BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Berkeley Center for
Law & Technology

Chris Jay Hoofnagle
Lecturer in Residence
University of California, Berkeley
School of Law
424 Sutardja Dai Hall
Berkeley, CA 94720-1764
510-664-4327
bclt.berkeley.edu

February 18, 2011

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Comments of Chris Jay Hoofnagle on A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"; comments upon the Concurring Statement of Commissioner William E. Kovacic

Dear Staff and Commissioners of the FTC:

Thank you for accepting comment upon "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." I submit the following comments:

The need for benchmarks

In 1995, Beth Givens suggested that the FTC set benchmarks to evaluate the FTC's approaches. If we had followed Givens' suggestion, we could more precisely state how much more invasive tracking is today than in 1995, and we could even evaluate the claims of the notice model, the harm model, and future approaches to addressing online privacy.

I urge the Commission to evaluate the state of online privacy through adopting basic benchmarks. They could include:

- How many tracking objects are present on popular websites?
- Can consumers practically block this tracking?
- To what extent can consumers exercise choice over this tracking?
- Are there centralized methods to exercise choice?
- To what extent are web services circumventing users' choices?
- How often do website privacy policies clearly disclose third party marketing sharing?

- And so on.

Americans' attitudes towards privacy

On page ii, the Staff Report adopts the frame of consumer attitudes towards privacy developed by Alan Westin. A number of academics have illuminated nuances to Westin's conclusions. In light of these developments, the Staff Report should reflect a different framing on consumer attitudes towards privacy.

Ponnurangam Kumaraguru and Lorrie Cranor found that Westin used different criteria and different answers for developing his framework.[1] They attempted to find Westin's surveys, but most of them are no longer available, since they were not academically published.

Most importantly, the very idea of a "privacy pragmatist" is flawed, in that Westin made that group the default category. That is, under Westin's approach, if one is not a privacy fundamentalist or privacy unconcerned, they are placed in the pragmatist bucket. This makes little sense, because pragmatism requires certain affirmative behavior, such as taking time to evaluate different options. One is not a pragmatist by default; in fact, millions of Americans see pragmatism as morally questionable.

Westin's screening questions illustrate the foundational problems with his framework. Westin's questions ask individuals about their attitudes towards consumer control, business use of data, and existing law. None of these questions have anything at all to do with the behaviors that define pragmatism. It is impossible to answer Westin's screening questions, and come to the conclusion that a group of them, "…weigh[s] the potential pros and cons of sharing information; evaluate the protections that are in place and their trust in the company or organization. After this, they decide whether it makes sense for them to share their personal information."

---

[1] Ponnurangam Kumaraguru & Lorrie Faith Cranor, Privacy Indexes: A Survey of Westin's Studies, Dec. 2005, available at http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf.

Behaviorally, the idea of three privacy segments does not hold up. In June 2004, a Westin poll showed that both privacy fundamentalists and pragmatists engage in a high level of privacy protection. In the study, respondents were asked whether they had engaged in one of seven actions to protect their privacy. Three-quarters of privacy fundamentalists had taken at least four of the seven actions, and 65% of "pragmatists" had taken at least four of the seven actions. Even those who were labeled "unconcerned" had a high level of taking action to protect privacy--46% had taken at least four of the seven steps to protect privacy. Thus nearly half of those labeled “privacy unconcerned” act similarly to those labeled highly concerned.

My research adds a layer of complexity to the Westin framework: those identified as privacy pragmatists and the unconcerned are less knowledgeable about privacy rules. When we asked a sample of Californians about basic privacy rights in the offline setting, privacy fundamentalists, as a group, were more likely to be correct than pragmatists and the unconcerned on eight of the nine questions.[2] This finds consonance with the work of Oscar Gandy, who found that individuals knowledge and experience was a powerful factor in explaining their placement in the Westin segmentation.[3]

Thus, the description of Americans’ attitudes towards privacy should be conformed to more recent research that illuminates Westin’s work. The Staff Report should note that 1) the conception of a privacy pragmatist is flawed and lacks foundation, 2) those currently identified as privacy pragmatists and unconcerned have less understanding of privacy rules than privacy fundamentalists, and 3) even those labeled privacy unconcerned do take action to protect their privacy.

---

[2] CJ Hoofnagle & J King, *Research Report: What Californians Understand About Privacy Offline*, (2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075.
[3] Oscar H. Gandy, Jr., The Role of Theory in the Policy Process, A Response to Professor Westin, in TOWARD AN INFORMATION BILL OF RIGHTS AND RESPONSIBILITIES (C. Firestone and J. Schement (Eds.) Aspen 1995).

