.pdf](http://futureofprivacy.org/wp-content/uploads/2010/09/Privacy%20Papers%20for%20Policy%20Makers_FULL%20BK.pdf) (Bamberger/Mulligan paper was selected as a leading “Privacy Paper for Policy Makers” in a project of the Future of Privacy Forum).

<sup>3</sup> The authors also warn that overly prescriptive or regulated privacy laws can reduce government flexibility in privacy enforcement, which can produce adverse unintended consequences.

<sup>4</sup> A variety of pending legislative measures would give the FTC rulemaking authority over privacy policies, data breaches, data security, and related matters. Proponents urge that specific rules would provide greater certainty and predictability than the agency’s enforcement actions that arise under its authority to prevent “unfairness” and “deception.” However, the rulemaking process also has the potential to delay the setting of standards and to result in compromises that produce less stringent rules than those coming from enforcement actions.

At the state level, legislatures have become the proving grounds for new statutory approaches to privacy regulation. Some of these developments include the enactment of data security breach notification laws (which not only serve to inform consumers of incidents that threaten them with identify theft but also act as a “negative incentive” to companies to improve their data security lest they be required to report data breaches) as well as highly detailed data security laws, enacted largely in response to data breaches. This partnership has resulted in a set of robust standards for the protection of personal data. Even in jurisdictions with broad proscriptions against the misuse of personal information, the specific standards emanating from the United States may serve to inform and augment privacy protections. Today, for example, we see the concept of data security breach notification laws being borrowed in the European Union in proposals for augmentation of the EU Data Protection Directive.<sup>5</sup>

## A. FTC Privacy Regulation

The primary enforcer of consumer privacy regulations in the United States is the FTC. The FTC, however, does not have a specific mandate to create and enforce general privacy regulations. Instead, its principal authority comes from Section 5 of the FTC Act, which prohibits businesses from engaging in “unfair or deceptive acts or practices in or affecting commerce.”<sup>6</sup>

The FTC has never litigated a privacy case. Instead, all businesses that the FTC has pursued and has found responsible for privacy violations have entered into settlements (called “consent decrees”) in which they do not formally admit fault but promise to cease engaging in the practice at issue and agree to periodic audits to ensure they have corrected the privacy violation and that they have implemented a comprehensive information security program. These consent decrees then serve as notice to other companies to conform their privacy practices to the standards announced in the decree or risk being the next target of an FTC investigation.

The FTC’s use of this authority started with some of the most clear-cut privacy violations. In these cases, the FTC, under its authority to regulate “deceptive” trade practices, investigated businesses that made false claims about the privacy protections applied to the consumer information they collected. For example, in one of its first online privacy investigations, the FTC en-

<sup>5</sup> See STEWART DRESNER & AMY NORCUP, *DATA BREACH NOTIFICATION LAWS IN EUROPE* (2009), available at [http://privacylaws.com/Documents/data\\_breach\\_conference.pdf](http://privacylaws.com/Documents/data_breach_conference.pdf).

<sup>6</sup> 15 U.S.C. § 45(a). In addition to the FTC Act, privacy at the federal level is governed by a number of sector-specific statutes, such as the Gramm-Leach-Bliley Act (GLBA), which covers the privacy of financial information, and the Health Insurance Portability and Accountability Act (HIPAA), which covers the privacy of medical information. Some portions of these statutes are enforced by the FTC, and some by other federal government agencies. Though many agencies have jurisdiction over similar aspects of privacy for varying industry sectors, they regularly communicate and their standards for privacy and data security do not vary greatly where left to the discretion of the agencies and not prescribed by statute. The FTC is the leading agency in developing and implementing these standards, and in many instances the other agencies rely on how the FTC regulates and enforces privacy under the FTC Act, so this paper focuses on a discussion of the FTC’s enforcement of privacy as a proxy for federal privacy enforcement in the United States.

tered into a consent decree with a web host, Geocities, that had promised users that it would not sell or share their information without prior consent, but in fact sold users' personal information.<sup>7</sup> In another case, the FTC investigated pharmaceutical manufacturer Eli Lilly when the company accidentally addressed an e-mail message to all 669 registered users of its website who had signed up for prescription refill reminders for the anti-depressant Prozac to inform them that the reminder service was being suspended. That lapse meant that every Prozac-using registrant knew who the other Prozac-using registrants were. Eli Lilly had a policy promising that it would apply safeguards to ensure that user information would not be disclosed to others.<sup>8</sup>

The terms of the consent decrees with both Geocities and Eli Lilly required them to discontinue the practices in question and to provide consumers with proper disclosures, and imposed other organizational requirements such as employee training, designation of employees responsible for privacy practices, and the institution of information privacy and security programs.

In a 2002 enforcement action, Microsoft agreed to settle FTC charges regarding the privacy and security of personal information collected from consumers through its "Passport" web services.<sup>9</sup> In that case, the FTC found a false representation in a privacy policy regarding security protections Microsoft promised it would apply to personal data. In addition to requiring only truthful representations in privacy policies going forward, the FTC required specific data security protections be implemented as a remedy for the false representations.<sup>10</sup> The Commission initiated its investigation of the Passport services following a July 2001 complaint from a coalition of consumer groups led by the Electronic Privacy Information Center (EPIC), which—along with other nongovernmental organizations (NGOs) in the United States—frequently reports privacy and data security issues to the FTC. Privacy-concerned NGOs continue to play an important role in privacy enforcement in the United States by bringing issues to the attention of regulators.

Since these early cases, the FTC has brought enforcement actions against companies for a much more expansive variety of conduct.<sup>11</sup> The advent of state data security breach notification laws and the corresponding

publicity surrounding announced breaches have provided the FTC with targets for investigation of data security practices. The FTC does not just investigate the circumstances surrounding a breach for which notification has been provided, but also examines the target company's entire data protection process, looking at the physical, administrative and technical safeguards the company utilizes, as well as compliance with public promises about the handling of personal data. If an investigation uncovers deficiencies, the failure to implement industry-standard data security measures is deemed to be an "unfair" trade practice in violation of Section 5 of the FTC Act. Consequently, the lax data security practices that led to the breaches at issue—such as the failure to encrypt credit card transactions transferred over public networks, the failure to use anti-virus software, and the failure to properly dispose of customer records containing sensitive personal information—have become de facto requirements of the FTC Act.

