BEFORE THE
DEPARTMENT OF COMMERCE

OFFICE OF THE SECRETARY
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
INTERNATIONAL TRADE ADMINISTRATION
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Request for Comments

INFORMATION PRIVACY AND INNOVATION IN THE INTERNET ECONOMY

DOCKET# 100402174–0175–01

COMMENTS OF THE FUTURE OF PRIVACY FORUM

Jules Polonetsky
Co-Chair and Director, The Future of Privacy Forum
919 18th Street NW
Washington, DC 20036
202-713-9466
julespol@futureofprivacy.org

Christopher Wolf
Co-Chair, The Future of Privacy Forum
Bret Cohen
HOGAN LOVELLS US LLP
555 13th Street NW
Washington, DC 20004
202-637-8834
202-637-5910 (fax)
christopher.wolf@hoganlovells.com
Counsel for THE FUTURE OF PRIVACY FORUM

June 14, 2010

TABLE OF CONTENTS

Page

I. INTRODUCTION

The Future of Privacy Forum ("FPF") submits these Comments in response to the Department of Commerce Notice of Inquiry dated April 23, 2010 ("*NOI*").[1] In the *NOI*, the Department announced a comprehensive review by its Internet Policy Task Force of the nexus between privacy policy and innovation in the Internet economy.[2] The Department is seeking comments regarding the impact of the current privacy framework on Internet commerce and innovation. The Department also is soliciting input on the necessity of adjusting today's privacy framework to promote innovation and privacy in the web-centric information environment.[3]

The Internet plays an important role in America's economic growth, and in the everyday lives of Americans. It is an unprecedented medium for communication, education, entertainment, and commerce. Increasingly, online technology enables businesses to collect, use, share, and store vast amounts of personal and anonymous information about people using the Internet. Such use of data promises to fuel additional economic growth online. But, increasingly, people are concerned about their privacy online.[4] Thus, for Internet commerce to flourish, privacy protection must improve.

---

[1] *Information Privacy and Innovation in the Internet Economy*, Notice of Inquiry, 75 Fed. Reg. 21,226 (Apr. 3, 2010).

[2] *Id.*

[3] *Id.* at 21,228.

[4] According to a recent study by the Pew Internet & American Life Project, young people especially are concerned about their online privacy. *See* Pew Internet & Am. Life Project, Reputation Management and Social Media: How people monitor their identity and search for others online (May 26, 2010), *available at* http://pewinternet.org/Press-Releases/2010/Reputation-Management.aspx.

At a time when many are calling for a new paradigm to protect personal data online as the way to improve privacy, the reality is that the well-known Fair Information Practices,[5] with their bedrock transparency principle, will continue to underlie the ways in which personal privacy is protected for some time to come. Thus, while FPF encourages and supports new thinking about structural ways in which privacy can be protected and enhanced online, we also encourage innovations within the current Fair Information Practices framework, as well as implementation of all of the principles contained within the framework whenever feasible.[6] Given the Department's role in supporting and facilitating U.S. business today and in the near term, we focus in this submission on ways in which online privacy can be enhanced within the existing framework.

We believe there is ample room for improvement and innovation. For example, the results of a research study released by FPF earlier this year indicate that simplified and user-friendly methods to communicate about data use can substantially improve transparency and consumers' understanding about how their information is used online. An example of a notice icon developed collaboratively by FPF is described below. We also highlight in the submission recent innovations and improvements in online privacy, and identify areas where improvements are needed.

Finally, we suggest ways in which the Department can exercise leadership in promoting online privacy (and thereby promote online commerce) through specific initiatives.

---

[5] *See, e.g.*, CTR. FOR DEMOCRACY & TECH., COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY ON THE STAFF DISCUSSION DRAFT OF CONSUMER PRIVACY LEGISLATION 1-2 (June 4, 2010), *available at* http://cdt.org/files/pdfs/20100604_boucher_bill.pdf.

[6] In addition to transparency, other widely accepted Fair Information Practices include Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Accountability and Auditing, and Security. *Id.*

II. ABOUT THE FUTURE OF PRIVACY FORUM AND ITS ROLE IN THE DEVELOPMENT OF IMPROVED PRIVACY PRACTICES

FPF is a Washington, DC-based think tank whose purpose is to examine current and emerging challenges to personal privacy and to propose practical ideas to improve personal privacy now and in the future.[7] The efforts of such a non-governmental, non-profit entity is one way to advance privacy that should be encouraged by the Department, and we briefly highlight our recent efforts here.

As an example of FPF's role in the evolution of privacy practices, FPF recently led a project for the design of new forms of timely, informative, and eye-catching privacy notices concerning the collection of personal information for targeted advertising online. The genesis of the project was the realization that static and densely written privacy policies are limited in their ability to communicate clearly with consumers about what information is being collected and used by online businesses. Addressing this issue, the Federal Trade Commission ("FTC") expressed concern early last year that privacy policies were not being read or understood by consumers, and it urged the industry to develop new ways to notify consumers about online data collection and use.[8]

[7] FPF is supported by Adobe, AOL, AT&T, The Better Advertising Project, BlueKai, Deloitte, eBay, Intel, Lockheed Martin, Microsoft, The Nielsen Company, Proctor & Gamble, Qualcomm, Verizon, Visa, and Yahoo! and has an advisory board comprised of leading figures from industry, academia, law, and advocacy groups. The positions taken by FPF are entirely its own and do not necessarily reflect those of its supporters and advisory board members.

[8] *See* FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://ftc.gov/os/2009/02/P085400behavadreport.pdf.

With this in mind, FPF partnered with the global marketing communications company WPP to launch a consumer-focused effort that relied on the skill of advertising and communications professionals to produce notices accessible through symbols or "icons."[9] The icons were tested with an Internet survey of a large group of users to determine their utility in providing effective notice, and to select the most effective symbols and language.[10] The icons and associated language that were selected already have been deployed for testing by Yahoo!, AT&T, and eBay and they have been adopted as part of the self-regulatory programs of a coalition of leading industry groups. Thus, FPF has taken a leadership role in the undertakings urged by the FTC.[11]

Another major FPF initiative concerns privacy and the Smart Grid. Modernization efforts are underway to make the current electrical grid "smarter" through the collection of data about consumer usage. FPF is taking the lead here as well, working with the GridWise Alliance, the Privacy Commissioner of Ontario, and others to address the potential privacy concerns

---

[9] *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-forim-release-behavioral-notices-study.

[10] *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.

[11] FTC Chairman Jon Leibowitz recently reinforced his support for these efforts, stating that the FTC is not interested in regulating behavioral advertising so long as the 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. He also said the commission has "great hopes" for proposed self-regulatory guidelines proposed by direct and online marketers in conjunction with the Better Business Bureau.

implicated by the Smart Grid and to propose that privacy protections be built into the Smart Grid network as it is developed, using the principles of "Privacy by Design."[12]

Finally, among the major ongoing FPF initiatives, FPF is beginning to focus attention on the data collection issues raised by the growing popularity of Internet-based applications, or "apps," especially those supported by social networking platforms and by mobile devices. FPF believes that users should be provided with sufficient and timely information by app developers so that users can understand how data about them may be used when they interact with apps.

As the name suggests, FPF is focused on privacy issues that loom large for the future, which is why we are pleased to make this submission in connection with the Department's focus on the future of online privacy in the United States.

