Federal Trade Commission

The Evolution of "Privacy Policy" at the Federal Trade Commission: Is It Really Necessary?

J. Thomas Rosch[1]
Commissioner, Federal Trade Commission

at
The Mentor Group Boston
Forum for EU-US Legal Eco Affairs
Paris, France

September 14, 2012

Good afternoon. I am pleased to be here today to discuss some of my thoughts on privacy, behavioral tracking and the push for "Do Not Track" mechanisms, self-regulation and the importance of informed consumer choice. For today's discussion, when I refer to "Do Not Track" mechanisms I mean a method by which an Internet user can make a choice whether or not to allow the collection and use of data regarding their online activities – things like search and browsing.[2] Some have likened the concept of "tracking" to being followed around a store as you shop. However, computer technology allows online tracking to be more comprehensive, pervasive and detailed than the tracking that can occur offline.

---

[1] The views stated here are my own and do not necessarily reflect the views of the Commission or other Commissioners. I am grateful to my attorney advisor Beth Delaney for her invaluable assistance in preparing these remarks.

[2] The concept of Do Not Track was presented in the preliminary Staff Privacy Report, issued in December 2010. *See* Fed. Trade Comm'n, Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

"Do Not Track" and Self-Regulation

As many of you may be aware, I dissented in large measure from the Commission's Privacy Report issued in March, 2012.[3] One of my objections was to what I viewed as the overly optimistic description in the Report of the status of browser mechanisms and self-regulatory efforts regarding the concept of "Do Not Track." More specifically, the Report asserted that both the development of browser mechanisms and the evolution of self-regulation regarding "Do Not Track" had advanced substantially since the issuance of the staff's preliminary privacy report in December 2010. Indeed, the Chairman of the Commission was quoted extensively as predicting that consumers could use these Do Not Track mechanisms by the end of 2012.

I was a "doubting Thomas." The Report, the Chairman, and the White House all touted a browser-based opt-out mechanism to prevent tracking.[4] The major browser firms' agreed to implement a browser-based mechanism,[5] and the Digital Advertising Alliance (DAA) committed

---

[3] Fed. Trade Comm'n, FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf; Dissenting Statement of Commissioner J. Thomas Rosch, Issuance of Federal Trade Commission Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012), *available at* http://www.ftc.gov/speeches/rosch/120326privacyreport.pdf.

[4] Kenneth Corbin, *Obama Backs 'Consumer Bill of Rights' for Online Privacy*, CIO, Feb. 23, 2012, *available at* http://www.cio.com/article/700735/Obama_Backs_Consumer_Bill_of_Rights_for_Online_Privacy.

[5] Julia Angwin, *Web Firms to Adopt 'No Track' Button*, Wall Street Journal, Feb. 23, 2012, *available at* http://online.wsj.com/article/SB10001424052970203960804577239774264364692.html.

[6] Edward Wyatt, *White House, Consumers in Mind, Offers Online Privacy Guidelines*, N.Y. Times, Feb. 23, 2012, *available at* http://www.nytimes.com/2012/02/23/business/white-house-outlines-online-privacy-guidelines.html?_r=1; *see also* Press Release, Digital Advertising Alliance, *White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumers Online Privacy* (Feb. 23, 2012), *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

[7] I have raised this argument before. *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, *Do Not Track: Privacy in an Internet Age*, Remarks at Loyola Chicago Antitrust Institute Forum (Oct. 14, 2011), *available at* http://www.ftc.gov/speeches/rosch/111014-dnt-loyola.pdf. Furthermore, in reviewing the

understood the standard the W3C was working on, it was a Do Not Track signal that the major browser firms would send to various websites about whether or not the website wished to have consumers' online activities "tracked." It was then up to the recipient website or service to honor the Do Not Track request (for example, by not deploying "cookies" that could track consumer data.) In this instance, the consumer himself would not be required to communicate that request to the recipient website or service.

To be sure, there are other methods for the consumer to directly communicate that request to the website or ad network (for example, by visiting a website and "opting out" of having information tracked or collected). Frequently, however, that process took at least three or more "clicks." So there was a real question as to whether the consumer could enforce the website's choice to honor (or not) a Do Not Track signal received from a browser.[8] Moreover, since that signal was an "all or nothing" signal, the W3C option – at least insofar as it has developed to date – did not offer the consumer the option of exercising a "nuanced" choice (allowing collection in some circumstances, but not others).