Over its past few enforcement actions, the standards employed by the FTC have become increasingly granular. For instance, in one investigation the FTC singled out a company's failure to monitor and filter outbound traffic to identify and block the export of sensitive personal information without authorization.<sup>12</sup> In another, the FTC took a more restrictive view of what constitutes sufficient notice to collect personal information, obtaining a consent decree from a company that informed consumers participating in a promotion that it would download tracking software onto their computers, but buried the details of the tracking in a notice deep within a lengthy terms of service agreement that showed up only at the end of a protracted registration process.<sup>13</sup>

The net effect of these privacy enforcement actions has been to create a "common law" of consent decrees that dictates what privacy violations, including data security lapses, constitute a violation of the FTC Act. But this approach to privacy regulation has not just served to define the scope of privacy protections in the United States. With new privacy standards added to this common law with every enforcement action, it is not enough for companies to merely comply with existing enforcement actions. When considering policies and business practices relating to data security, companies must now consider which of those policies and practices the FTC will deem to be a violation of the FTC Act.

As Bamberger and Mulligan put it, the "definitional ambiguity" inherent in the FTC Act has "required companies to embrace a dynamic, forward-looking outlook toward privacy."<sup>14</sup> The FTC has embraced this ambiguity, and the power it carries. That has resulted in greater vigilance on the part of businesses in the United States with respect to the privacy and data security of personal information.

<sup>7</sup> *FTC v. ReverseAuction.com, Inc.*, FTC File No. 002-3046 (2000), available at <http://ftc.gov/os/2000/01/reverseconsent.htm>.

<sup>8</sup> *Eli Lilly & Co.*, FTC File No. 012-3214 (2002), available at <http://ftc.gov/os/2002/05/elilillydo.htm>.

<sup>9</sup> *Microsoft Corp.*, FTC File No. 012-3240 (2002), available at <http://ftc.gov/opa/2002/08/microsoft.shtm>.

<sup>10</sup> Microsoft's Passport privacy policies included statements such as, "Passport achieves a high level of Web Security by using technologies and systems designed to prevent unauthorized access to your personal information" and "Your Passport is protected by powerful online security and a strict privacy policy." The FTC found those representations were not accurate because of security holes in the Passport product.

<sup>11</sup> For example, these enforcement actions have established the requirements for businesses to secure wireless networks used for the transmission of personal data, to use encryption, and to implement other physical, administrative and technical safeguards such as the proper credentialing of data recipients and using prudence in the disposal of personal information. See [http://ftc.gov/privacy/privacyinitiatives/promises\\_enf.html](http://ftc.gov/privacy/privacyinitiatives/promises_enf.html) for a listing of FTC enforcement actions with respect to privacy and data security.

<sup>12</sup> *Dave & Buster's, Inc.*, FTC File No. 082-3153 (2010), available at <http://ftc.gov/opa/2010/03/davebusters.shtm>; see also <http://hldataprotection.com/2010/03/articles/data-security-breaches-include/ftc-consent-decree-requires-monitoring-and-filtering-of-outbound-computer-traffic-to-block-export-of-sensitive-information>.

<sup>13</sup> *Sears Holdings Mgmt. Corp.*, FTC File No. 082-3099 (2009), available at <http://ftc.gov/opa/2009/06/sears.shtm>.

<sup>14</sup> Bamberger & Mulligan, *supra* note 3, at 21.

Thus, the FTC's enforcement powers do not even have to be exercised in order to be effective. As a further illustration of the effect of an *announced* threat of enforcement, earlier this year FTC issued warning letters to 100 organizations that personal information, including sensitive data about customers and employees, was vulnerable on peer-to-peer (P2P) file-sharing networks due to P2P software downloaded to those organizations' computers.<sup>15</sup> The clear implication was that despite the absence of formal rules, the FTC would regard a breach of data over a P2P network to be an unfair data security practice and a violation of the FTC Act, and that the organizations receiving the letter (and even those that did not) risked inaction at their own peril.

This ambiguity and uncertainty about the scope of the regulatory landscape is a significant component driving corporate adoption of privacy practices in the United States today. By not knowing which data security standard the FTC will next incorporate into the FTC Act, businesses wishing to remain in compliance are spurred to proactively assess their corporate privacy protections against industry-standard data security standards.

Moreover, and quite possibly the most positive development of this style of FTC regulation, more and more U.S. businesses are incorporating "Privacy by Design"<sup>16</sup> in the adoption of new information systems and applications, ensuring that privacy and data security concerns are considered at every step of the design and development processes. The effect has been the incorporation of more robust privacy protections into the information systems and applications of companies subject to the FTC Act.

The leverage the FTC gains from the ability to bring privacy enforcement actions allows it to use other regulatory tools outside of the enforcement context to encourage businesses to adopt stronger privacy controls. For example, the FTC has framed the debate over online behavioral advertising—a process by which businesses track consumers' web browsing habits to deliver them online advertisements tailored to the consumers' interests—cautioning that it will issue formal regulations or pursue enforcement actions if industry self-regulatory efforts do not meet certain principles published by the agency.<sup>17</sup> The FTC has also used its status as lead privacy regulator in the United States to convene three "Privacy Roundtables" over the past year, during which privacy stakeholders—including regulators, privacy advocates, and businesses—met to discuss how best to protect consumer privacy while supporting beneficial uses of the information and technological in-

novation.<sup>18</sup> The FTC is expected to release a report detailing its findings from the Roundtables later this year.

The effect of these non-enforcement activities on bottom-line consumer privacy in the United States cannot be understated. Bamberger and Mulligan identify three types of regulatory goals furthered by these activities.<sup>19</sup> First, the publicity generated by the FTC has helped to increase the transparency of corporate privacy practices. As a result, businesses face greater scrutiny from privacy advocates and the media to implement and maintain consumer-friendly privacy practices.<sup>20</sup> Second, as described above, the FTC has used the threat of looming enforcement actions to motivate industry to act preemptively without being subject to regulation. In addition to using this power to influence industry self-regulation for online behavioral advertising, as described above, the FTC has played a major role in encouraging the adoption of privacy policies among many other pro-privacy developments. Third, the FTC's encouragement of dialogue on privacy issues has empowered privacy-focused NGOs—such as the Future of Privacy Forum—to be meaningful participants in the advancement of privacy.

## B. State Privacy Regulation

Though nationwide privacy regulation in the United States necessarily emanates from the federal government, state governments play an important role, and have greatly influenced corporate privacy practices. Indeed, while federal law has a nationwide reach, so too do some state laws. That is because the laws protect the residents of the states, no matter where their data is stored. Thus, if the personal data of a California resident is stored in a New York computer, the New York entity is subject to the requirements of California privacy law.