In a 2008 paper with Jennifer King, we concluded that Westin's segmentation creates a perverse outcome for consumers. The Staff Report should not continue to perpetuate this outcome:

> *It is intuitively appealing to frame a public policy approach as serving the interests of a balanced, reasonable group—the privacy pragmatists. But this survey shows that this group is either misinformed or overly optimistic about rules concerning use of their data in many ordinary, offline transactions. If one's membership in a segment is explained by knowledge and experience, as [Oscar] Gandy argues, then the Westin approach does not serve privacy Pragmatists. Instead it manipulates them, by relying upon their ignorance of rules and practices to support a policy outcome that they would likely oppose, if better informed.*[4]

The Value of Behavioral Targeting

The value of behavioral targeting is a key unknown. This issue is important because contextual advertising is highly effective and at the same time, much less privacy invasive than behavioral targeting, which involves tracking individuals over time. In fact, Google used to distinguish its search advertising as more relevant and less invasive than competitors because it was based upon the context of a single search event.[5] *Thus, the difference in value between contextual advertising, which does not require extensive tracking of individuals, and behaviorally-targeted ads is key to the Commission's decisionmaking.*

---

[4] *Id*.

[5] Chris Hoofnagle, *Beyond Google and evil: how policy makers, journalists and consumers should talk differently about Google and privacy*, 14 FIRST MONDAY, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2326/2156.

The need to police terms

The discussion on page 26 notes that consumers may not be aware that a company has hundreds of affiliates. Indeed, the KnowPrivacy team attempted to learn the affiliate structure of the top 50 websites, but they found it impossible to learn this information, even after sending information requests to the companies themselves. They concluded, "Based on our experience, it appears that users have no practical way of knowing with whom their data will be shared."[6]

Complicating this problem is that some companies use the word "affiliates," "family of companies," "sister companies," or even "marketing partners" to mean third parties with which they have an arms-length relationship. A privacy policy model cannot work if different companies can use key terms to mean different things. Reading privacy policies under the current approach is like trying to work through your legal rights in conversation with Humpty Dumpty.

The Staff Report should indicate that certain key terms, such as "affiliate" and "third-party" must conform to a standard definition. California has mandated this in the context of the "Shine the Light Law," which requires disclosures surrounding third party marketing disclosures.[7]

---

[6] Joshua Gomez, Travis Pinnick, and Ashkan Soltani, KnowPrivacy (2009), available at http://knowprivacy.org/affiliates.html

[7] See Cal. Civ. Code § 1798.83(e)(8):
(8) "Third party" or "third parties" means one or more of the following:
(A) A business that is a separate legal entity from the business that has an established business relationship with a customer.
(B) A business that has access to a database that is shared among businesses, if the business is authorized to use the database for direct marketing purposes, unless the use of the database is exempt from being considered a disclosure for direct marketing purposes pursuant to subdivision (d).
(C) A business not affiliated by a common ownership or common corporate control with the business required to comply with subdivision (a).

Quality of survey research

Footnote 72 on page 29 recognizes the limits of consumer survey research. This is a valid point. While it is true that survey research has limitations, it is also true that some survey research is better than other survey research. The work that Joseph Turow and I have done exceeds the quality of competing research on this topic, because:

- Our research is telephonic, on both wireless and wireline numbers. Other surveys in this field use internet samples that have no external validity. That is, these researchers use internet advertising to recruit a panel for a survey about internet advertising.
- We have academic PhD statisticians on our team.
- Our papers are freely available to whomever wants to download them. Other survey research quietly disappears soon after the policy window the sponsors wish to affect closes. Many of these studies do not reveal the questions asked or the methods used adequately. Many require interested readers to ask a PR firm for permission to access the report.
- We do not adopt the Westin strategy of including an answer "in the middle" that allows triangulation and the adoption of any conclusion that the author wishes to take.[8]
- We ask straightforward questions.
- Our results are consonant with other researchers. For instance, Gallup (using a telephonic poll) recently found that 67% did not think that advertisers should be allowed to match ads to interests based upon websites previously visited.[9] This is very close to our finding that 66% of Americans do not want ads tailored to their interests.

---

[8] Here is a spectacular example from Alan Westin's 1991 Equifax study: "A majority of the public (55%) favors protecting consumer privacy by using the present system (31%) or setting up a nonregulatory privacy board (24%). A strong minority (41%) believe a regulatory privacy commission is needed." One could use the same data to come to a different conclusion entirely—65% prefer rejecting the present system in favor of some type of government privacy commission, while only 31% prefer the present system.

