From: Lee Tien, Electronic Frontier Foundation Nov. 9, 2009
To: Federal Trade Commission
Re: Privacy Roundtables – Comment, Project No. P095416

Introduction

The Electronic Frontier Foundation (EFF) submits these comments for the Commission's Dec. 7, 2009 privacy roundtable. Our main, overarching point is that society recognizes a basic "interest in avoiding disclosure of personal matters" and "in independence in making certain kinds of important decisions," *Whalen v. Roe*, 429 U.S. 589, 598-600 (1977), which should not be conceptualized solely in terms of possible concrete harms such as identity theft, discrimination, social stigma, or other adverse consequences. For example, the law recognizes that having one's private communications intercepted is a privacy violation even if nothing untoward results from the interception.

Privacy has always been closely linked to notions of dignity and respect. As the sociologist Erving Goffman wrote: "The practice of reserving something of oneself from the clutch of an institution . . . is not an incidental mechanism of defense but rather an essential constituent of the self."[1]

Furthermore, we would not limit this interest to individuals: families or households, as well as groups, are also proper subjects of privacy. After all, in many homes all family members use one computer to access the Internet. It would be wrong to think only of each family member's interest; the family as a whole has a distinct privacy interest. Similarly, a household's communication records (such as "call detail records") are not merely about the individuals in the household, but also about the life of the household as a group or community. Location tracking sharpens the point: that two cellphones travel together and then separate every weekday morning says something not just about the individual phones but about the relationship between the two individuals that possess them.

A third global point is that while the Commission's stated area of inquiry is *consumer* privacy, suggesting that the relevant risks are associated with the actions of private businesses, EFF believes that it is essential to recognize that government collection and use of data is a concern inextricably linked to consumer privacy. Law-enforcement or intelligence agencies have easy yet seemingly unaccountable access to business records and commercial databases via a wide range of tools such as subpoenas, national security letters, or even simple commercial subscriptions. Leakage of personal information must

[1] Goffman, ASYLUMS 319 (1961); see also White, *The Fourth Amendment as a Way of Talking About People*, 1974 Supreme Ct. Rev. 165, 167, 217 ("[T]he decision of a Fourth Amendment case is a point at which a judgment is made about how people will be talked about in our public world. . . . [T]he Court . . . writes a drama, as it were, of public significance. . . . In what language are the interests or values protected by the Fourth Amendment to be stated? What notions of security or privacy or property or autonomy are to be employed, and how are they to be given meaning? . . . What shall be the treatment of arrangements made by the individual with others, parcelling out, sharing, and qualifying whatever it is that is the object of Fourth Amendment protection?").

be thought of in terms of governmental, as well as commercial, use: there is a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[2]

Finally, we note that the technological and organizational complexity of the modern social landscape makes it harder to hold individual actors accountable. The problem goes beyond the fact that data flows are difficult for the consumer to map and follow. In the online context, privacy-insensitive infrastructural elements like web protocols that expose user information by default have become useful for tracking and data collection purposes, whether or not those purposes were intended by the original designers. In the telecommunications context, network design mandates for law enforcement surveillance have apparently contributed to the growth of an industry devoted to equipment for "deep packet inspection." In short, modern privacy-invasive practices are often built on yesterday's technologies, exploiting privacy weaknesses perhaps only dimly seen before, but which become much clearer in hindsight.

Agent-specific risks and concerns

Whether the proper subject of privacy is an individual or a group, there are several types of risks. First is the fundamental concern that others have learned something that the person or group did not intend to disclose.

More standard concerns can flow from such disclosure, collection, dissemination and use. Intrusions like spam and telemarketing calls may arise purely from the leakage of access information, such as email address and phone number. Unwanted attention can also arise from targeting based on interests or attributes. Harm can arise here whether or not the information is actually true: an erroneous inference can have serious consequences. Leakage of particular types of information, or inferences based on them—religious and political beliefs, sexual orientation, reproductive status, mental health, genetic data, and so on—can lead to stigmatization or other adverse consequences, whether the loss of a benefit or job, the imposition of a sanction, or simply needing to explain oneself.