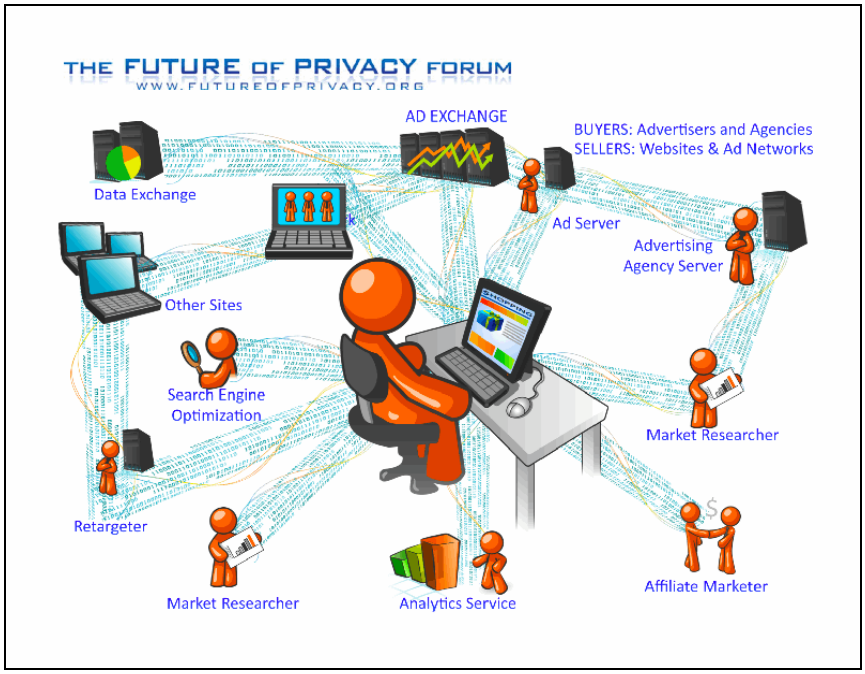
[12] FPF filed comments to the National Institute of Standards and Technology's Smart Grid Interoperability Standards Project to encourage responsible data management practices by all entities involved in the Smart Grid ecosystem and facilitate stakeholder discussions to develop best practices. Comments of the Future of Privacy Forum, Report to the National Institute of Standards and Technology on the Smart Grid Interoperability Standards Roadmap, Department of Commerce, Docket No. 0906181063-91064-01 (filed July 30, 2009); *see also* THE FUTURE OF PRIVACY FORUM & INFO. AND PRIVACY COMM'R OF ONT., SMARTPRIVACY FOR THE SMART GRID: EMBEDDING PRIVACY INTO THE DESIGN OF ELECTRICITY CONSERVATION (2009), *available at* http://ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf; Comments of the Future of Privacy Forum to the FCC on NBP Public Notice #2, GN Docket No. 09-47 (filed Oct. 2, 2009).

III. EXAMPLES OF INNOVATION AND AREAS OF NEEDED IMPROVEMENT IN ONLINE PRIVACY

This proceeding provides the opportunity for FPF to highlight best practices and to identify areas for improvement in online privacy. We hope that the Department will continue to provide a forum for the exchange of this kind of information that will incentivize the development of privacy-enhancing technologies and practices by those in the online ecosystem.

We begin by examining new methods of information exchange and the ways in which organizations inform users about and provide choices regarding the online collection and use of personal data.

The Internet has led to the development of highly efficient online data use platforms through which companies collaborate and combine their individual expertise to promote online commerce and to improve consumers' experiences. Whether an online user knows it or not, by visiting one website he or she can share data with dozens of companies: a web publisher, an ad exchange, a search engine, an analytics company, advertisers, and more. An example of these information exchanges is illustrated in the following graphic:



The success and efficiency of these platforms generates value for publishers and contributes to the growth of an open Internet with free content. Despite the fact that consumers may believe the site they are visiting is responsible for all data activity resulting from their visit, the fact is that data collection and use is often far from transparent. It is by no means clear whose privacy policy controls the collection, use, and sharing of data collected from visits to web pages.

A number of companies in the online ecosystem have taken the initiative to provide innovative features that increase the transparency of their uses of consumer information and maximize the level of control that consumers have over these uses. In the following section, we highlight a few notable innovations in privacy-enhancing technologies.

A. Noteworthy Innovations

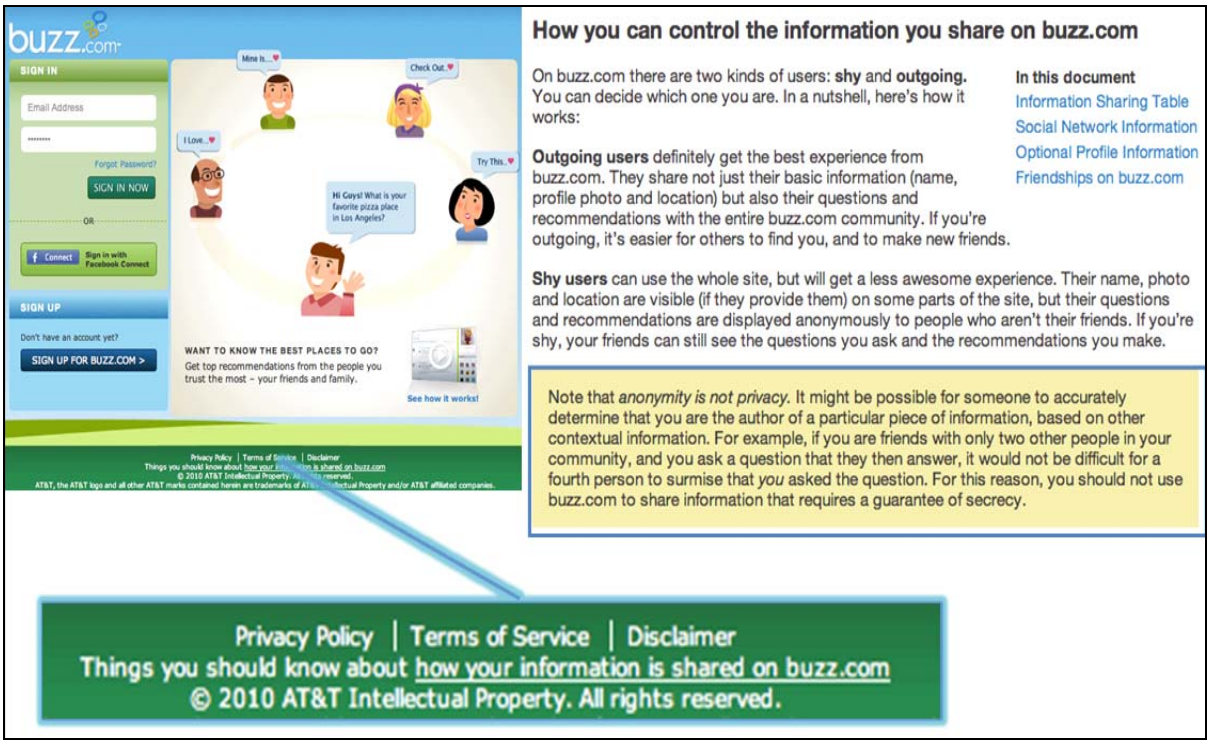
1. Labeling privacy policies in a common-sense fashion by directing users to see "how your information is being used"

Privacy policies remain the primary means of providing legally required notice to consumers 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.[13] 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.