The primary means by which data protection has occurred through state legislation is through security breach notification (SBN) laws. Under the laws of forty-six states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, entities maintaining certain types of personally identifiable information of residents of those jurisdictions are required to report any breach to affected individuals. Once reported, these breaches are often further publicized by the media and privacy advocates, leading to reputational harm. For instance, the Privacy Rights Clearinghouse maintains an online list of data breaches that have occurred since 2005, most identified due to the reporting requirement under SBN laws.<sup>21</sup> Companies not only face reputational harm from the publication of these breaches, but financial damages as well. The publication of breaches frequently leads to consumer class-action lawsuits under a theory that organizations owe a duty to secure the data they maintain, and which require resources to defend, whether successful or not. According to a recent study, the average cost of a data breach in 2009 was \$204 per compromised customer record, and \$6.75 million per

<sup>15</sup> See Widespread Data Breaches Uncovered by FTC Probe: FTC Warns of Improper Release of Sensitive Consumer Data on P2P File-Sharing Networks (Feb. 22, 2010), <http://ftc.gov/opa/2010/02/p2palert.shtm>.

<sup>16</sup> Privacy by Design is a concept that was developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, that advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks. Rather, privacy assurance must ideally become an organization's default mode of operation. For more about Privacy by Design, see <http://privacybydesign.ca>.

<sup>17</sup> See FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), available at <http://ftc.gov/os/2009/02/P085400behavadreport.pdf>.

<sup>18</sup> See FTC, Exploring Privacy: A Roundtable Series, <http://ftc.gov/bcp/workshops/privacyroundtables>.

<sup>19</sup> See Bamberger & Mulligan, *supra* note 3, at 35-37.

<sup>20</sup> See, for example, the Wall Street Journal's recent series on online privacy, "What They Know," <http://wsj.com/wtk>.

<sup>21</sup> Privacy Rights Clearinghouse, Chronology of Data Breaches, available at <http://privacyrights.org/ar/ChronDataBreaches.htm>.

incident.<sup>22</sup> Due to these reputational and financial costs of a reported breach, Bamberger and Mulligan identify state SBN laws as one of the major drivers of the investment in data security measures in the United States.<sup>23</sup>

In addition to SBN laws, states have “mini-FTC Acts” under which they have authority similar to that of the FTC to bring enforcement actions in response to unfair or deceptive trade practices within their state. These laws provide a similar broad authority to the states, but also sometimes specifically proscribe specific privacy violations.<sup>24</sup> While most regulatory efforts with respect to behavioral advertising and other privacy issues have taken place at the federal level, some recent privacy-related actions filed by states are worth noting. Connecticut, for example, filed an action earlier this year that, among other things, claimed that a company violated Connecticut’s mini-FTC Act for failing to disclose a breach of personal information in a timely fashion as required under Connecticut’s breach notification statute.<sup>25</sup> In another example, in 2006 Washington announced a \$1 million settlement with a New York-based company under an anti-spyware law based on the company’s marketing of software that falsely claimed computers were infected with spyware and then enticed consumers to pay for a program that claimed to remove it.<sup>26</sup>

States have also begun to pass and implement laws and regulations that prescribe specific data security rules for companies collecting and maintaining personal data. For example, Massachusetts recently issued its “Standards for the Protection of Personal Information of Residents of the Commonwealth,”<sup>27</sup> which became effective March 1, 2010. These regulations provide definitive data security guidelines for companies that store the personal data of Massachusetts residents (unlike FTC standards that have been developed piecemeal through enforcement actions), and are sector neutral, unlike the similarly (and in some cases less) comprehensive regulations passed under both the GLBA and HIPAA.<sup>28</sup>

<sup>22</sup> Ponemon Institute, Ponemon Study Shows the Cost of a Data Breach Continues to Increase (Jan. 25, 2010), available at <http://ponemon.org/news-2/23>.

<sup>23</sup> See Bamberger & Mulligan, *supra* note 3, at 40.

<sup>24</sup> Nebraska and Pennsylvania, for example, have laws explicitly deeming false or misleading statements in privacy policies regarding the use of personal information to be violations of their mini-FTC Acts. NEB. STAT. § 87-302(14); 18 PA. C.S.A. § 4107(a)(10).

<sup>25</sup> See Complaint, *Connecticut v. Health Net of the Northeast, Inc.*, No. 10-cv-00057 (D. Conn. filed Jan. 13, 2010).

<sup>26</sup> See Press Release, Wash. State Office of the Attorney General, Attorney General McKenna Announces \$1 Million Settlement in Washington’s First Spyware Suit (Dec. 4, 2006), available at <http://atg.wa.gov/pressrelease.aspx?id=5926>.

<sup>27</sup> 201 MASS. CODE REGS. 17.00.

<sup>28</sup> While the Massachusetts Standards are the most comprehensive state regulations pertaining to data security, most states have some form of law requiring organizations that store personal data to use “reasonable” measures to protect the security of that data. See, e.g., CAL. CIV. CODE § 1798.81.5 (requiring the implementation of “reasonable security procedures and practices” to protect personal data “from unauthorized access, destruction, use, modification, or disclosure,” and also requiring that when disclosing personal data to a third party, organizations require by contract that the third party provide similar security procedures and practices). A few others, like Oregon and Nevada, have gone past this baseline

## II. Collaboration Between Regulators and Industry

As mentioned, the FTC works with various stakeholders, including privacy advocates and industry, to shape privacy protections that best serve the interests of consumers while not unduly restricting innovation. Achieving the optimal balance between privacy and innovation was the expressly stated goal of this year’s FTC Privacy Roundtables.<sup>29</sup>

The FTC Report on online behavioral advertising in 2009 warned industry that it would push to formally regulate if self-regulatory efforts did not better protect consumer privacy.<sup>30</sup> In recent months FTC leadership has expressed support for industry-developed privacy-enhancing efforts.<sup>31</sup>

U.S. government interest in engaging industry on privacy issues is not limited to the FTC. On April 23, the U.S. Department of Commerce (DOC) announced a comprehensive review by its Internet Policy Task Force of the nexus between privacy policy and innovation in the internet economy, and sought public comment regarding the impact of the current U.S. privacy framework on internet commerce and innovation.<sup>32</sup> The DOC received seventy-four comments<sup>33</sup> and intends to review those comments and submit a report making recommendations to the President about the policy stance

of requiring “reasonable” measures and, like Massachusetts, require companies to take certain affirmative steps to protect the security of personal data. See, e.g., OR. REV. STAT. § 646A.622 (requiring any organization that owns, maintains, or otherwise possesses consumer personal information to implement an information security program that includes specific administrative, technical, and physical safeguards); NEV. REV. STAT. § 603A.215 (requiring organizations to encrypt personal information transferred over public networks or stored on portable devices moved outside the logical or physical boundaries of the organization).