Risks to freedom of speech and association are also common in this context. The First Amendment protects anonymous speech and association. "[A]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind."[3] The privacy of reading and viewing records is well established by the many state laws protecting library records as well as federal laws protecting video rental records and cable TV viewing records.

First Amendment law also recognizes that threats to privacy or anonymity in the speech or associational context create "chilling effects," which can be thought of as reactive harms flowing from the anticipation of adverse consequences. Persons might refrain from legitimate behavior in the first place, or they might feel it necessary to take excessive precautions to protect their privacy and anonymity.

---

[2] *Whalen*, 429 U.S. at 605.
[3] *Talley v. California*, 362 U.S. 60, 64 (1960)

Societal risks

There are also risks and concerns at a societal level. An obvious concern is the existence of many large private and public databases of personal information, which create a risk of aggregation or informational connectedness.

Goffman noted that "every time an individual joins an organization or a community, there is a marked change in the structure of knowledge about him — its distribution and character — and hence a change in the contingencies of information control. . . . An individual, then, may be seen as the central point in a distribution of persons who either merely know about him or know him personally, all of whom may have somewhat different amounts of information concerning him."[4]

The Supreme Court has recognized that aggregation creates privacy threats. "In an organized society, there are few facts that are not at one time or another divulged to another. . . . Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[5]

Quite apart from the aggregation risk, any of these databases might be accessed or stolen by hackers and used for purposes such as identity theft, physical theft[6], or even spying by foreign nations. Although the probability of any given database being stolen at any time may be low, it only takes one hacking incident to create a massive data leak affecting millions of people. Current laws such as the REAL ID Act, aimed at creating a vast national ID system, only exacerbate these risks.

Here again, the risks have a broader aspect. For a given subject, whether individual or group, dataveillance reveals not only simple facts but also behavior patterns that the subject may not even be aware of. And as more persons and groups are dataveilled, even larger behavior patterns are revealed.[7]

In short, the combination of online behavioral tracking, offline data aggregation, and routine social surveillance such as the increased deployment of videosurveillance,

---

[4] Goffman, STIGMA: NOTES ON THE MANAGEMENT OF SPOILED IDENTITY 67, 72 (1963).

[5] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763-764 (1989); id. at 763 n. 14 ("[m]eaningful discussion of privacy . . . requires the recognition that ordinarily we deal not with an interest in total nondisclosure but with an interest in selective disclosure.") (quoting Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 Law & Contemp. Prob. 342, 343-344 (1966)).

[6] There are documented instances of burglars using public data on Facebook to target victims: http://mashable.com/2009/08/27/facebook-burglary/. But such threats could apply equally to people who do not use Facebook but are tracked by other, less voluntary, behavioral systems.

[7] Carter Jernigan and Behram F.T. Mistree, *Gaydar: Facebook friendships expose sexual orientation*, 14 First Monday, *at* http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302

wireless/cellular, transponder and other tracking technologies is generating a surveillance infrastructure that is bad for civic hygiene in two ways.

First, widespread routine surveillance threatens our social privacy norms, which evolve from our social expectations and practices. Legitimizing routine online behavioral surveillance may, over time, lead Americans to either accept or acquiesce in more surveillance. While it is difficult to quantify this risk, it should be recognized.

Second, our surveillance practices can pose a risk to other societies. The 1994 Communications Assistance to Law Enforcement Act, for example, required U.S. telecommunications carriers to ensure law enforcement access to digital communications; partly as a result, telecommunications vendors around the world now design their equipment with "lawful intercept" capabilities that repressive governments can use to surveil political, religious and cultural dissidents.[8]

Consumer expectations

Research into Americans' attitudes toward consumer privacy highlights two key points: Americans value their privacy, but are poorly informed about both the law and actual information practices. Neither point is surprising.

Consumer information has been a part of marketing for a long time. But while one-way mass media sought to create attention, interest, desire and action, the ability to observe consumers was more or less limited to actual purchase behavior, augmented by coupons and loyalty card programs. The rise of interactive media has led to enormous differences in the kinds of information available to marketers. As a result, we need to ask whether consumers understand that they are being tracked, how they are being tracked, what information about them is being collected and stored, who has access to or receives that information (or derived data like profiles), how that information is actually used, and of course, how they can avoid being tracked.