---

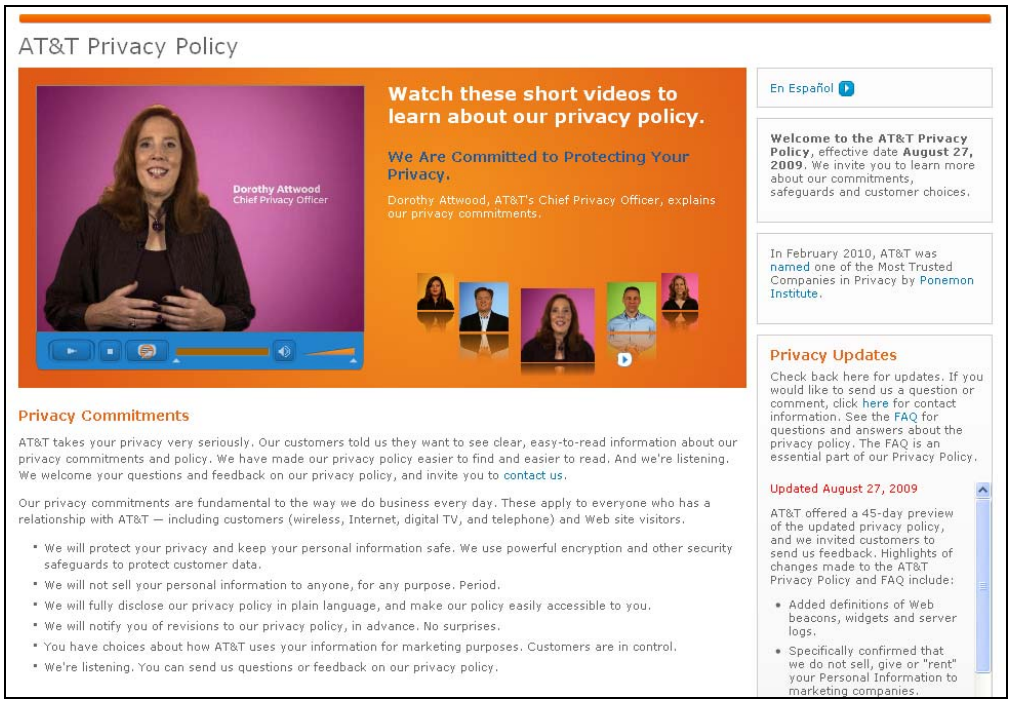
[13] *See* Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575-22579. Also, a recent discussion draft of a bill released by Representatives Rick Boucher (D–VA) and Cliff Stearns (R–CA) would require companies to post privacy policies when they collect and share user information online for advertising purposes. Draft bill § 3, http://boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf. The FTC, using its investigative and enforcement authority under Section 5 of the FTC Act, 15 U.S.C. § 45, ensures that promises made in online privacy policies are kept. *See* FTC, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority (July 2008), http://ftc.gov/ogc/brfovrvw.shtm.

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:

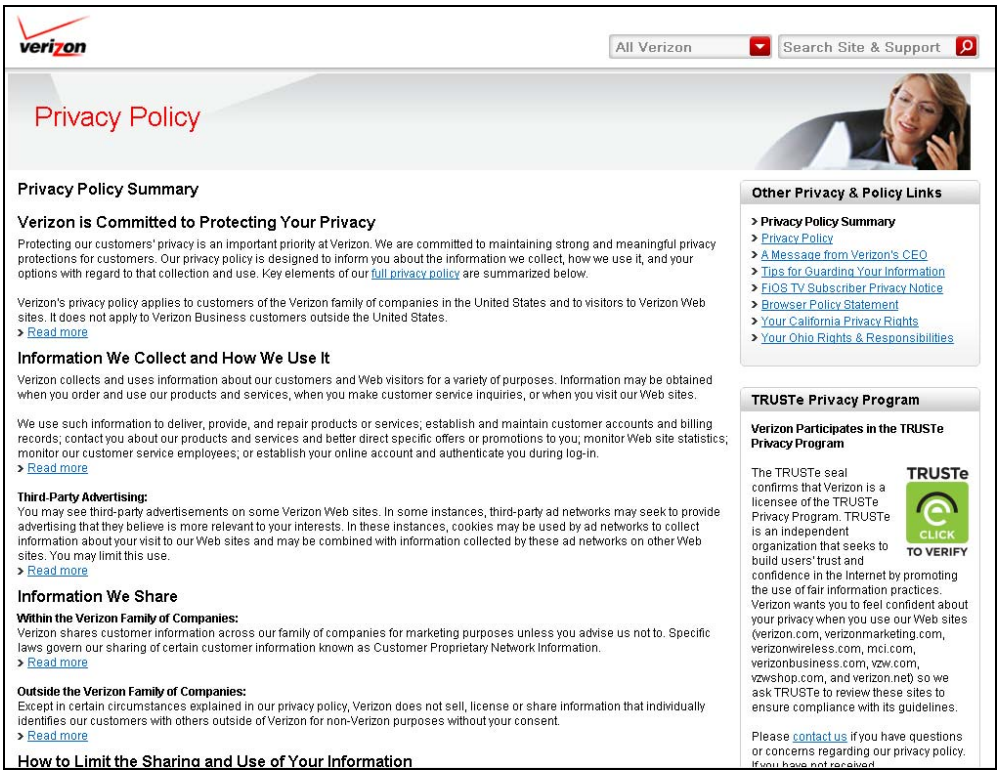


As another example, in June 2009, communications company AT&T unveiled a new, unified privacy policy that replaced seventeen separate privacy policies for various AT&T companies, products, or services.[14] In drafting this policy, AT&T incorporated feedback from focus groups. Before the policy went into 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.

[14] 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.



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:



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

2. The use of an icon to attract consumer attention and link to information

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.[15] Earlier this year, FPF released the results of a research study that tested, as an alternative to the privacy policy approach, the effectiveness of using new icons and key phrases to provide web surfers with more transparency and choice about behavioral advertising practices.[16] 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 behavioral advertising by 37%. The study was praised by FTC Chairman Jon Leibowitz, who in the past has urged companies to provide succinct notice about ad targeting,[17] as well as FTC Consumer Protection Director David Vladeck, who called the icon a step "for the good" at the FTC Privacy Roundtable this year.[18]

---

[15] *See infra* Section III.B.2.

[16] FUTURE OF PRIVACY FORUM, ONLINE BEHAVIORAL ADVERTISING "ICON" STUDY: SUMMARY OF KEY RESULTS (Jan. 25, 2010), *available at* http://futureofprivacy.org/final_report.pdf.

[17] 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_aid=106519.

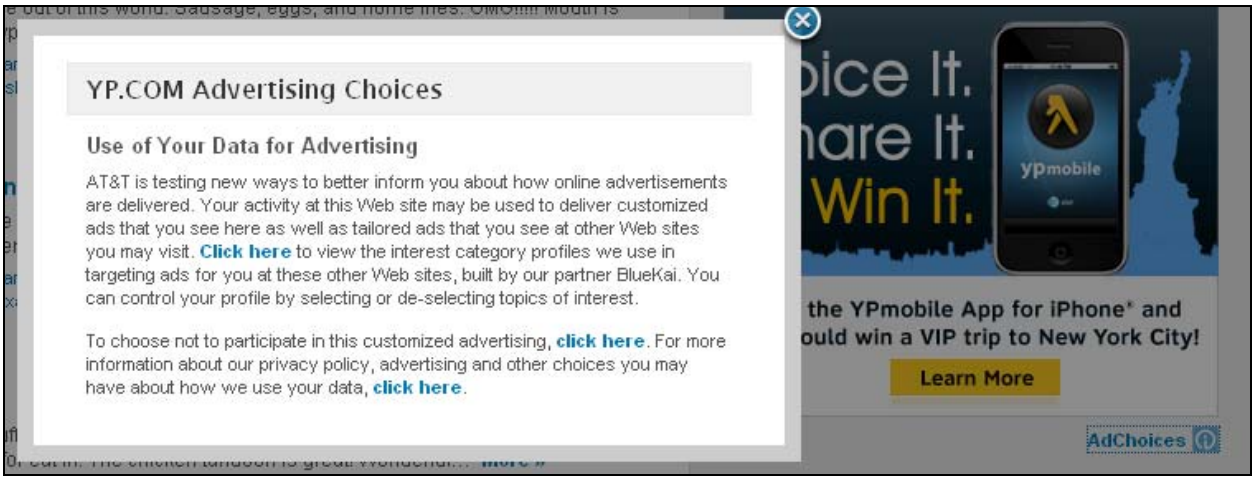
[18] *See* Jules Polonetsky, Behavioral Ads Good for Business, Sez the NAI (Mar. 24, 2010), http://futureofprivacy.org/2010/03/24/behavioral-ads-work-and-cost-more-sez-the-nai.