<sup>29</sup> See *supra* note 19 and accompanying text.

<sup>30</sup> See *supra* note 18 and accompanying text.

<sup>31</sup> Speaking of these efforts this past May, FTC Chairman Jon Leibowitz stated that the FTC was not interested in regulating online behavioral advertising so long as industry is making “progress” toward self-regulation. Jon Eggerton, *Leibowitz: FTC Not Interested in Regulating Behavioral Ads If Industry Can Do Job*, Broadcasting & Cable (May 12, 2010), [http://broadcastingcable.com/article/452590-Leibowitz\\_FTC\\_Not\\_Interested\\_in\\_Regulating\\_Behavioral\\_Ads\\_If\\_Industry\\_Can\\_Do\\_Job.php](http://broadcastingcable.com/article/452590-Leibowitz_FTC_Not_Interested_in_Regulating_Behavioral_Ads_If_Industry_Can_Do_Job.php). He also said the FTC has “great hopes” for proposed self-regulatory guidelines proposed by direct and online marketers in conjunction with the Better Business Bureau. See also *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 14 (July 27, 2010) (statement of Jon Leibowitz, Chairman, FTC), available at [http://commerce.senate.gov/public/?a=Files.Serve&File\\_id=057baf64-4393-4b42-8fe1-d216f45d3be0](http://commerce.senate.gov/public/?a=Files.Serve&File_id=057baf64-4393-4b42-8fe1-d216f45d3be0) (“[The FTC’s online behavioral advertising] report was the catalyst for industry to institute a number of self-regulatory advances. While these efforts are still in their developmental stages, they are encouraging. We will continue to work with industry to improve consumer control and understanding of the evolving use of online behavioral advertising.”).

<sup>32</sup> *Information Privacy and Innovation in the Internet Economy*, Notice of Inquiry, 75 Fed. Reg. 21,226 (Apr. 3, 2010), available at [http://ntia.doc.gov/frnotices/2010/FR\\_PrivacyNOI\\_04232010.pdf](http://ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf).

<sup>33</sup> See Public Comments on Docket #100402174-0175-01, <http://ntia.doc.gov/comments/100402174-0175-01>. For an example, see the comments of the Future of Privacy Forum, available at <http://futureofprivacy.org/2010/06/17/fpf-submits-comments-in-response-to-department-of-commerce-privacy-noi>.

the United States should take on privacy issues moving forward.

What the FTC, DOC, and other American regulators have realized is that by collaborating with industry, which has the greatest control over the products and services in commerce that most directly affect consumer privacy, they are able to become better educated about the issues and use their authority to achieve a better balance between privacy and innovation. A perfect example of this is the FTC's encouragement of self-regulatory organizations to ensure that consumers are not harmed by deceptive or unfair advertising. The use of these self-regulatory organizations helps take the burden off of government regulators, with the regulators retaining jurisdiction to step in when they find cases of unfairness or deception.

Collaborating with all parties concerned with privacy and data security is an essential part of the success of the American approach. Still, the FTC (and other regulators with jurisdiction over privacy issues) retain their enforcement authority and exercise it regularly. This "carrot and stick" approach has produced advances in privacy protection in the United States. The FTC's willingness to collaborate with industry and support the self-regulatory environment has inspired companies to develop innovative privacy-enhancing technologies that increase the transparency of their uses of consumer information and maximize the level of control that consumers have over these uses.

## Innovations in the Presentation of Privacy Policies

For example, privacy policies remain the primary means of providing legally required notice to consumers in the United States about the collection and use of their information. California's Online Privacy Protection Act requires most companies that operate online in the United States to have privacy policies.<sup>34</sup> Given that privacy policies likely will remain the norm for the foreseeable future, some companies have undertaken commendable efforts to transform these policies into a format more easily understood by the average internet user.

A good example of this innovation is buzz.com that, in addition to its listed privacy policy, maintains a link to "how your information is shared on buzz.com." This link provides concise, straightforward information about buzz.com's information sharing practices, even noting that anonymity does not guarantee secrecy, as shown here:

**How you can control the information you share on buzz.com**

On buzz.com there are two kinds of users: **shy** and **outgoing**. You can decide which one you are. In a nutshell, here's how it works:

**Outgoing users** definitely get the best experience from buzz.com. They share not just their basic information (name, profile photo and location) but also their questions and recommendations with the entire buzz.com community. If you're outgoing, it's easier for others to find you, and to make new friends.

**Shy users** can use the whole site, but will get a less awesome experience. Their name, photo and location are visible (if they provide them) on some parts of the site, but their questions and recommendations are displayed anonymously to people who aren't their friends. If you're shy, your friends can still see the questions you ask and the recommendations you make.


Note that *anonymity is not privacy*. It might be possible for someone to accurately determine that you are the author of a particular piece of information, based on other contextual information. For example, if you are friends with only two other people in your community, and you ask a question that they then answer, it would not be difficult for a fourth person to surmise that *you* asked the question. For this reason, you should not use buzz.com to share information that requires a guarantee of secrecy.

Privacy Policy | Terms of Service | Disclaimer  
 Things you should know about how your information is shared on buzz.com  
 © 2010 AT&T Intellectual Property. All rights reserved.  
 AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

<sup>34</sup> See Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575-22579. Also, Congress is currently discussing legislation that would require companies to post privacy policies when they collect and share user information online for advertising purposes. See Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards (BEST PRACTICES) Act, H.R. 5777, 111th Cong. § 102, available at [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111\\_cong\\_bills&docid=f:h5777ih.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h5777ih.txt.pdf); Discussion Draft of Privacy Legislation § 3, available at [http://boucher.house.gov/images/stories/Privacy\\_Draft\\_5-10.pdf](http://boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf).

As another example, in June 2009, communications company AT&T unveiled a new, unified privacy policy that replaced seventeen separate privacy policies for various AT&T companies, products, or services.<sup>35</sup> In drafting this policy, AT&T incorporated feedback from focus groups. Before the policy went into effect, AT&T offered customers a forty-five-day preview, answered questions, and made clarifications to policy language. The result, illustrated below, included videos of AT&T employees describing aspects of its policy to make it more easily understood by consumers.

## AT&T Privacy Policy








**Dorothy Attwood**  
Chief Privacy Officer

**Watch these short videos to learn about our privacy policy.**

**We Are Committed to Protecting Your Privacy.**

Dorothy Attwood, AT&T's Chief Privacy Officer, explains our privacy commitments.