Consumers value their privacy

Recent research strongly indicates that consumers strongly value their privacy. Researchers at the University of Pennsylvania and the University of California-Berkeley[9] found that:

> • 69% of American adults thought that the law should give them the right to know everything that a website knows about them.[10]

[8] Danny O'Brien, EFF International Outreach Coordinator, *Learning from Tehran and Urumqi*, San Francisco Chronicle (July 22, 2009), at http://sfgate.com/cgi-bin?f=/c/a/2009/07/22/EF3E18SLV9.DTL
[9] Univ. of Penn., Univ. of Cal. at Berkeley, *Americans Reject Tailored Advertising and Three Activities that Enable It*(2009),*t* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.
[10] Id. at 3.

• 92% thought that the law should require websites and advertising companies to delete all stored information about them, if asked to do so.[11]

• 63% thought that the law should require advertisers to immediately delete information about their Internet activity.[12]

Perhaps most important, the vast majority of the surveyed consumers rejected the very notion of online tracking, even when told that such tracking would be anonymous: 68% said they "definitely" would not allow it, and 19% said they "probably" would not allow it.[13]

The researchers thus suggested:

"The rejection of even anonymous behavioral targeting by large proportions of Americans may mean that they do not believe that data about them will remain disconnected from their personally identifiable information. It may also mean that anonymity is not the only worry they have about the process. Being labeled in ways they consider unfair by marketers online and off may be just as important a concern…. *Americans are worried about others' use of data about them in ways they do not know or understand, and might not like*."[14]

These concerns are echoed to some extent by another recent study comparing Internet users' attitudes toward privacy between 2002 and 2008.[15]

• "the 2008 respondents are more concerned about disclosures of their purchasing patterns than the 2002 respondents," and "more concerned about the trading/selling of Personally Identifiable Information (PII) to third parties"[16]

• "the 2008 respondents are more concerned about websites recording information regarding previously visited web sites"[17]

• "The 2008 respondents are more concerned about their browsing experiences being customized in general [] and their purchasing patterns being monitored [].

---

[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] Id. at 4-5 (emphasis added). Some have argued that concerns about price discrimination underlie many consumers' privacy concerns. Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet* (2004), http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf.
[15] Anton et al, *How Internet Users' Privacy Concerns Have Evolved Since 2002*, N.C. State University Computer Science Technical Report # TR-2009-16 (2009), http://theprivacyplace.org/blog/wp-content/uploads/2009/07/tr_2009_16.pdf. The study notes that "in 2002, the only online activity in which over 40% of respondents were engaged in was product purchasing. In contrast, in 2008, education, financial services, product purchasing, and research were all activities for over 70% of the respondents." Id. at 5.
[16] Id. at 5.
[17] Ibid.

> In addition, the respondents are more concerned about their PII being used for marketing or research activities"[18]

According to the authors, the "2008 survey results suggest that individuals are more uncomfortable with companies, such as data brokers and credit bureaus, trading/sharing/selling PII with the companies with which they engage in business,"[19] and "reveal an increase in individuals' level of concern about information collection, specifically with regard to websites collecting information about previously visited websites."[20] The authors concluded that "[s]ince the 2002 survey, individuals have become more concerned about personalization with regard to customized browsing experiences, monitored purchasing patterns, and targeted marketing and research."[21]

Consumers do not understand the limits of legal protection

The 2009 Pennsylvania-Berkeley study also showed that Americans believe they have more legal protection for their privacy than they actually have. "Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them. When asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assume government regulations prohibit the sale of data."[22]

These findings are consistent with the 2008 Hoofnagle-King study of Californians' understanding of business practices with respect to the selling of personal information in nine different contexts.[23] "In six of those contexts (pizza delivery, donations to charities, product warranties, product rebates, phone numbers collected at the register, and catalog sales), a majority either didn't know or falsely believed that opt-in rules protected their personal information from being sold to others. In one context—grocery store club cards—a majority did not know or thought information could be sold when California law prohibited the sale. Only in two contexts—newspaper and magazine subscriptions and sweepstakes competitions—did our sample of Californians understand that personal information collected by a company could be sold to others."[24]