The "Power I," pictured at right, has been adopted following the release of the FPF Report.[19] It will serve as part of the self-regulatory programs of the Internet Advertising Bureau ("IAB"), the Network Advertising Initiative ("NAI"), the Association of National Advertisers, and the American Association of Advertising Agencies, and will be managed by the Better Business Bureau. Furthermore, in April, the NAI and IAB, both self-regulatory organizations for the online advertising industry, jointly released their CLEAR Ad Notice technical specification that enables the use of standard meta data in ad delivery coding to provide more detailed information about the type of ad targeting taking place. This enhanced notice will be accessible to users via the Power I symbol,[20] as shown here:

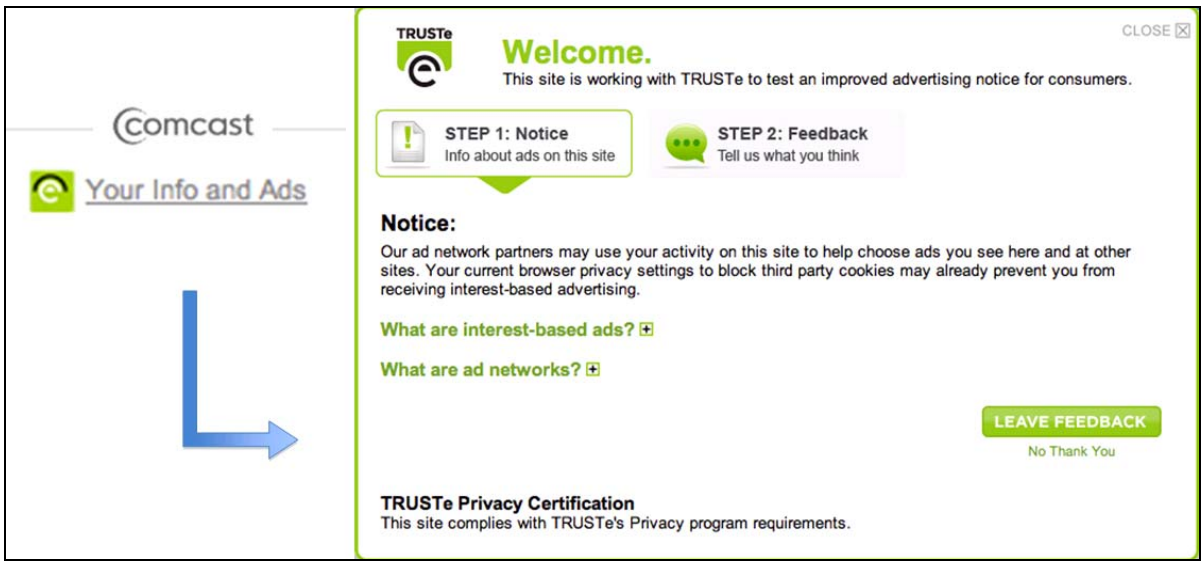
[19] *See* Stephanie Clifford, *A Little 'I' to Teach About Online Privacy*, N.Y. TIMES, Jan. 26, 2010, at B3, *available at* http://nytimes.com/2010/01/27/business/media/27adco.html; Am. Ass'n of Adver. Agencies, Ass'n of Nat'l Advertisers, Direct Mktg. Ass'n, Interactive Adver. Bureau, & Council for 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/dispannouncements?article=1379.

[20] *See* IAB & NAI, CLEAR AD NOTICE: TECHNICAL SPECIFICATIONS FOR THE IMPLEMENTATION OF THE INTERACTIVE ADVERTISING SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 5-6 (Apr. 2010), *available at* http://iab.net/media/file/CLEAR_Ad_Notice_Final_20100408.pdf.

Websites like Yahoo!, yp.com, and eBay also have already 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:



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.

3. Limiting the retention of search queries and deleting data used for targeted advertising after a defined period

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 IP addresses and cookies in server logs within the last two years: Google has reduced its retention period from eighteen months to nine months,[21] Microsoft has reduced its retention period from eighteen months to six months,[22] and Yahoo! has reduced its retention period from thirteen months to three months.[23] Notably, Yahoo! has applied its retention program to both search logs and to adserving 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

[21] 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.

[22] Peter Cullen, Chief Privacy Strategist, Microsoft, Microsoft Advances Search Privacy with Bing (Jan. 18, 2010), http://microsoftontheissues.com/cs/blogs/mscorp/archive/2010/01/18/microsoft-advances-search-privacy-with-bing.aspx.

[23] 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.

business need" and to publish their retention periods on their websites.[24] Note, for example, Lotame Solutions, an NAI member which explains that it keeps adserving log data for no longer than nine months.[25]

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.

4. Minimizing IP address details in web analytics

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.[26]

---

[24] 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.

[25] *See* Lotame, Privacy Policy, http://lotame.com/privacy (last visited June 14, 2010).

[26] *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-forim-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.

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 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.

5. Stronger browser privacy 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 submenus 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.[27]

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

[27] 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.

control over how their information is shared and how they will allow websites to interact with their computers. Privacy has also become 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.[28] 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.

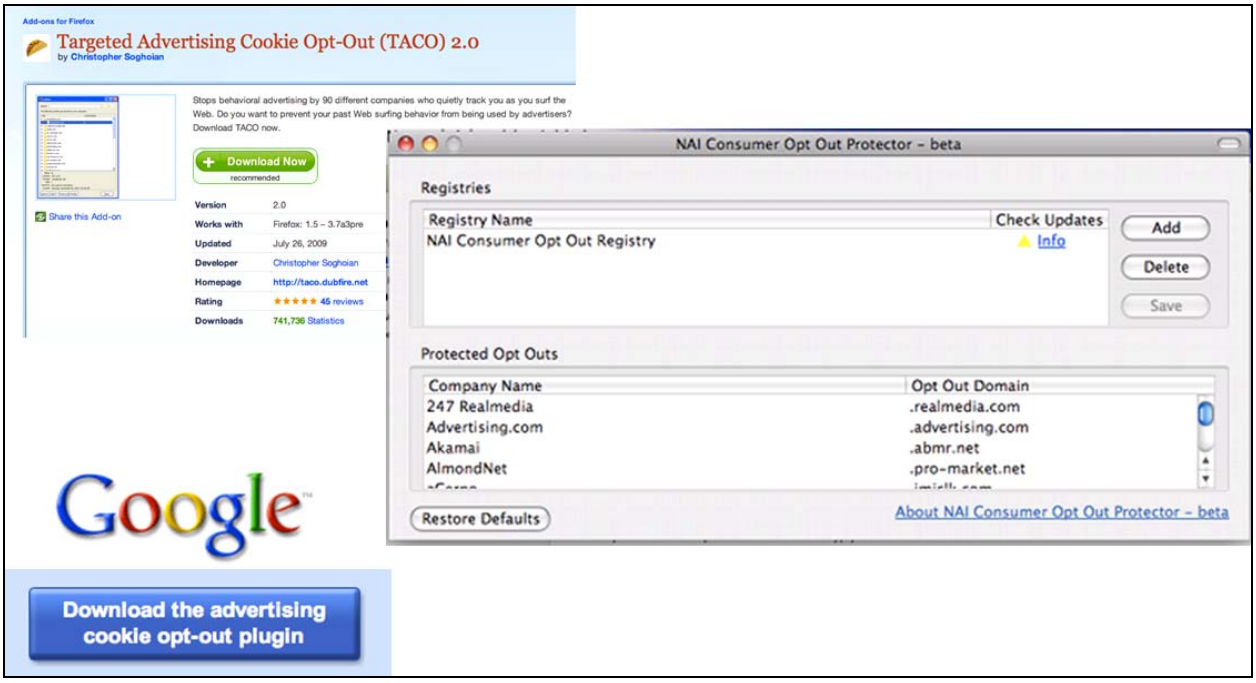
6. Plug-ins that ensure opt-out status even after clearing cookies