**Privacy Commitments**

AT&T takes your privacy very seriously. Our customers told us they want to see clear, easy-to-read information about our privacy commitments and policy. We have made our privacy policy easier to find and easier to read. And we're listening. We welcome your questions and feedback on our privacy policy, and invite you to contact us.

Our privacy commitments are fundamental to the way we do business every day. These apply to everyone who has a relationship with AT&T — including customers (wireless, Internet, digital TV, and telephone) and Web site visitors.

- We will protect your privacy and keep your personal information safe. We use powerful encryption and other security safeguards to protect customer data.
- We will not sell your personal information to anyone, for any purpose. Period.
- We will fully disclose our privacy policy in plain language, and make our policy easily accessible to you.
- We will notify you of revisions to our privacy policy, in advance. No surprises.
- You have choices about how AT&T uses your information for marketing purposes. Customers are in control.
- We're listening. You can send us questions or feedback on our privacy policy.

En Español 

**Welcome to the AT&T Privacy Policy**, effective date **August 27, 2009**. We invite you to learn more about our commitments, safeguards and customer choices.

In February 2010, AT&T was named one of the Most Trusted Companies in Privacy by Ponemon Institute.

**Privacy Updates**

Check back here for updates. If you would like to send us a question or comment, click here for contact information. See the FAQ for questions and answers about the privacy policy. The FAQ is an essential part of our Privacy Policy.

**Updated August 27, 2009**

AT&T offered a 45-day preview of the updated privacy policy, and we invited customers to send us feedback. Highlights of changes made to the AT&T Privacy Policy and FAQ include:

- Added definitions of Web beacons, widgets and server logs.
- Specifically confirmed that we do not sell, give or "rent" your Personal Information to marketing companies.

Likewise, Verizon employs a plain English, layered approach to its privacy policy, with simple statements on how it collects and uses personal information, and hyperlinks for users to obtain more detailed information about the privacy policy, as shown here:

<sup>35</sup> AT&T, AT&T Named One of the Most Trusted Companies in Privacy: Ponemon Institute Survey Shows Consumers Rank AT&T Among Leaders in Protecting Personal Information (Feb. 25, 2010), <http://att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=30569>.

**Privacy Policy**

**Privacy Policy Summary**

**Verizon is Committed to Protecting Your Privacy**

Protecting our customers' privacy is an important priority at Verizon. We are committed to maintaining strong and meaningful privacy protections for customers. Our privacy policy is designed to inform you about the information we collect, how we use it, and your options with regard to that collection and use. Key elements of our [full privacy policy](#) are summarized below.

Verizon's privacy policy applies to customers of the Verizon family of companies in the United States and to visitors to Verizon Web sites. It does not apply to Verizon Business customers outside the United States.

> [Read more](#)

**Information We Collect and How We Use It**

Verizon collects and uses information about our customers and Web visitors for a variety of purposes. Information may be obtained when you order and use our products and services, when you make customer service inquiries, or when you visit our Web sites.

We use such information to deliver, provide, and repair products or services; establish and maintain customer accounts and billing records; contact you about our products and services and better direct specific offers or promotions to you; monitor Web site statistics; monitor our customer service employees; or establish your online account and authenticate you during log-in.

> [Read more](#)

**Third-Party Advertising:**

You may see third-party advertisements on some Verizon Web sites. In some instances, third-party ad networks may seek to provide advertising that they believe is more relevant to your interests. In these instances, cookies may be used by ad networks to collect information about your visit to our Web sites and may be combined with information collected by these ad networks on other Web sites. You may limit this use.

> [Read more](#)

**Information We Share**

**Within the Verizon Family of Companies:**

Verizon shares customer information across our family of companies for marketing purposes unless you advise us not to. Specific laws govern our sharing of certain customer information known as Customer Proprietary Network Information.

> [Read more](#)

**Outside the Verizon Family of Companies:**

Except in certain circumstances explained in our privacy policy, Verizon does not sell, license or share information that individually identifies our customers with others outside of Verizon for non-Verizon purposes without your consent.

> [Read more](#)

**How to Limit the Sharing and Use of Your Information**

**Other Privacy & Policy Links**

- > [Privacy Policy Summary](#)
- > [Privacy Policy](#)
- > [A Message from Verizon's CEO](#)
- > [Tips for Guarding Your Information](#)
- > [FIOS TV Subscriber Privacy Notice](#)
- > [Browser Policy Statement](#)
- > [Your California Privacy Rights](#)
- > [Your Ohio Rights & Responsibilities](#)

**TRUSTe Privacy Program**

**Verizon Participates in the TRUSTe Privacy Program**

The TRUSTe seal confirms that Verizon is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent organization that seeks to build users' trust and confidence in the Internet by promoting the use of fair information practices. Verizon wants you to feel confident about your privacy when you use our Web sites (verizon.com, verizonmarketing.com, verizonwireless.com, mci.com, verizonbusiness.com, vzw.com, vzwshop.com, and verizon.net) so we ask TRUSTe to review these sites to ensure compliance with its guidelines.

Please [contact us](#) if you have questions or concerns regarding our privacy policy. If you have not received

The alternatives to dense, legalistic privacy policies offered by AT&T, Verizon, and others constitute an important move towards greater transparency and consumer understanding.

### The Emergence of Recognizable Icons to Inform Consumers

The most common criticism of the privacy policy approach to notice and choice is that most website users do not read or understand lengthy legalistic policies accessible only by clicking on a tiny link at the bottom of a web page. Earlier this year, FPF released the results of a research study that tested, as a method of improving consumer privacy choices online, the effectiveness of using new icons and key phrases to provide web surfers with more transparency and choice about behavioral advertising practices.<sup>36</sup> The results indicated that the icons and phrases, plus an education campaign, can play an important role in educating consumers about behavioral advertising. The study also found that applying transparency and choice to behavioral ads increased the percentage of those who were comfortable with online behavioral advertising by 37 percent.

The response from regulators was immediate and overwhelmingly positive. FTC Chairman Jon Leibowitz praised the research and development of the icon,<sup>37</sup> and FTC Consumer Protection Director David Vladeck called the icon a step "for the good" at one of the FTC Privacy Roundtables this year.<sup>38</sup> Even the EU Article 29 Working Party, in its opinion released this past June regarding online behavioral advertising, specifically lauded FPF's efforts in developing icons as a method of providing EU data subjects with a greater understanding of how their information will be

<sup>36</sup> FUTURE OF PRIVACY FORUM, ONLINE BEHAVIORAL ADVERTISING "ICON" STUDY: SUMMARY OF KEY RESULTS (Jan. 25, 2010), available at <http://futureofprivacy.org/2010/01/27/future-of-privacy-forum-releases-behavioral-notices-study>.

