BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Berkeley Center for
Law & Technology

Chris Jay Hoofnagle
Lecturer in Residence
University of California, Berkeley
School of Law

April 14, 2010

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20001

Re: Roundtables - Comment, Project No. P095416

Dear Commissioners,

Thank you for soliciting comment upon the FTC Privacy Roundtable Series. The Roundtables were an excellent opportunity for the Commission to refocus upon the privacy risks of online profiling.

The 1996 Staff Report

The Commission has been building a strong record on this issue since its 1996 Staff Report. In a large sense, the issues have remained the same: companies can track users over time for various purposes. Another aspect hasn't changed, and yet we seem to be unable to learn it: just like in 1996, today advocates of self-regulation have proposed narrow, vague, unenforceable, and often pointless interventions in place of substantive rights and responsibilities in this area. Many of the entities discussed in the 1996 report disappeared shortly after that event, and others effectively stopped operating after the regulatory spotlight moved onto other subjects.

The impermanence of self-regulatory groups is a major problem. What regulatory approach will encourage a persistent revisiting and revaluation of self-regulatory approaches? How can we ensure that self-regulatory groups don't just disappear (like IRSG did) or functionally dissolve (like NAI)[1] shortly after regulatory pressure subsides?

The failure of the market for PETs is also problematic. The 1996 Report featured technologies such as PICS and Universal Registration Systems. But the lawyers stood in the way of these technologies, particularly P3P, in part because they required the company to state in a binary fashion how they were going to use data. How can we have a market for privacy when many market participants simply refuse to clearly say what they are going to do with data?

Is "Trust" Part of the Problem?

The FTC created an atmosphere in the 1990s that fostered the adoption of privacy policies. Now it is time for a more difficult task: replacing formalism with privacy substance. Standing in the way of this is "trust."

[1] As of this writing, I cannot find the 2000 NAI Principles on the NAI website. This underscores the procedural problem with some self-regulatory groups. They cannot even perform the basic function of being a repository for their own documents! See http://www.irsg.org/ for a similar situation.

Currently, there is no market for substantive guarantees in privacy policies—consumers misunderstand their very purpose. They think all privacy policies require a commitment to strict rules and responsibilities. After all, it is a *privacy policy*, not a sharing policy, or an information reuse policy. This gulf between consumers and actual practices is distorting the market for privacy protection.

This lack of competition for privacy substance creates disincentives for good actors. Some companies are using "trust" as a proxy for responsible information practice while competitors implement better privacy practices. That is, they link brand identity and quality to privacy issues such that a good brand is equated with substantive privacy policies and procedures. Larry Ponemon's annual report on the most trusted companies[2] is an excellent articulation of this problem. Some companies on it have had major privacy debacles; in others, consumers are clearly confusing good service with good privacy practices.

To align users' expectations with practices, the FTC should find ways to encourage privacy competition, instead of reputation competition. We have a market that produces privacy lemons because consumers have no way of evaluating privacy meaningfully and companies are not rewarded for good privacy interventions. In fact, increasingly, they are experiencing "blow*forward*" instead of blowback when introducing new services that are transgressive.

In the search log retention field, the FTC could create a race to the top by policing terms like "anonymization." Reasonable consumers would reasonably assume that anonymization means that the data collector is using robust procedures to deidentify data. Until this term is policed, some companies will use the term to describe inadequate practices, while good companies that invest in real anonymization will get no benefit from their efforts.

Collection Limitation

Many participants at the Roundtables expressed support for a use-based privacy law, one that had no limitations upon collection of data. I suggest that this would be a very problematic approach.

First, even use-based laws have aspects that function as limits on collection. For instance, the FCRA's requirement that consumer reporting agencies maintain "maximum possible accuracy" operates as a collection limitation, because some information that was reported prior to the passage of the FCRA, such as whether a person keeps a clean home or is homosexual, is essentially unverifiable. As I understand it, the proposals made at the Roundtable would allow companies to collect any type of information, even if it is inherently unverifiable.

Second, without some collection limitation, abuses practices would abound. Spyware would be legal. Tricking individuals into revealing information would be legal. Pretexting would be legal.

Third, self-regulatory groups have already promised to avoid health information and other "sensitive" information. A solely use based law could obviate these promises, and represent a step backward.

Fourth, without collection limitation, controversial secondary uses become impossible to avoid. Once an organization has personal data and is presented with the opportunity to increase advertising ROI, secondary uses will be adopted.

[2] Ponemon Institute, Ponemon Survey Names Twenty Most Trusted Companies for Privacy, Feb. 26, 2010, available at http://www.ponemon.org/news-2/26

The First/Third Party Distinction and Retention

The first/third party distinction, so prevalent in privacy laws, needs to be rethought. This distinction is intuitively appealing. However, concentration in search and information-intensive companies have made first parties the modern privacy risk.