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 ("TACO") plug-in for Mozilla's Firefox browser, the NAI Consumer Opt Out Registry, and Google advertising cookie opt-out plug-in,

[28] Joel Schechtman, *Firefox 4 has simpler design, more privacy control*, ASSOCIATED PRESS (May 11, 2010), *available at* http://news.yahoo.com/s/ap/20100511/ap_on_hi_te/us_tec_techbit_firefox_browser.

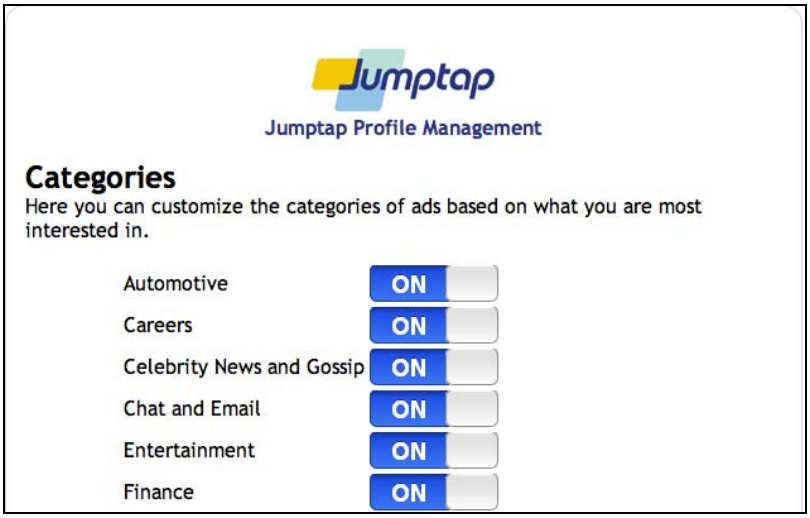
shown below, each ensure that a user's opt-out status is maintained even after opt-out cookies expire or are cleared by the user.



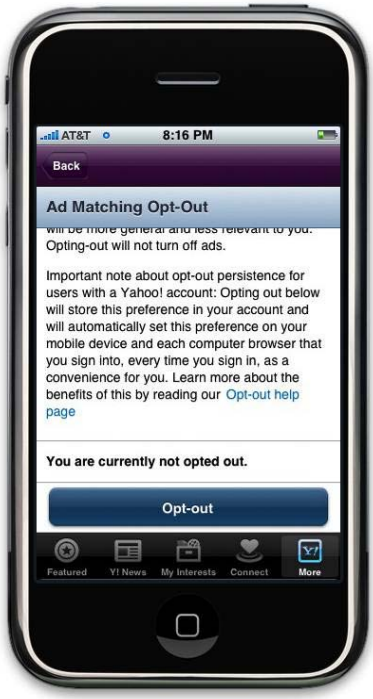
7. Creating a mobile opt out and mobile profile viewers that bring new behavioral controls being implemented on the web to mobile devices

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 below:

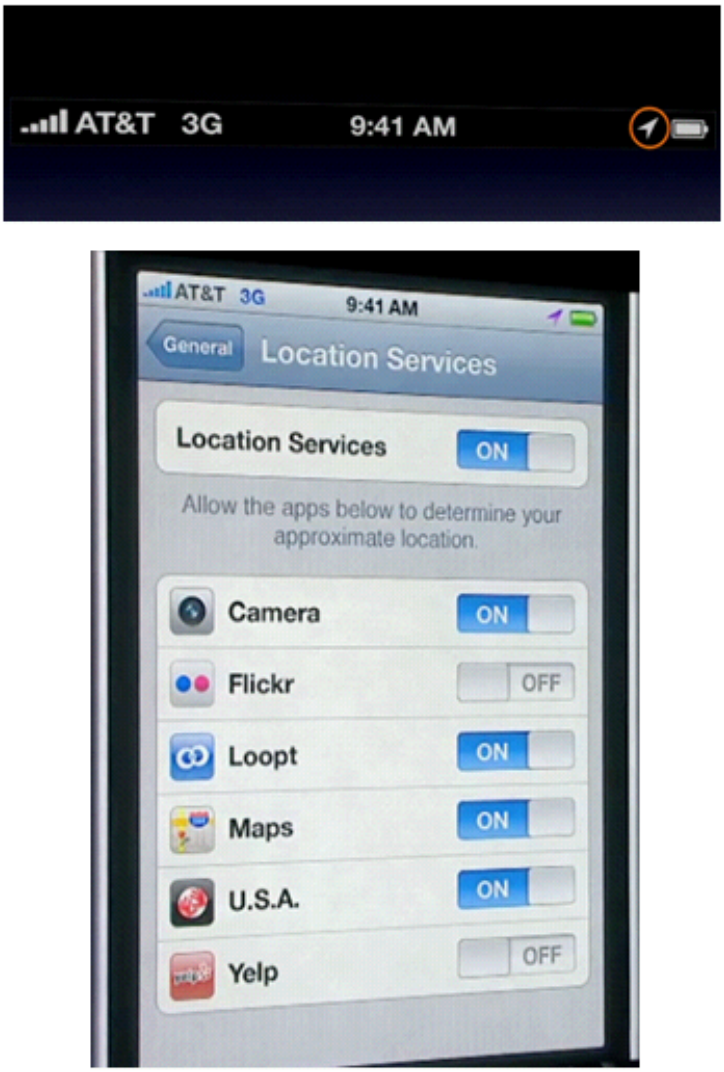


Many of the leading mobile ad networks already offer a mobile cookie opt-out, as noted in the Yahoo! disclosure shown below. The FTC has been clear in its behavioral advertising guidance that consumers should be entitled to opt out of behavioral ads, regardless of the platform involved.