<sup>37</sup> Chairman Leibowitz stated: "I'm very heartened with what the Future of Privacy Forum has announced. Most current online privacy policies are essentially incomprehensible from even the savviest online users." Wendy Davis, Can WPP Demystify Behavioral Targeting? (May 20, 2009), [http://mediapost.com/publications/?fa=Articles.showArticle&art\\_id=106519](http://mediapost.com/publications/?fa=Articles.showArticle&art_id=106519).

<sup>38</sup> See Jules Polonetsky, Behavioral Ads Good for Business, Sez the NAI (Mar. 24, 2010), <http://futureofprivacy.org/2010/03/24/behavioral-ads-work-and-cost-more-sez-the-nai>.

collected and used online.<sup>39</sup> FPF may not have supported this research, however, if it were not for the FTC's initial efforts in encouraging the industry to seek alternative forms of notice to consumers. In addition, subsequent approval of the use of icons by regulators gives businesses the comfort that their use of icons to deliver privacy notices will likely be deemed adequate notice by the regulators. In this way, the dialogue between regulators and industry (with the FPF acting as an intermediary) has led to the development of a privacy-enhancing technology concept that has increased the privacy of consumers while giving businesses the comfort that they will not likely face an enforcement action from a regulator for insufficient notice.



Spurred by this research, as well as the FTC's prodding to implement better privacy-enhancing technologies to increase consumer understanding of online behavioral advertising, the "Power I" icon developed from the FPF's research (pictured at right), or variations on it, have been adopted following the release of the FPF Report.<sup>40</sup> The concept served as support for self-regulatory programs that are emerging now.

Self-regulatory organizations and organizations have been doing the hard work of building out the requirements and operational needs of a full scale effort in this area and they have worked to further refine permutations of the Power I into something that will work for their industries. For example, websites like Yahoo!, yp.com, and eBay adopted the Power I icon and an explanatory phrase when delivering targeted ads. Clicking on the icon on these websites links to a list of preferences that gives users information about the specific ad and allows them to opt out of future targeted ads. For example, clicking on the icon on yp.com leads to the following screen:

The Power I has not been the only innovation in achieving heightened consumer notice. TRUSTe, a provider of online privacy accreditation services, also has launched a program to allow websites to provide enhanced notice to users and to add better opt-out controls. An example of this program, as adopted by Comcast, is shown here:

<sup>39</sup> See ARTICLE 29 DATA PROTECTION WORKING PARTY, WP 171, OPINION 2/2010 ON ONLINE BEHAVIOURAL ADVERTISING 16 n.35 (2010), available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf).

<sup>40</sup> See Stephanie Clifford, *A Little 'I' to Teach About Online Privacy*, N.Y. TIMES, Jan. 26, 2010, at B3, available at <http://nytimes.com/2010/01/27/business/media/27adco.html>; Am. Ass'n of Adver. Agencies, Ass'n of Nat'l Advertisers, Direct Mktg. Ass'n, Interactive Adver. Bureau, & Council for the Better Bus. Bureaus, Trade Groups Announce the Selection of the Wording and Link/Icon that Will be Used to Indicate Adherence to Industry Self-Regulatory Principles for Online Behavioral Advertising (Jan. 27, 2010), available at <http://the-dma.org/cgi/dispanouncements?article=1379>.

**TRUSTe** **Welcome.** This site is working with TRUSTe to test an improved advertising notice for consumers. CLOSE

**STEP 1: Notice**  
Info about ads on this site

**STEP 2: Feedback**  
Tell us what you think

**Notice:**  
Our ad network partners may use your activity on this site to help choose ads you see here and at other sites. Your current browser privacy settings to block third party cookies may already prevent you from receiving interest-based advertising.

What are interest-based ads? +

What are ad networks? +

**LEAVE FEEDBACK**  
No Thank You

**TRUSTe Privacy Certification**  
This site complies with TRUSTe's Privacy program requirements.

If implemented in concert with serious self-regulatory efforts and continued technology advances encouraging their adoption, these programs relying on icons and phrases represent an important step in the evolution of notice and choice from sometimes-convoluted privacy policies to a more visceral, understandable method that better informs consumers about how their information is used by the websites they visit.

### Reduced Data Retention Periods

It is axiomatic that if data does not exist, it cannot be misused or used in a way that surprises consumers. Some companies have undertaken efforts to limit the time that they retain certain information about consumers' online activities. For example, the operators of the three most popular search engines have reduced their retention of internet protocol (IP) addresses and cookies in server logs within the last two years: Google has reduced its retention period from eighteen months to nine months,<sup>41</sup> Microsoft has reduced its retention period from eighteen months to six months,<sup>42</sup> and Yahoo! has reduced its retention period from thirteen months to three months.<sup>43</sup> Notably, Yahoo! has applied its retention program to both search logs and to ad-serving log files. There also have been self-regulatory efforts to publicize retention periods to help consumers make informed choices based on how long their information is retained. The NAI, for example, requires its members to retain personal data only as long as necessary to fulfill

a "legitimate business need" and to publish their retention periods on their websites.<sup>44</sup> Note, for example, Lotame Solutions, an NAI member which explains that it keeps ad-serving log data for no longer than nine months.<sup>45</sup>

The shortening of retention periods for data that can be used to personally identify consumers is an important step toward ensuring consumers' privacy in their internet use.

Another privacy-enhancing technique is the minimization of IP address details in web analytics. Website owners hire web analytics companies to provide certain details about the usage and performance of their sites, such as the number of unique users, the ability of users to navigate to the content they seek, and the usability of a website in general. Necessarily, companies providing web analytics services are initially sent user IP addresses. Although these addresses do not explicitly identify a particular individual, the potential for identification in some circumstances calls for more conservative practices. FPF recommends that IP addresses logged by web analytics providers be obscured or deleted as soon as possible and previously recommended this practice be adopted by federal government agencies that use such analytics tools.<sup>46</sup>

Some companies have taken commendable steps toward minimizing the collection, reporting, and retention of the IP addresses of the users of the websites they track. A number of companies can provide clients with a feature that ensures the IP addresses collected for

<sup>41</sup> Peter Fleischer, Global Privacy Counsel, Jane Horvath, Senior Privacy Counsel & Alma Whitten, Software Eng'r, Google, Another step to protect user privacy (Sept. 8, 2008), <http://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html>.

<sup>42</sup> John Vassallo, Vice President – EU Affairs, Microsoft, Microsoft Advances Search Privacy with Bing (Jan. 19, 2010), <http://microsoft.eu/Posts/Viewer/tabid/120/articleType/ArticleView/articleId/483/Microsoft-Advances-Search-Privacy-with-Bing.aspx>.