We need to consider creating a ceiling to limit how long first parties can retain personal information. A ceiling on retention could create a level playing field for competitors and reduce the civil liberties risk associated with online profiling. Some say that a retention approach will be ineffective—companies will simply create a "shadow" profile of users. However, even a shadow profile would be less privacy invasive than a complete click stream record of individuals' actions.

Most importantly, a retention limit would shift the burden away from consumers, who must now navigate a faulty opt out process that does nothing to address the underlying privacy issue present in online profiling. That is, even if one opts out of online profiling, one is still tracked.

Access and Deletion

In 2009, we asked consumers, "Do you think there should be a law that gives people the right to know everything that a website knows about them, or do you feel such a law is not necessary?" 69 percent desired such a law.[3] When segmenting this issue based on age, we found that Americans of all ages were similar in their support for a right to access.[4]

A number of individuals at the Roundtables invoked access as a right that could ensure that companies engaged in more responsible information practices. Access has played a central role in the FCRA. It remains to be seen whether consumers will, in large numbers, make access requests for data concerning online advertising and other non-credit-reporting issues.

The FTC could attain many of the benefits of an access mandate by creating an access or delete option. That is, a company could choose to either create a system to give users access to a broad range of data about the consumer, or the company could choose to forgo creating such a system, and guarantee that the company will delete information about the customer from its databases upon request. California's SB27 creates a similar either/or option: Californians can obtain a list of third party information sharing partners of a company, or if the company wishes to not disclose such a list, the company must opt the consumer out of third party sharing.

There is stronger support for a right to delete among American internet users. We found in 2009 that 92 percent supported the creation of "a law that requires websites and advertising companies to delete all stored information about an individual, if requested to do so."[5] As with the access issue, consumers of all ages support a right to delete.[6]

---

[3] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, SSRN ELIBRARY (2009), http://ssrn.com/paper=1478214.
[4] Chris Jay Hoofnagle et al., How Different Are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?, SSRN eLibrary (April 14, 2010), available at http://ssrn.com.
[5] Id. at Fn. 3.
[6] Id. at Fn. 4.

Enhancement

The FTC has yet to bring a case involving enhancement, the practice of buying additional data to supplement personal information shared by the consumer. This practice violates the principle that information should be collected directly from the data subject. Individuals strongly oppose enhancement,[7] and falsely believe that it is illegal.[8] Enhancement also contravenes the individual's expectation that selective revelation will prevent a company from obtaining certain contact information.

In practice, enhancement is largely a technique to fool the consumer into thinking a company is not collecting data about them. It negates all the rhetoric about trust, respect for the consumer and their preferences, and even the idea that the consumer can decide what information to share. The recent *Pineda* case[9] is a perfect illustration of this. If a company has a desire for the home address of a customer standing before them, the proper thing to do is ask for it directly.[10]

Respectfully submitted,

/s

Chris Jay Hoofnagle

---

[7] Joseph Turow, Lauren Feldman, & Kimberly Meltzer, Open to Exploitation: American Shoppers Online and Offline, Annenberg Public Policy Center of the University of Pennsylvania, Jun, 1, 2005, available at http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31 (90% polled disagreed or disagreed strongly with the statement, "If I trust an online store, I don't mind if it buys information about me from database companies without asking me.")

[8] CJ Hoofnagle & J King, What Californians Understand about Privacy Online, SSRN eLibrary (2008), http://ssrn.com/paper=1262130 ("…42.4% thought privacy policies prohibited enhancement activities, and 12.3% didn't know").

[9] "Jessica Pineda visited a store in California owned by Williams-Sonoma Stores, Inc. (the Store) and selected an item to purchase. She then went to the cashier to pay for the item with her credit card. The cashier asked for her zip code, but did not tell her the consequences if she declined to provide the information. Believing that she was required to provide her zip code to complete the transaction, Pineda provided the information. The cashier recorded it into the electronic cash register and then completed the transaction. At the end of the transaction, the Store had Pineda's credit card number, name and zip code recorded in its databases.

"After acquiring this information, the Store used customized computer software to perform reverse searches from databases that contain millions of names, e-mail addresses, residential telephone numbers and residential addresses, and are indexed in a manner that resembles a reverse telephone book. The Store's software then matched Pineda's now-known name, zip code or other personal information with her previously unknown address, thereby giving the Store access to her name and address."
Pineda v. Williams-Sonoma Stores Inc., Cal. Ct. App., 4th Dist., No. D054355, certified for publication 10/23/09, available at www.courtinfo.ca.gov/opinions/documents/D054355.DOC.

[10] Enhancement is sometimes defended as a method of conveniently collecting data that the consumer wants to share. If this were true, the store in *Pineda* could have asked, "will you share with us your zip code so that we can determine your home address."