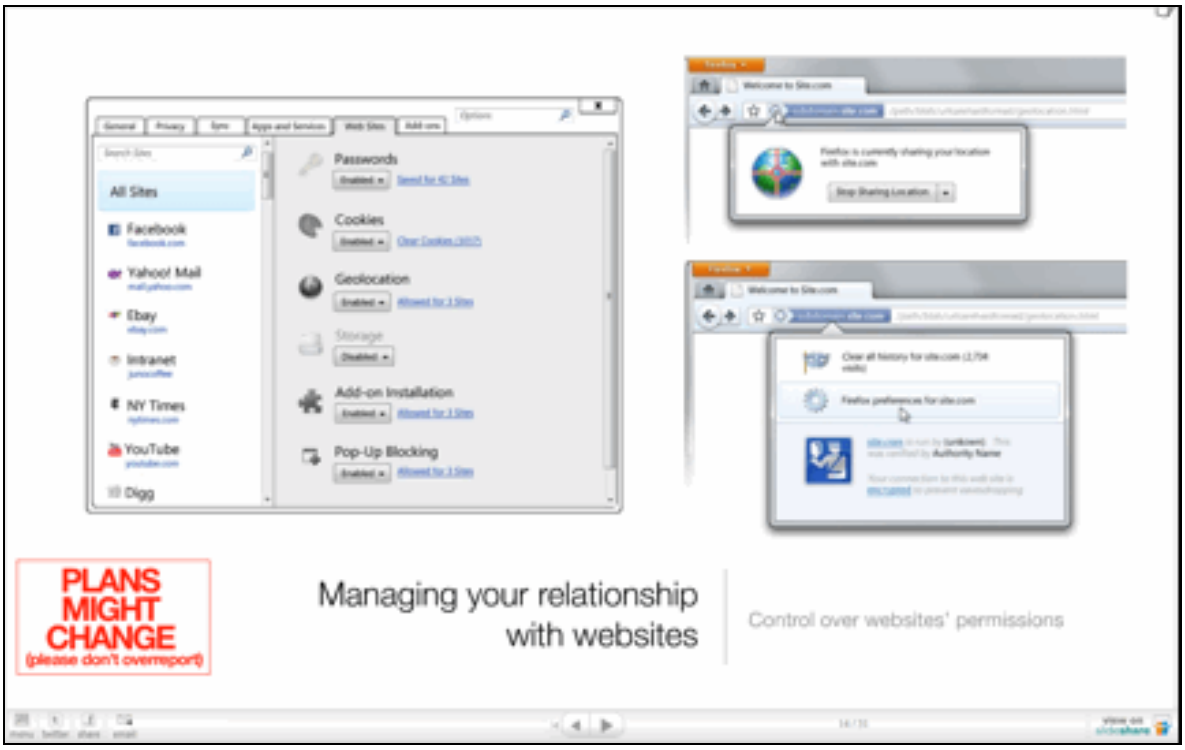


8. Indicators showing when one is being geolocated

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 here. 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.

B. Areas Needing Improvement

The efforts described above represent important steps forward in providing consumers with notice, choice, and control over their privacy options, as well as limitations on the retention of data. However, several challenges remain. This section outlines some key issues that FPF believes still need to be addressed.

1. Lack of usability of privacy controls, particularly for social networking

Social networking services have exploded in popularity over the past few years. So too has the amount of information – some of it sensitive personal information – that individuals are willing to post online through these services. As the popularity of these services has grown, social network operators have implemented new and innovative features in their products. With each new feature, however, the complexity of users' privacy controls grows.

The challenge for social networking services is to provide users with more granular privacy controls without the control interface becoming overly complex. While recent changes to privacy settings pages at the leading social networks have been a good step forward, the usability challenge remains clear. The more privacy options available, the more difficult it becomes to design a "usable" interface.

2. Privacy policies are cumbersome and inaccessible to users

As information uses, privacy choices, and privacy controls increase in complexity, so do the length and complexity of privacy policies. Complete disclosure of all aspects of an organization's privacy commitments is a lengthy process, and the number of such aspects is only likely to grow. Yet reading and digesting long privacy policies is impracticable for the average consumer, even assuming they possess the requisite technical and legal sophistication to understand the policies. One study suggests that it would take the average American

approximately 200 hours annually to read all the privacy policies viewed during the course of each year.[29] Thus, further innovations for communicating the essential contents of privacy policies are needed. While the full details of the privacy practices of online companies need to be disclosed for examination by regulators and privacy advocates (as well as interested consumers), there should be better ways to communicate the basics of how an online entity is collecting, using, sharing, and storing data from individuals.

3. Lack of transparency and control with respect to certain tracking technologies

Traditional browser cookies are a well-known technology for which there are a variety of privacy controls built into most web browsers. Other technologies exist, however, that are used to track user activity and for which users have little or no ability to control their privacy settings. Two common examples are tracking pixels and Flash cookies.

Tracking pixels, also known as "clear GIFs" or "web beacons," are small, transparent images placed into web pages and HTML-format emails that can track when a user views the web page or opens the email that contains them. These images can be specially coded to identify users individually. It is virtually impossible for the average user to opt out of this type of tracking because, unlike with traditional browser cookies, there is no universal method to identify that an image is a tracking pixel as opposed to any other type of transparent image on a web page.[30] Transparent images are, for example, often used to ensure proper spacing and alignment. While some email software does not automatically load images, if a user wants to

---

[29] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A J. OF L. & POL'Y FOR THE INFO. SOC'Y, ISSUE 3 (2008).

[30] It is worth noting that in the absence of a persistent cookie to which to connect the fact that a page was viewed or an email was opened, tracking pixels provide limited tracking information. However, their tracking functionality remains enabled even if a user has disabled cookies.

view any of the images in HTML format the user generally must indicate that he or she wishes to view all of the images, thus triggering the tracking pixel.

Adobe Flash is a multimedia software platform compatible with many web browsers that allows the delivery of graphics, audio, video, and interactive controls not supported by traditional HTML-based web pages. Flash cookies are items in persistent storage within the local copy of the Adobe Flash Player installed in a user's web browser. They can be used to store information and track users in a manner similar to traditional browser cookies. While Adobe does provide functionality to purge one's Flash player of Flash cookies,[31] these controls are not integrated into most browsers and traditional browser privacy controls do not currently affect Flash cookies. Some companies have leveraged this gap to misuse Flash cookies and thwart the preferences of users who have intentionally deleted browser tracking cookies. The FTC has confirmed at least one active investigation of this concern.[32]

Adobe does not condone the misuse of Flash cookies in this manner and has been in discussion with browser vendors regarding developing comprehensive browser privacy controls.[33] This is an area, however, where better collaboration between the relevant companies is needed to speed progress.

---

[31] *See* Flash Player Help – Settings Manager, http://macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html (last visited June 14, 2010).

[32] *See* Wendy Davis, Flash of Criticism at FTC Privacy Roundtable (Jan. 28, 2010), http://mediapost.com/publications/?fa=Articles.showArticle&art_aid=121524.

[33] *See* Comments from Adobe Systems Incorporated – Privacy Roundtables Project No. P095416 (Jan. 27, 2010), *available at* http://ftc.gov/os/comments/privacyroundtable/544506-00085.pdf.

4. Lack of a standardized definition of "personal" or "sensitive" information and related terms

The terms "personal" and "sensitive" information appear frequently in discussions about privacy and in privacy-oriented laws such as state security breach notification statutes. There is little formal agreement, however, about what exactly constitutes the definition of "personal" or "sensitive" information. The state breach notification statutes, for example, all define such information to include at least a combination of an individual's name and at least one of their Social Security Number, Driver's License/ID number, or financial or payment card account number. However, while nearly all jurisdictions' statutes include this base set of "information pairs," many jurisdictions allow additional elements to be combined with an individual's name to constitute personal, personally identifiable, or sensitive information. Furthermore, each of these definitions involves the combination of at least two data elements – name and another item – which in itself can be confusing when trying to determine data protection obligations.