[9] Lymari Morales, U.S. INTERNET USERS READY TO LIMIT ONLINE TRACKING FOR ADS, http://www.gallup.com/poll/145337/internet-users-ready-limit-online-tracking-ads.aspx.

Forgoing the benefits of targeted advertising.

The report at page 29 highlights the need for survey research to report degree of discomfort or the proportion of individuals who are willing to forego the benefits of targeted advertising. At least two studies speak to this—the above mentioned Gallup poll (which was released after the Staff Report), which found that only 35% of respondents felt that the invasion of privacy involved in tracking was worth free access; and Joseph Turow's 2003 survey, which presented a common web tracking scenario to users and recorded their responses to it.[10]

The challenge of delay, displacement, and technical circumvention

The Staff Report reflects a lot of work. This initiative builds upon the agency's 15-year investigation of privacy issues. Three roundtables were held. Comments were received and processed on all three. Now, comment is being taken on the Staff Report.

It is important for the FTC to proceed carefully, but it is equally important to recognize that some actors in this debate are pursing a strategy of delay. *They do not believe that users should have any control over tracking.*[11] No amount of data or care demonstrated by the agency will turn them from this conviction. Their invocations of "free market" values is often a stalking horse for big business interests that privately abhor libertarianism, but publicly enjoy its demagogic appeal.

All of this is part of a strategy of delay, one that enables displacement. That is, by the time the FTC identifies a problematic practice, spends years collecting comments about it, etc., the industry will move on to other forms of tracking that are just as invasive but outside the scope of the agency's interventions.

---

[10] J Turow, *Americans and Online Privacy The System is Broken*, 21-22, ANNENBERG PUBLIC POLICY CENTER (2003), http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf.

[11] For instance, the NAI's opt out procedure does not prevent tracking. Additionally, the point of Flash cookie respawning was to negate consumers' deletion of HTTP cookies.

If the FTC does not move more quickly, the DNT venture will be obsolete, because online trackers will use delay to find technical means to reframe their activities as “first party” tracking.

Key in this risk are Google and Facebook. Google may claim that their tracking is “first party,” because website operators include JavaScript code on their sites that gives Google the ability to set first-party cookies. The KnowPrivacy Report found Google trackers on 88% of a sample of almost 400,000 unique domains. All of that tracking would be outside the DNT intervention if Google is considered to have a first party relationship.

The other, larger fake first party risk is presented by Facebook. That company operates as a third party on many other websites through the “like” feature, and in doing so, can track behavior on a wide variety of popular websites. DNT interventions have to treat such activities as third party, otherwise Google and Facebook will become the biggest winners of DNT.

Simplified choice surrounding first-party marketing is too broad and will contravene consumers’ reasonable expectations

The discussion surrounding first-party marketing and choice fails to recognize consumers’ legitimate interest in preventing first-party data collection and use. The language is too broad and will result in first-party practices that are transgressive and contravene consumers’ preferences. As businesses develop new ways to identify individuals (often without the consumer’s knowledge), consumers will want more ability, not less, to control whether data is collected and how it is used.

Consumers are hesitant to share information with many first parties, even reputable ones. As an example, consider the *Pineda v. Williams Sonoma* case. Williams Sonoma collected zip codes from consumers and used enhancement in order to discover the home addresses of its customers. Williams Sonoma had to engage in that practice precisely because consumers do not want to share their contact information with every business they frequent. This practice should not be commonly accepted, simply because it is engaged in by a first party.

Sometimes we buy things and do not wish the seller to engage in more data collection or solicitation, because the purchase was sensitive or "private." Consumers may not want targeted ads, emails, or mail from companies in these contexts.

Most importantly, consumers technically have relationships with hundreds or perhaps thousands of companies. Just think of every fast food store one visits on a road trip, or every bodega visited in life. Currently, these entities are sharply limited in how well they can identify consumers. In order to do so reliably, even when credit cards are involved, they have to adopt some type of loyalty program or a backend enhancement system like William Sonoma's. This could change radically as mobile payment systems become popular. The incentive structure in new payment systems is to maximize data collected about the consumer,[12] and in many cases, identify the consumer and provide contact information to the vendor. In a world of more perfect consumer identification, many individuals will find themselves profiled and contacted as a result of incidental purchases.