These findings are also consistent with older research finding that "in general, consumers are not at all aware of the facts regarding privacy in industries with which they deal on a regular basis."[25] Focus group research indicated that many consumers did not realize that: life insurance underwriting might include the ordering of a credit report; employee health

---

[18] Ibid.
[19] Ibid.
[20] Id. at 6.
[21] Ibid.
[22] Penn-Berkeley study at 2.
[23] Hoofnagle & King, *Research Report: What Californians Understand About Privacy Offline* (2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075.
[24] Id. at 2.
[25] H. Jeff Smith, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 146-147 (1994).

insurance claims were shared with employers (many believed that claim information was completely confidential and never revealed to employers at all); credit card issuers sometimes use information about their purchases to place cardholders in psychographic categories; banks use information from loan applications to target their marketing activities.

The relevance of consumer expectations

Industry is typically skeptical of such attitudinal studies, often arguing that consumer actions contradict their professed desire for privacy. But if consumers do not actually know that their actions reveal information or that the law permits their information to be disseminated, the contradiction vanishes.

We therefore contend that consumer expectations are relevant but must be viewed in terms of consumer knowledge. Several factors come into play here.

First and foremost, privacy harms are hard to detect. When a person is harmed by a merchant -- goods are defective, service is delayed or denied, and so on -- he or she usually knows that he or she has been harmed, who is responsible, what was lost, how much it cost, and so on.

Harms to privacy are usually different. It is easy to gather information about a person covertly through various forms of surveillance. A person may be induced to provide personally identifiable information (PII) through seemingly innocuous acts. Most people probably do not think about privacy when a website offers weather forecasts based on zip code, and horoscopes based on one's birth date and gender. Yet combining these simple facts -- gender, birth date and zip code -- is a powerful way to identify and "profile" a person, given the wealth of available demographic data.[26] Finally, one may have no real choice but to provide PII. If a person wants to rent an apartment or open a bank account, he or she is unlikely to refuse to provide personal information to obtain those necessities.

After the initial data collection, the unauthorized use, disclosure, or exchange of PII often occurs "behind the scenes." The ordinary consumer has no way of knowing that a company uses his or her PII for an unauthorized purpose or shares it with a business partner. Often, a person only realizes that his or her PII has been "shared," "leaked" or "stolen" when he or she receives junk mail or discovers unauthorized card charges or credit problems.

Another problem is identifying who is responsible for the harm. If a new car breaks down for no obvious reason, there is a clear target: the car dealer. Privacy harms are different. Once a person discovers that she is a victim of ID theft, she is still unlikely to know who is responsible for the violation. The "thief" may be impossible to find. And some other entity may also have been at fault in not safeguarding the information. Was it a bank or an insurance company? How would a person know?

---

[26] L. Sweeney, *Uniqueness of Simple Demographics in the U.S. Population*, LIDAPWP4. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA: 2000.

Third, neither businesses nor government entities have strong incentives to address privacy issues. California's pioneering notice of security breach law, for example, exposed poor security practices that had been concealed for years.[27] Especially after 9/11, incentives favor "knowing your customer." Perhaps more to the point, the consumer perceives the loss of control over PII as a harm, while business and government perceive it as a benefit.

All of these problems are exacerbated by the complexity of online technologies and of the arrangements among online players. Most consumers, we suspect, have little understanding of what kind of data is available, and to whom, when they use the Web.

By now, many Web users are aware of the simple and ubiquitous HTTP cookie. But they are probably less aware of web bugs, HTTP referrer data, and browser metadata. Moreover, a recent paper shows that due to the appearance of several kinds of "supercookies," even cookie management tools have become completely ineffective in many instances.[28]

One such supercookie is the "Adobe Flash cookie." These files are stored on a user's hard drive outside of the browser's normal control mechanisms and never expire. Thus, users are not notified when flash cookies are set, and cannot use their web browsers to view or delete flash cookies.[29] Equally important, flash cookies rely on Adobe's Flash plug-in; partly because the code is proprietary, third-party developers have been slow to develop flash cookie management tools. And, as we note below, businesses use flash cookies to circumvent user attempts to prevent being tracked.