Worse, I was concerned that the major browser firms and the recipient websites and online services did not mean the same thing when it came to defining the meaning of "Do Not Track." It appeared that the browser firms and some of the websites would interpret it to really mean "Do Not Collect" data. But it appeared that the balance of the websites interpreted "Do Not Track" to mean simply "Do Not Target" advertising to consumers. That difference became clear when the Digital Advertising Alliance (DAA), a coalition of industry trade association

---

[8] *Cf.* Dan Goodin, *Apache Webserver Updated to Ignore Do Not Track Setting in IE 10*, Ars Technica, Sept. 10, 2012, *available at* http://arstechnica.com/security/2012/09/apache-webserver-updated-to-ignore-do-not-track-settings-in-ie-10/.

understanding that consumers wishing to not be tracked would need to select that option. Because the behavioral economics literature suggests that consumers generally don't deviate from default settings,[13] it is arguable that in the real world, consumers might not change these default settings implemented by Microsoft. (Indeed, for that reason, the Commission has adopted a rule attaching stringent conditions to use of any "negative option" in consumer transactions.) Moreover, because Microsoft has a huge installed base, at least in the United States (accounting for most of the browsers installed as original equipment in desktop and laptop computers), it has been suggested that Microsoft has acted more strategically and opportunistically to disadvantage rivals (particularly Google) than out of concern for consumer privacy.[14]

Second, the development and implementation of this standard puts the "scope" of the choice in the hands of those other than consumers. The major browser firms and the recipient websites and online services, not consumers, will continue to have the final say regarding what "Do Not Track" means. And that will remain the *status quo* no matter what technical standard the W3C adopts. The W3C standard merely will determine the signal that will be sent by the browsers and how the recipient websites are supposed to respond to it.[15] The W3C standard will

---

ts-do-not-.html.

[13] Maurice E. Stucke, *The Implications of Behavioral Antitrust*, University of Tennessee Legal Studies Research Paper No. 192, at 7 (Aug. 7, 2012), *available at* http://ssrn.com/abstract=2109713.

[14] Kelly Clay, *Is Microsoft Going After Google With IE10?*, Forbes, June 4, 2012, *available at* http://www.forbes.com/sites/kellyclay/2012/06/04/is-microsoft-going-after-google-with-ie10/.

[15] Jim Edwards, *Here's the Gaping Flaw in Microsoft's 'Do Not Track' System For IE10*, Business Insider, Aug. 29, 2012, *available at*

http://www.businessinsider.com/heres-the-gaping-flaw-in-microsofts-do-not-track-system-for-ie10-2012-8 ("The hole is that the DNT is merely a signal telling advertisers about users' preferences to not be tracked—**it's *not***

Fifth, however, we should not expect a workable Do Not Track that consumers can use to exercise "their" choice to occur anytime soon.[18] To suggest that it will happen by the end of the year is just folly. There is still too much technical work to be done for that to be feasible.

Informed Consumer Choice and Self-Regulation

I am a big fan of consumer choice. But only if it is informed consumer choice. I am not just talking about "information asymmetry" – economist-speak for consumers having information about the transaction that is inferior to the information possessed by sellers. I am referring also to consumers being fully informed about the consequences of the choices they make, then afterward being given the chance to opt out or opt in. That is why I am frustrated by the current debate about privacy and behavioral tracking. Many consumers may not want to take chances with their privacy. They may want to zealously guard against identity theft and the use by others of truly personal information like health information or information about their sexual preferences and practices. For that kind of information, an opt-in option may be appropriate. On the other hand, there is no reliable data on what percentages of consumers insist on protecting against behavioral tracking so zealously. I am inclined to favor an opt-out option unless and until there is reliable data to establish that most consumers are as determined to eliminate behavioral tracking as some consumer advocates say they are. In either case, however, I continue to believe that before either option is exercised, consumers should be fully informed about the consequences of their choices.

---

[18] *See also* Jasmin Melvin, *Little Progress on "Do Not Track" After 10 Months of Talks*, Chicago Tribune (Reuters), July 23, 2012, *available at* http://articles.chicagotribune.com/2012-07-23/business/chi-little-progress-on-do-not-track-after-10-months-of-talks-20120723_1_internet-privacy-user-data-ad-revenue.

[27] *See* Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in International Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984) ("Unfairness Policy Statement"), *available at* http://www.ftc/gov/bcp/policystmt/ad-unfair.htm

There does not appear to be any such limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" (in the form of the Commission or the Congress) as the watchdog over these practices not only in the online world but in the offline world.[30] That is not only paternalistic, but it goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).[31] I would instead stand by what we have said and challenge information collection practices, including behavioral tracking, only when these practices are deceptive, "unfair" within the strictures of Section 5(n) and our commitments to Congress, or employed by a firm with market power and therefore is arguably challengeable on a stand-alone basis under Section 5's

[30] *See* Report at 13.

[31] Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312.