There is also substantial misunderstanding (and perhaps misuse) of the terms "anonymous" and "identifiable." This is particularly true as information systems become more advanced and the ability to "re-identify" data – that is, assign identities to otherwise anonymous elements of a dataset based other characteristics present in the dataset – evolves. A common definition of what constitutes anonymous data is necessary to improve communication with consumers and increase their understanding of privacy choices. This requirement is equally true for what constitutes identifiable data, in part because of problems of re-identification and in part because of the current lack of consensus on what constitutes personal or sensitive information.

This lack of consensus presents substantially confusing messages to consumers. Asking the average consumer to recall whether they have provided a combination of certain data

elements as part of determining whether they want to share their "personal information" is a complex question, and doing so potentially applies only in a single geographical jurisdiction or in a single industrial sector.[34] Uniform standards for personal information, sensitive information, anonymity, and related terms will help consumers better understand not only their choices, but also what a company means when it commits to "protect your personal information." The lack of a standardized definition for these terms hampers the ability of consumers and organizations to communicate about privacy issues. The issue also continues to be a source of tension between U.S. companies and international regulators, as the different methods by which search engines claim to anonymize search logs vary and have yet to satisfy many authorities in the European Union.[35]

5. The need for a plug-in to maintain a stable opt-out status

As discussed previously, some vendors have developed plug-ins to ensure that a user's decision to opt out of tracking online is maintained even after opt-out cookies expire or are cleared by the user.[36] Presently, plug-ins are the only solution that will ensure a stable opt-out status. This presents a problem for the average user who is not likely to know that a plug-in is required, particularly given the lack of transparency in how tracking technologies operate as discussed elsewhere in these Comments. Others may not wish to take the additional step of downloading a plug-in. Browser manufacturers can address this issue by using a browser header flag as an opt-out indicator, or by other methods that may be more effective. It seems clear,

---

[34] Health care information, for example, is subject to additional regulation through the Health Insurance Portability and Accountability Act, which has its own definitions of individually identifiable information and protected health information. *See* 45 C.F.R. § 160.103.

[35] *See, e.g.*, Article 29 Data Protection Working Party, EU data protection group says Google, Microsoft and Yahoo! do not comply with data protection rules (May 26, 2010), *available at* http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_26_05_10_en.pdf.

[36] *See supra* Section III.A.6.

however, that without additional efforts – such as those we suggest in Section IV of these Comments – it is unlikely that progress will come quickly in this area.

6. Increased data collection by applications

Social media platforms and smart devices have spurred the development of an amazing number and diversity of applications. Many of these are free or nominally priced. Developed by hundreds of thousands of individuals and small businesses around the world, these bits of software have added great value to the interactive environment. But, although some of these companies have grown quickly, many have little capacity to ensure the privacy or security of the data they collect. Large amounts of user data are available to these developers through integration into social networks and smart devices. Since the "app" business models are reliant on the monetization of user data, app developers are incentivized to collect as much data as possible. It is certainly clear that the incentives here should align to promote privacy and trust along with innovation and the development of new applications; it is unclear, however, whether market incentives will do so before substantial harm to consumers occurs.[37]

Privacy presents an interesting economic dilemma in that many consumers would like to have good privacy controls and many firms would like engage in good privacy practices but there is little incentive for an individual consumer or individual firm to do so. For the individual, exercising additional privacy – in the absence of good privacy practices integrated into applications – means completely abstaining from various web applications that have become integral to modern society. For the firm, integrating good privacy controls can be expensive,

[37] As noted above, these smaller actors may lack the resources to ensure the privacy and security of data they collect about users. These smaller actors, therefore, make attractive targets for identity thieves and others looking to misuse data collected about individuals.

reducing its competitiveness among competitors who spend less money on privacy or collect additional information.

7. The illusion of privacy control

Partially in response to a call by the FTC for increased self-regulation by the online advertising industry,[38] a number of companies have developed online tools to help consumers control their information. A recent study found, however, that 62% of consumers believe that the mere presence of a privacy policy alone implies certain privacy protections, such as restrictions on the sharing of data with third parties.[39]

This incorrect assumption by consumers highlights a disconnect between website users and operators regarding the effect of privacy policies and privacy controls. The mere *existence* of privacy controls may create a false illusion of privacy protections or of a user's ability to make privacy choices.[40] In fact, those protections may require the user to take additional proactive steps, or the choices a user actually wants to make may not be available. In both cases, the user may come to the incorrect conclusion because of a lack of understanding about how the privacy controls are implemented. This lack of understanding is likely at least partly a result of the complexity and lack of transparency of privacy policies. If users cannot understand the effect of privacy choices and controls, they will not be able to enact their preferences. Thus, online

---

[38] *See* FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://ftc.gov/os/2009/02/P085400behavadreport.pdf.

[39] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities That Enable It* (Sept. 29, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[40] *See, e.g.*, Laura Brandimarte, Alessandro Acquisti & George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, preliminary draft prepared for Workshop on the Economics of Information Security 2010 (Mar. 2010), *available at* http://weis2010.econinfosec.org/papers/session2/weis2010_brandimarte.pdf (draft cited with prior permission) (finding that, paradoxically, the more options for control presented to consumers, the more willing they were to share personal information even though the outcomes and risks of the sharing were the same in both cases).

companies must engage in comprehensive education and awareness campaigns to provide consumers with the understanding they need to make privacy choices online.

IV. THE ROLE OF THE DEPARTMENT OF COMMERCE IN ADVANCING ONLINE PRIVACY

The preceding discussion demonstrates that industry efforts are helping to advance online privacy while at the same time there is still work to be done to increase transparency and choice. The Department can play a leadership role to promote greater attention to online privacy by companies.

First, the Department should conduct, encourage, and fund research and other collaborative efforts to advance the evolution of technologies and practices that improve consumer transparency and choice. Second, in the forthcoming report to be issued pursuant to this *NOI*, the Department should recommend that the Administration take steps to more aggressively use existing legal tools to investigate and enforce against misuse of personal data, and to thus protect personal privacy online.

A. The Department Should Conduct, Encourage, and Fund Further Research and Other Collaborative Efforts to Advance the Evolution of Technologies and Practices that Improve Consumer Transparency and Control

One method the Department can use to promote the adoption of privacy-enhancing practices is to conduct, encourage, and fund public, private, and non-profit research that aims to improve consumer privacy. Not only would this help spur further privacy innovations, it would also signal the Department's and the Administration's commitment to the protection of consumer privacy, an increasingly relevant and mainstream issue in this country. The Department can pursue this agenda through a variety of means. Internally, the Department can conduct its own research, such as by leveraging the extensive technical competencies of the National Institute of Standards and Technology ("NIST"). Externally, the Department can fund the research of private and non-profit institutions or provide grants for start-up companies and small businesses that incorporate privacy in their business plans.

Perhaps the most effective way for the Department to encourage the development and adoption of privacy-enhancing practices is to engage in collaborative efforts with industry, advocacy groups, government agencies, and other stakeholders. For example, the Department can convene task forces that include public and private actors to focus on identifying options and solutions to contemporary privacy issues, directly fund Centers of Excellence to conduct research in partnership with industry and academia, and host or participate in symposia and other programs that focus specifically on the areas where a log-jam needs to be broken. The increased cooperation and free flow of ideas resulting from these collaborations can contribute substantially to the development and implementation of privacy practices that benefit consumers.

The Department should focus these efforts on developing privacy-enhancing technologies, developing privacy-enhancing business practices, and standardizing the definitions of "personal" and "sensitive" information and related terms.