<sup>43</sup> Anne Toth, Vice President of Pol'y & Head of Privacy, Yahoo!, Your data goes incognito (Dec. 17, 2008), <http://ycorpblog.com/2008/12/17/your-data-goes-incognito>.

<sup>44</sup> NAI, 2008 NAI PRINCIPLES: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT III.2(a)(vi), 9(a) (2008), available at [http://networkadvertising.org/networks/2008%20NAI%20Principles\\_final%20for%20website.pdf](http://networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20website.pdf).

<sup>45</sup> See Lotame, Privacy Policy, <http://lotame.com/privacy>.

<sup>46</sup> See Future of Privacy Forum, Future of Privacy Forum Release Behavioral Notices Study (Jan. 27, 2010), <http://futureofprivacy.org/2010/01/27/future-of-privacy-forum-release-behavioral-notices-study>; FPF's Reply Comments to the Federal Websites Cookie Policy (Aug. 10, 2009), <http://futureofprivacy.org/2009/08/10/fpf-s-reply-comments-to-the-federal-websites-cookie-policy>.

analytics purposes will be immediately obscured. Encouraging wider spread of such efforts will ensure that analytics and other similar services are able to provide functionality in a manner that maintains user privacy.

### Stronger Browser Controls

Stronger browser controls are another way to protect online privacy. A substantial majority of consumers interact with third parties over the internet through a free, commercial web browser. These browsers serve as important gatekeepers between ordinary consumers and third parties to which these consumers transfer information. In their role as gatekeeper, developers of browsers generally increased the number of privacy controls available to users in recent years. These controls, however, were often buried deep within sub-menus and tabs and largely were unknown to the average user. Even if users were able to find these controls, recent studies demonstrated that users experience substantial confusion about the results of actions they take within their browsers and do not understand how the technology works.<sup>47</sup>

To rectify some of these issues, the major browser developers have designed enhanced privacy options to allow more users to customize and control how their information is shared with the websites they visit. Internet Explorer's InPrivate Browsing, Chrome's Incognito mode, Safari's Private Browsing, and Firefox's Stealther add-on all provide more straightforward interfaces and collections of privacy options that provide users with more transparency and control over how their information is shared and how they will allow websites to interact with their computers. Privacy has also be-

<sup>47</sup> Aleecia M. McDonald & Lorrie Faith Cranor, *An Empirical Study of How People Perceive Online Behavioral Advertising*, Carnegie Mellon University CyLab Technical Reports (Nov. 10, 2009), available at [http://www.cylab.cmu.edu/research/techreports/2009/tr\\_cylab09015.html](http://www.cylab.cmu.edu/research/techreports/2009/tr_cylab09015.html).

come a competitive element in new browser releases. Mozilla, for example, recently released details about the new version of its Firefox browser that includes a single menu to display what information websites are gathering and allow users to decide which cookies to allow and which to disable.<sup>48</sup> These continued enhancements of privacy controls, and a recognition that consumers may now choose their browser in part based on privacy features, bode well for the continued evolution of comprehensible privacy controls in web browsers.

### Plug-ins that ensure opt-out status even after clearing cookies

While many behavioral advertisers have taken affirmative steps to self-regulate, such as through the NAI and IAB, these efforts are limited by the means through which they implement a user's choice to opt out of behavioral targeting of advertisements. Such opt out is generally achieved by placing an "opt-out cookie" on a user's web browser that signals participating network advertising websites not to track that user's activities or place additional tracking cookies. Unfortunately, because these cookies expire after a certain period or are deleted whenever a user clears his or her cookie repository, the user must go through the opt-out process again whenever that opt-out cookie is deleted.

There are, however, technological solutions to achieve a more stable, persistent opt-out status. The Targeted Advertising Cookie Opt-Out plug-in for Mozilla's Firefox browser, the NAI Consumer Opt Out Registry, and Google advertising cookie opt-out plug-in, shown below, each ensure that a user's opt-out status is maintained even after opt-out cookies expire or are cleared by the user.

<sup>48</sup> Joel Schechtman, *Firefox 4 has simpler design, more privacy control*, ASSOCIATED PRESS (May 11, 2010), available at <http://abcnews.go.com/Technology/wireStory?id=10618620>.

The screenshot displays the Firefox Add-ons page for the 'Targeted Advertising Cookie Opt-Out (TACO) 2.0' by Christopher Soghoian. The interface includes a 'Download Now' button, version information (2.0), and a 'Share this Add-on' checkbox. Below this, there is a 'Google' logo and a large button that says 'Download the advertising cookie opt-out plugin'.

On the right side, a preview of the 'NAI Consumer Opt Out Protector - beta' interface is shown. It features a 'Registries' section with a table for adding registries and a 'Protected Opt Outs' section with a table of domains.

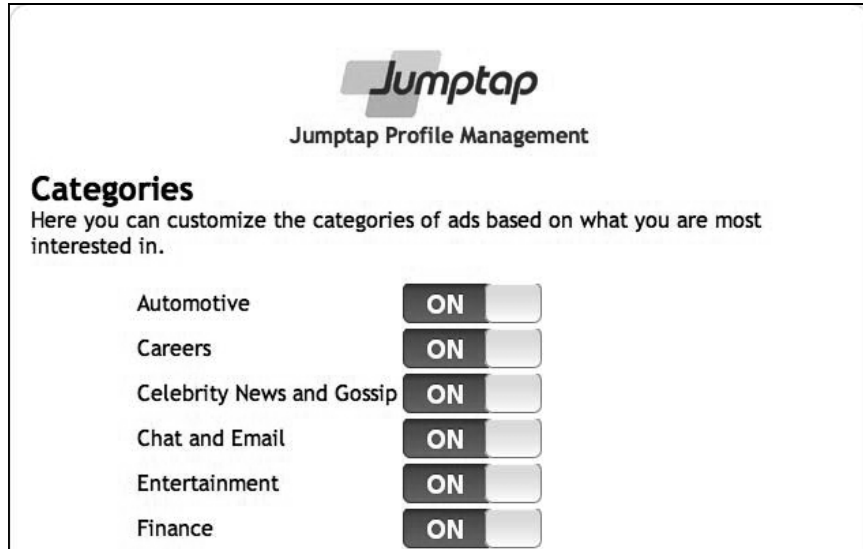
Registry Name	Check Updates	Info	Add	Delete	Save
NAI Consumer Opt Out Registry					

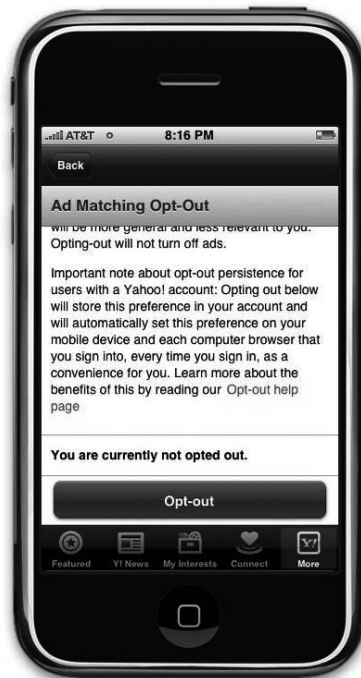
Company Name	Opt Out Domain
247 Realmedia	.realmedia.com
Advertising.com	.advertising.com
Akamai	.abmr.net
AlmondNet	.pro-market.net
...	...