There are principled ways to addressing these problems. One is to require that information be collected from the consumer herself. Thus, the framework should reject enhancement as a practice unless the consumer is informed directly of the practice and given the opportunity to object. For instance, in the Williams Sonoma example, the store could ask the customer whether she wants the catalog, and say, "in order to save you time, we can look up your home address using a database if you simply provide your zip code." If consumers really want the first party to have this information, they will provide it. The fact that trickery and backend databases have to be used suggests they don't really want it, or that the company cannot be bothered to treat the consumer with respect and ask first.

---

[12] For instance, both Paypal and Google Checkout make "track 3 data," that is, precisely what the consumer purchased, available to the payment provider. In the world of credit cards, issuing banks and the network itself rarely know what the consumer bought, instead they knew how much was spent and where. In this way, these new forms of payment are less private than credit cards.

Enhancement breaks the basic narrative surrounding "trust," which holds that consumers should protect themselves in the marketplace by only sharing data with certain companies. If those companies can buy information from third parties, the consumer loses all ability to protect herself through a grant of trust. Enhancement circumvents consumers' basic tool of selective revelation, and makes them an unwitting participant in their own profiling.

Comments on the concurring statement of William E. Kovacic

Many researchers have earnestly and without ideological commitment attempted to characterize the problems with marketplace approaches to privacy. Your comments call for more research on a number of topics. This skepticism is justified, but at the same time, I often wonder how much more work has to be done in this field to satisfy opponents of regulatory intervention.

This question is why I am such an advocate of benchmarks, and why I believe you—of all the Commissioners—should be as well. Benchmarks could help us evaluate regulatory approaches, and advocates of different approaches could actually test their ideas against marketplace behavior.

Benchmarks could help bust the problem of moving goalposts, especially among those who continually call for more research as a delay tactic.

Benchmarks will also help address the problem of double standards for our assumptions. For instance, in your comment, you call for the need for more evidence for the proposition that consumer expectations of privacy are largely going unmet.[13] This is what I call "privacy's problem with problems." To justify privacy laws, critics often demand proof of wrongs and evidence of unmet expectations. But in order to unmask these problems, one often needs the very information-forcing rules created by privacy laws.

---

[13] The record is full of such evidence; my own research, which is corroborated by others, shows that consumers fundamentally misunderstand privacy protections and mistakenly believe that strong laws protect them by default.

You continue by arguing that incentives for privacy are understated by the report. However, the evidence you use to support this argument could more cogently be used to illuminate marketplace failures--

- Security breaches. Security breaches aren't really about the kinds of privacy protections sought in this report. But assuming that they are, we only know of them because of regulatory intervention, not because of the market. Market approaches obscured breaches, just as they hide information practices that consumers would object to if fully informed of them.
- TACO. The Targeted Advertising Cookie Opt Out does nothing to protect users' privacy. It simply tells third party advertising networks not to deliver targeted ads to the user. The network is still free to track that user, thus more aggressive cookie and script blocking tools needed to be wedded to TACO to make it an effective PET. TACO has been downloaded over 800,000 times, but even if those are unique downloads, that is still less than one percent of American households. The NAI rules that brought about the opt out cookie and thus TACO only occurred because of the threat of regulatory intervention, and the NAI effectively disappeared once the FTC signed off on its principles.
- NoScript. NoScript's existence is evidence of a disaster in online privacy and security. Scripting allows all sorts of malicious attacks and tracking that cannot be controlled through the browser. Think of it this way: sophisticated, market-dominant actors themselves are unable to determine what tracking technologies they are hosting.[14] As a result, knowledgeable users are blocking all scripting by default.

I point these out, because it seems like any evidence, even bad or contradictory evidence, can be invoked successfully to support market

---

[14] Julia Angwin & Scott Thurm, WEBSITE OPERATORS MOUNT DEFENSE (2010), http://online.wsj.com/article/SB10001424052748704011904575538372505294514.html ("Eleven of the nation's largest website operators defended their privacy practices to lawmakers, saying it is impossible for them to monitor all the tracking technologies their sites install on visitors' computers").

approaches,[15] while consumer interventions must be justified with exactitude. Benchmarks could create greater parity in the demands made on both claims supporting consumer interventions, and the vague, evergreen arguments for market approaches.

Respectfully submitted,

/s

Chris Jay Hoofnagle

[15] Elizabeth Warren, *The Market for Data: The Changing Role of Social Sciences in Shaping the Law*, 2002 WISCONSIN LAW REV. 1 (2002), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=332162.