1. Developing privacy-enhancing technologies

As described in Section III.A, great strides have been made in developing privacy-enhancing technologies to increase consumer comprehension of how their information is used online and what their privacy options are. Despite their success, however, these technologies only represent preliminary steps in the "featurization" of data use – that is, the full integration of meaningful, understandable privacy notices into online applications and features.[41] In this regard, the demonstrated use of advanced disclosures to better present notice and choice, such as through the use of the Power I icon, is progress but not the end goal. "Evolving" these methods of notice

[41] One proposal for such featurization is the "use-based" model of privacy mentioned in the *NOI*, which would define the types of uses for which advertisers could employ personal information as opposed to regulating what personal information can be collected. *NOI* at 21,229. FPF recommends that the Department *not* settle on any one model of privacy at this point, instead supporting research about multiple models to ensure that it considers all viable options. Proceeding in this fashion will also help ensure the robustness of the model ultimately chosen.

provides the best opportunity to increase consumer transparency and choice, and to consequently develop consumer trust for the future. To that end, the Department should seek to focus further research on the development of evolving privacy-enhancing technologies designed to ensure consumer transparency and choice regarding the online use of their information, building upon the developments already achieved in this field.

One area on which the Department can focus is the development of identity management solutions. As noted in the *NOI*, the Federal Communications Commission's National Broadband Plan recommended developing identity management solutions to assist consumers in managing their data.[42] Online businesses that collect large amounts of personal information from users, such as social networking websites, have also introduced applications and settings that allow users to exercise a certain level of control over their online identities. Recent research has also attempted to explore the feasibility of enacting identity management solutions and the attendant risks to privacy.[43]

At this time when both government agencies and industry are experimenting with these identity management solutions, we are at a critical turning point. Identity controls can either be an enabler of privacy advances, providing both additional value and greater user control over data, or if done improperly can provide a grave threat to users' control over their information.[44] At the same time, there is relatively little known about the effectiveness of available identity management solutions, and what aspects of these solutions are best at enhancing consumer privacy while still maintaining value for business. Therefore, the Department should consider

---

[42] *NOI* at 21,231.

[43] *See, e.g.*, Susan Landau et al., *Achieving Privacy in a Federated Identity Management System*, Financial Cryptography & Data Security '09, *available at* http://labs.oracle.com/people/slandau/Achieving_Privacy.pdf.

[44] *See, e.g.*, *supra* Section III.B.7 on the "Illusion of Control."

sponsoring research or convening a task force that examines recent progress in the development of identity management systems and their benefits to consumers, their effect on the online advertising ecosystem, and their effect on data sharing and personalization business models.

2. Developing privacy-enhancing business practices

Many companies fail to commit the resources necessary to ensure online privacy protection. This is often because privacy is an afterthought that follows, rather than is part of, the development of new online products, services, and technologies. To ensure that proper attention is given to privacy, companies must embrace the concept of "Privacy by Design" – considering privacy at every step of the research and development process.[45] The Department should promote "Privacy by Design" as a fundamental for companies engaged in online activities.

3. Standardizing the definitions of "personal" and "sensitive" information and related terms

As discussed in Section III.B.4, the lack of standardized definitions for "personal information," "sensitive information," "anonymous," and "identifiable" presents several privacy challenges. Varying definitions increase consumer confusion and make it more difficult for data custodians to understand and comply with their data protection obligations. These differences also make it more difficult for website operators and applications developers to communicate privacy choices to users. The development of uniform definitions and standards for the usage of these terms can help consumers better understand their privacy options and make informed decisions. The Department, leveraging the competencies of NIST, should sponsor research or support a task force to develop such uniform definitions and use standards. These should include,

[45] A proponent of such a system is the Privacy Commissioner of Ontario, Dr. Ann Cavoukian, who developed a Privacy by Design framework that provides a set of guiding principles encouraging information system owners to proactively and pervasively incorporate privacy protections into the design of their systems. *See* Privacy by Design, http://privacybydesign.ca (last visited June 14, 2010).

at a minimum, definitions for the terms "personal information," "sensitive information," "anonymous," and "identifiable." The Department should also recommend to the Administration that it undertake efforts to promote the adoption of uniform definitions and use standards for these terms.

B. The Department Should Recommend that the Administration Take Steps to More Aggressively Use Existing Legal Tools to Investigate and Enforce Against the Misuse of Personal Data

FPF recommends that the Department, in its forthcoming Report,[46] recommend that the existing legal tools available at the federal level be more aggressively used to investigate and enforce against the misuse of personal data. In addition to the civil authority vested in administrative and independent agencies, the Department of Justice has authority to proceed against criminals involved in spam, spyware, phishing, identity theft, malware, and "malvertising," though enforcement against these crimes has not been as robust as it can be.[47]

For example, malvertising occurs when criminal groups purchase banner ads from unsuspecting ad networks and implant malware in the computer code displaying the ads, after which the ads attack the computers of those who simply view the banners. Despite having an impact that has affected millions of users and thousands of networks, civil enforcement and industry self-regulatory or individual company measures have been unable to respond sufficiently to this concern, due to the need for coordination across many industries and business models.

---

[46] *See NOI* at 21,226.

[47] These are, of course, not the only crimes committed over the Internet. But by addressing these cybercrimes used to perpetrate fraud against consumers online, the Department could provide the needed impetus to convene the key actors needed to advance solutions to these problems before they undermine consumer confidence in using the Internet and slow the growth of electronic commerce.

While improvement in online privacy practices by legitimate companies will go far to build consumer confidence and thus help ensure the continued growth of online commerce so essential to the country's economic well-being, more robust law enforcement against illegal online conduct such as malvertising also must play a critical role in making the Internet a safe place for consumers to share data.

C. The Department Could Play a Unique Role in Supporting the Role of Chief Privacy Officer

Over the past decade, the role of Chief Privacy Officer has become a critical one for thousands of businesses seeking to ensure and enhance their data practices. Information about this role in the U.S. job market is limited to occasional surveys by the International Association of Privacy Professionals or the Ponemon Institute.[48] The Department could play a key role in identifying the numbers of such professionals across various industry sectors and could help advance the importance of this job function as a central way for companies to advance their data protection practices.

[48] *See, e.g.*, INT'L ASS'N OF PRIVACY PROF'LS, A CALL FOR AGILITY: THE NEXT-GENERATION PRIVACY PROFESSIONAL (2010), *available at* http://privacyassociation.org/images/uploads/IAPP%20Future%20of%20Privacy_Final%20Client.pdf; PONEMON INSTITUTE, PRIVACY & DATA PROTECTION PRACTICES: BENCHMARK STUDY OF THE FINANCIAL SERVICES INDUSTRY (2010), *available at* http://offers.compuware.com/register?cid=70170000000J6xN.

V. CONCLUSION

FPF commends the Department for its examination of online privacy and looks forward to further participation in the public-private dialogue about ways to improve privacy protections for Americans. We hope that the foregoing illumination of innovative practices and areas for improvement, as well as our recommendations for further Department engagement, are a useful contribution.

June 14, 2010

Respectfully submitted,

_____

Christopher Wolf
Co-Chair, The Future of Privacy Forum
Bret Cohen
HOGAN LOVELLS US LLP
555 13th Street NW
Washington, DC 20004
202-637-8834
202-637-5910 (fax)
christopher.wolf@hoganlovells.com
Counsel for THE FUTURE OF PRIVACY FORUM

Jules Polonetsky
Co-Chair and Director, The Future of Privacy Forum
919 18th Street NW
Washington, DC 20036
202-713-9466
julespol@futureofprivacy.org