Adequacy of existing law/self-regulation and technological innovation

Existing U.S. legal and self-regulatory regimes do not adequately protect consumer privacy today, for a variety of reasons. Many have observed that U.S. privacy law is an uneven patchwork quilt that is designed more for lawyers than consumers, and we will not dwell on this point. Nor will we discuss the myriad problems presented by large data brokers that aggregate vast amounts of personal information about consumers.

One of the main problems is that, as discussed above, privacy violations are difficult to detect and trace. Moreover, private rights of action often require a showing of concrete harm to identifiable persons. As a result, there is likely to be insufficient private litigation, despite its importance in a healthy regulatory system.

This problem is exacerbated by organizational complexity: while consumers may know the businesses they patronize, or the websites they visit, they are unlikely to know what other entities have access to their data. For instance, the vast number of entities in the

---

[27] Anton et al, at 2-3.
[28] See generally McKinley, *Cleaning Up After Cookies (Version 1.0)* (2008), https://www.isecpartners.com/files/iSEC_Cleaning_Up_After_Cookies.pdf.
[29] Id. at 5-6.

health care industry, from HIPAA covered entities to their many business associates, is breathtaking. The average consumer is simply in no position to understand the flows of health information or to know the contractual provisions that govern the flow of information between covered entities and their business associates. Similarly, many websites' privacy policies contain disclaimers saying that the policy applies only to the website, and not to its advertisers, when it is those third-party tracking/advertising firms that engage in the most problematic practices.

Moreover, the law suffers from technological obsolescence. Telecommunications privacy law provides some examples. The common search engine, for instance, does not fit cleanly into the Electronic Communications Privacy Act's concepts of "electronic communications service provider" or "remote computing service provider." Social networking sites like Facebook and MySpace likewise provide services that do not neatly fit these statutory definitions. Furthermore, such sites are under increasing pressure to offer their users sophisticated "internal" privacy settings, controlling which other users have the ability to access various parts of their profile data. But federal law lacks any kinds of mechanisms to reinforce these statements by individuals that they expect certain data to be kept private.[30]

Similarly, the law surrounding location data is unclear. EFF has been involved in several cases involving law enforcement access to location data collected or stored by wireless carriers, and no clear legal standard has emerged even though location data is protected under the Telecommunications Act, the Wiretap Act and the Stored Communications Act.[31] Matters become even more complicated with location-based services on mobile devices and RFID. Such issues will only become more obvious with public-sector tracking devices, such as common EZ-Pass and FasTrak transponders, and trends toward location monitoring in "pay-as-you-drive" insurance and congestion pricing schemes.[32]

The unsettled state of the law is also evident in two other areas: "smart grids" and biometrics. Smart grids and smart meters are likely to expose enormous amounts of information about household behavior to utilities that historically have had little need to think about privacy issues.[33] Biometrics exploits the general lack of privacy surrounding physical data we normally cannot help but present to the world, such as face, fingerprint, or DNA, some of which we have routinely used for identification purposes.[34] Today, the technologically enhancements surrounding these kinds of data raises significant privacy issues.[35]

---

[30] See generally World Privacy Forum, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* (2009), http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.
[31] See http://www.eff.org/issues/cell-tracking.
[32] See http://www.eff.org/wp/locational-privacy.
[33] See, e.g., Quinn, *Privacy and the New Energy Infrastructure* (2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731; Lyon, *Privacy Challenges Could Stall Smart Grid* (2009), http://featured.matternetwork.com/2009/6/privacy-challenges-could-stall-smart.cfm
[34] See http://www.eff.org/wp/biometrics-whos-watching-you
[35] Baker, Associated Press, *FBI uses facial-recognition technology on DMV photos* (Oct. 13, 2009), http://www.usatoday.com/tech/news/2009-10-13-fbi-dmv-facial-recognition_N.htm

Finally, the Commission asks: What are the costs, benefits, and feasibility of technological innovations, such as browser-based controls, that enable consumers to exercise control over information collection?