## Creating a mobile opt out and mobile profile viewers that bring new behavioral controls being implemented on the web to mobile devices

With the increased use of smartphones and other mobile devices that can access the internet, companies are seeing great value in delivering targeted advertisements to mobile device users based on their mobile browsing. Companies deliver such advertising using similar methods to those used when individuals browse from their computers, including the use of cookies. While there has been a concerted effort to develop tools that increase transparency and control for consumers who use computer-based internet browsers, these tools have been relatively absent in the mobile context. That trend, however, is changing. Jumptap, which manages a mobile ad network, created the first mobile behavioral profile viewer that allows consumers to edit the categories of ads they will receive, as shown here:

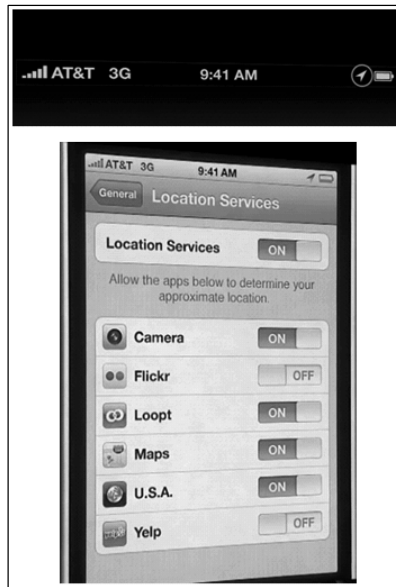


Many of the leading mobile ad networks already offer a mobile cookie opt-out, as noted in the Yahoo! disclosure shown at the right. The FTC has been clear in its behavioral advertising guidance that consumers should be entitled to opt out of behavioral ads, regardless of the platform involved.

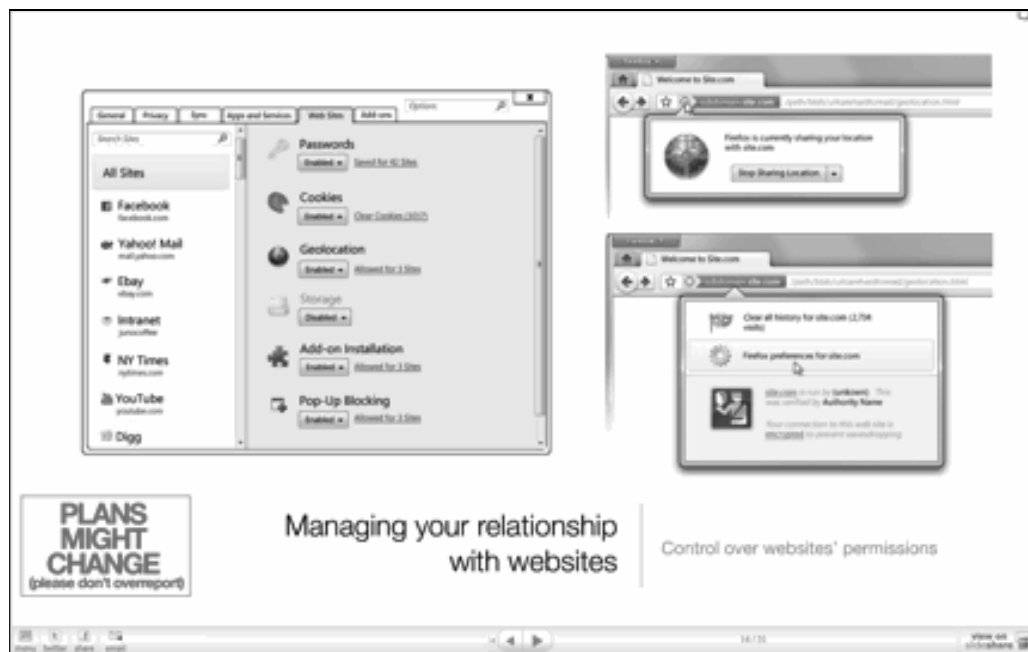


### Indicators showing when one is being geolocated

A significant trend in mobile advertising is the use of a mobile device user's exact geographic location (or "geolocation"), which is calculated and stored by mobile devices on an almost real-time basis, to deliver ads to the user relevant to that specific location. While ads specific to a consumer's location have the potential to deliver great value (such as by providing the consumer with a coupon for a nearby store), in many cases they can be unwanted, especially if the consumer perceives that he or she is being physically "watched" by advertisers. To better inform its customers, Apple included an icon in its new iPhone operating system informing users that their location information is being used, and allows users to control which apps can use that information, as shown at the right (the icon is circled). Verizon has also provided a similar symbol in recent years on many of the smart phones it supports.



Geolocation does not occur only on mobile devices. Some computer-based internet browsers, such as Firefox, allow websites to request geolocation information that the browser derives from a variety of sources such as by scanning local wireless access points. To alert users when a website requests their location in this manner, the new version of Firefox will now display an icon in the browser address bar, as shown below:



The iPhone's and Firefox's location tracking options are positive advancements in providing transparency and control over users' geolocation information.

\* \* \*

These technological innovations have occurred within the U.S. framework of privacy law and regulation and are an outgrowth of the privacy ecosystem documented by Professors Bamberger and Mulligan that has as its central feature robust enforcement by the FTC.

#### **IV. Conclusion**

There is much work to be done to advance privacy protections. Around the world, discussion continues

about optimal legal and regulatory structures, and needed changes in the face of new technologies and new generations of users. It is not intended to be jingoistic to cite the American experience as instructive. The combination of enforcement, targeted legal regulation, self-regulation, consultation and collaboration among stakeholders, and technological advances has created a framework of protection that is different than under other regimes, but nonetheless is worthy of study. The FPF hopes this exposition contributes to the global discussion about optimal approaches to the protection of personal privacy.