There have been many efforts to build browser-based controls to improve citizens' privacy on the web. These include the inclusion of extensive privacy, security, cookie management and "incognito mode" features into modern browsers, such as Internet Explorer 8, Firefox 3 and Google Chrome. They also include a range of optional or browser extension technologies including the "Targeted Advertising Cookie Opt" (TACO) plug-in, AdBlock Plus, CustomizeGoogle, NoScript, RequestPolicy, and Tor.

While such efforts are somewhat encouraging, several overarching problems remain:

Users who are concerned about privacy and take reasonable steps to configure their browser to protect privacy are unlikely to succeed in avoiding tracking and profiling. For instance, users who limit cookie retention in their browsers will be tracked by one of the five kinds of "supercookies" that do not respect ordinary browser cookie settings.[36] Very diligent users who succeed in learning about and blocking supercookies will be tracked by a combination of IP addresses and User-Agent data.

Only extremely sophisticated users have much chance of browsing the web in genuine privacy. Furthermore, those users will have to undergo a great deal of inconvenience in order to do so: they will have to use tools like Tor that slow browsing down, and they will have to use tools like RequestPolicy, NoScript and site-by-site cookie approval that require manual approval and disapproval of numerous web features in order to ensure that various sites remain accessible.

We do not expect that more than a tiny fraction of users will acquire the knowledge and make the sacrifices necessary to achieve protection this way. Indeed, the developers of sophisticated privacy software like Tor are careful to provide explicit cautions and disclaimers about the software's ability to protect users.[37]

At the moment, there is little reason for optimism that authors of privacy software will be able to outstrip the demonstrated efforts of tracking companies to find and deploy new tracking techniques.[38] Even when privacy software does actually work, there is little reason to expect that ordinary, privacy-concerned users will find the tools that actually work instead of those that merely seem to, or be able to browse the Web with the extra effort and inconvenience required by genuinely effective privacy tools.

---

[36] See http://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide

[37] See https://www.torproject.org/download.html.en#Warning.

[38] Recent research -- Soltani et al, *Flash Cookies and Privacy* (2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862 – has shown that flash cookies are often used to *deliberately* circumvent users' HTTP cookie policies. A site may intentionally store the same information in both HTTP cookie and flash cookie forms. The logical conclusion is that site operators know many users do not want to be tracked with cookies, but ignore those users' privacy preferences by developing more subtle and surreptitious tracking techniques.

A recent study shows that online practices are making it easier to link online tracking data to real-world identities if you use online social networks like LinkedIn, MySpace and Facebook.[39] When you log onto one of these sites, the social network includes advertising and tracking code so that selected third parties can see which account is yours and then add the contents of your profile page to their file. Indeed, the researchers were surprised to discover that some social networks were essentially violating the "same-origin" cookie principle by aliasing third-party tracking servers into the host site's domain name, enabling the third party to see cookies set by the host site.

Thus, the general problem is not merely consumer ignorance or the unavailability of tools, but companies' active efforts to track consumers regardless of the precautions they take.

Finally, we fear that user control tools may not be a scalable solution. Google's Ad Preferences Manager, for instance, is a recent and laudable attempt to allow users more granular control over behavioral tracking (interest-based advertising, in Google's terms). But does that approach really scale given the size of the behavioral advertising industry? Akamai, specificmedia, Omniture, Mediaplex, AdBrite, quantcast, Microsoft Advertising, Consumer Track, hitwise, and pulse360 are only some of the companies involved. Increasing granularity creates more preference management overhead. If each company were to emulate Google and implement a preference manager, it would be unrealistic to expect consumers to shoulder this burden for each ad network. Whether some sort of meta-tool could be developed for users to manage all of their preferences is unclear; the trajectory might point to some form of "do not track" list.

Respectfully submitted,
Lee Tien
Senior staff attorney
Electronic Frontier Foundation

[39] Krishnamurthy & Willis, *On the Leakage of Personally Identifiable Information Via Online Social Networks* (2009), http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf.