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.

to following the instructions that consumers made using such mechanisms.[6] This later evolved into a general agreement to develop a common Do Not Track mechanism based on the technical standard adopted by a standard-setting organization called the W3C (short for World Wide Web Consortium). My doubts about that "agreement" were twofold.

First, I was concerned that at least one of those major browser firms would act strategically and opportunistically to use privacy to protect its own entrenched competitive self-interest instead of acting in a fashion that would give consumers more choice with respect to whether to allow collection of their data.[7]

Second, I was concerned about whether a W3C technical standard would really give consumers a meaningful choice as to how much of their data really would be collected. As I

---

[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 Google Buzz consent for final approval, I raised the issue that sometimes firms are willing to swallow bitter medicine if there is a possibility that their rivals may also be forced to take the medicine, which they in turn may find even more bitter. More specifically, I pointed out that parts of that consent agreement seemed to be contrary to Google's self-interest. I therefore asked myself if Google willingly agreed to it, and if so, why it did so. Surely it did not do so simply to save itself litigation expense. But did it do so because it was being challenged by other government agencies and it wanted to "get the Commission off its back"? Or did it do so in hopes that certain provisions in the consent agreement would be used as leverage in future government challenges to the practices of its competitors? In my judgment, neither of the latter explanations was consistent with the public interest. *See* Concurring Statement of Commissioner J. Thomas Rosch, *In re Google Buzz*, File No. 1023136 (Mar. 30, 2011), *available at* http://www.ftc.gov/speeches/rosch/110330googlebuzzstmt.pdf.

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/.

members (which acted as a voluntary "self-regulatory" group), insisted on carving out an exception for data collected for "research" or "product development" purposes.[9] Under such circumstances, I was hard put to see how the W3C could fashion even a technical standard when there was no agreement between the senders and the recipients of the signal about what the standard actually was supposed to do.[10]

I'm afraid my doubts have been borne out. First, shortly after I first expressed my concerns, Microsoft announced that it would adopt a real Do Not Track as a default option.[11] According to news reports, that was squarely contrary to what participants in the W3C standard-setting process had been led to believe from the outset: according to those reports, participants were told that the proposed Do Not Track mechanism would not be set as the default.[12] Rather, the development of a Do Not Track standard was grounded on the

---

[9] For example, the DAA's Self-Regulatory Principles for Multi-Site Data do not apply to data collected for "market research" or "product development." *See* Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data*, at 3, 10 and 11 (Nov. 2011), *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf; *see also* Tanzina Vega, *Opt-Out Provision Would Halt Some, but Not All, Web Tracking*, N.Y. Times, Feb. 26, 2012, *available at* http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-web-tracking.html?pagewanted=all.

[10] Tony Romm, *What Exactly Does 'Do Not Track' Mean?*, Politico, Mar. 13, 2012, *available at* http://www.politico.com/news/stories/0312/73976.html.

[11] *See also* Letter from Commissioner J. Thomas Rosch, Fed. Trade Comm'n, to World Wide Web Consortium Tracking Protection Working Group (June 20, 2012), *available at* http://ftc.gov/speeches/rosch/120620W3Cltr.pdf.

[12] Julia Angwin, *Microsoft's "Do Not Track" Move Angers Advertising Industry*,Wall Street Journal, May 31, 2012, *available at* http://blogs.wsj.com/digits/2012/05/31/microsofts-do-not-track-move-angers-advertising-industry/; Wendy Davis, *Web Standards Group Criticizes Microsoft's Do-Not-Track Move*, Media Post, June 6, 2012, *available at* http://www.mediapost.com/publications/article/176314/web-standards-group-criticizes-microsof

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*

not solve the "accessability" problem that many consumers experience in trying make or modify their choices about information collection. Much less will it allow consumers to exercise any "nuanced" choice.

Third, there is still a disconnect between how the browser firms and the websites receiving the Do Not Track signal interpret that signal. The industry self-regulatory group (the DAA) has reiterated that it does not think that the objective of Do Not Track can, or should be, to prevent the collection of consumer data.[16] However, that is precisely what the major browser firms (or, at the very least, Microsoft) thinks it means.

Fourth, that does not mean the W3C is without any value. Both the White House and the Commission promised that there would be "workshops" later this year at which all of the relevant stakeholders could air their views.[17] To the best of my knowledge, workshops regarding Do Not Track have not yet occurred. So the W3C process is the "only game in town" where stakeholders can state their views, at least about what technical standard should be adopted.

---

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* a mechanism that actually blocks web ads from dropping tracking "cookies" onto browsers' desktops** and devices.") (emphasis in original).

[16] Press release, Digital Advertising Alliance, Digital Advertising Alliance (DAA) Comments on Microsoft Decision to Embed Do Not Track in IE 10 Set 'On' by Default (May 31, 2012), *available at* http://www.businesswire.com/news/home/20120531006914/en/Digital-Advertising-Alliance-DAA-Comments-Microsoft-Decision.

[17] *See, e.g.*,The Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, Feb. 23, 2012, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

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.

That is why I have so vigorously supported requiring clear, complete and accurate notices to consumers about how sellers will handle their personal information before consumers are obliged to make their choices. I consider the Commission's insistence that such notices be given to be the Commission's most significant contribution to consumer protection. That is why I bridled when the staff's preliminary privacy report did not differentiate between the two kinds of consumer information that were at issue (sensitive versus "not that sensitive"), made unsupported claims about what percentage of consumers preferred not to be subject to behavioral tracking (as opposed to merely being concerned about privacy or security breaches), and suggested that "notice" might be replaced by a new and untested paradigm based on "unfairness."[19]

The New – But Not Improved – Privacy Paradigm

In fact, my primary disagreement with the Commission's "final" Privacy Report is rooted in its insistence that the "unfair" prong, rather than the "deceptive" prong, of the Commission's Section 5 consumer protection statute, should govern information gathering practices (including "tracking"). "Unfairness" is an elastic and elusive concept. What is "unfair" is in the eye of the beholder. For example, most consumer advocacy groups consider behavioral tracking to be unfair, whether or not the information being tracked is personally identifiable information ("PII") and regardless of the circumstances under which an entity does the tracking. But, as I and others have said, consumer surveys are inconclusive, and individual consumers by and large do not "opt out" from tracking when given the chance to do so.[20]

---

[19] *See* Rosch Dissenting Statement, *supra* note 3.

[20] *See* Katy Bachman, *Study: Internet User Adoption of DNT Hard to Predict*, adweek.com, Mar. 20, 2012, *available at*

The Commission's "final" Privacy Report (like the staff's preliminary privacy report) repeatedly sides with consumer organizations and large enterprises. It proceeds on the premise that behavioral tracking is "unfair."[21] Thus, the Report expressly recommends that "reputational harm" be considered a type of harm that the Commission should redress.[22] The Report also expressly says that the "best practices include making privacy the 'default setting' for commercial data practices."[23] Indeed, the Report says that the "traditional distinction between PII and non-PII has blurred,"[24] and it recommends "shifting burdens away from consumers and placing obligations on businesses."[25] The Report goes on to imply that the Commission ought to embrace APEC and OECD principles respecting consumer privacy.[26] Although the U.S.

---

http://www.adweek.com/news/technology/study-internet-user-adoption-dnt-hard-predict-139091 (reporting on a survey that found that what Internet users say they are going to do about using a Do Not Track button and what they are currently doing about blocking tracking on the Internet, are two different things); s*ee also* Concurring Statement of Commissioner J. Thomas Rosch, Issuance of Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* http://www.ftc.gov/speeches/rosch/101201privacyreport.pdf.

[21] Report at 8 and n.37.

[22] *Id*. at 2. The Report seems to imply that the Do Not Call Rule would support this extension of the definition of harm. *See id*. ("unwarranted intrusions into their daily lives"). However, it must be emphasized that the *Congress* granted the FTC underlying authority under the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, to promulgate the Do Not Call provisions and other substantial amendments to the TSR. The Commission did not do so unilaterally.

[23] Report at i.

[24] *Id*. at 19.

[25] *Id*. at 23, *see also id.* at 24.

[26] *Id*. at 9-10, 23-24. This does not mean that I am an isolationist or am impervious to the benefits of a global solution. But, as stated below, there is more than one way to skin this cat.

government is a member and participant of these organizations, we should nevertheless carefully consider whether each individual policy choice regarding privacy is appropriate for this country in all contexts.

That is not how the Commission itself has traditionally proceeded. To the contrary, the Commission represented in its 1980, and 1982, Statements to Congress that, absent deception, it will not generally enforce Section 5 against alleged intangible harm.[27] The Commission also has not traditionally tethered itself to the policy judgments of other regimes about consumer privacy. Instead, it has tried, through its advocacy, to convince others that our approach to privacy – one that considers innovation – ought to be adopted. And, as I stated in connection with the recent *Intel* complaint, in the competition context, one of the principal virtues of applying Section 5 was that that provision was "self-limiting," and I advocated that Section 5 be applied on a stand-alone basis only to a firm with monopoly or near-monopoly power.[28] Indeed, as I have remarked, absent such a limiting principle, privacy may be used as a weapon by firms having monopoly or near-monopoly power to disadvantage rivals.[29]

---

[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; Letter from the FTC to Hon. Bob Packwood and Hon. Bob Kasten, Committee on Commerce, Science and Transportation, United States Senate, *reprinted in* FTC Antitrust & Trade Reg. Rep. (BNA) 1055, at 568-570 ("Packwood-Kasten letter"); and 15 U.S.C. § 45(n), which codified the FTC's modern approach.

[28] *See* Concurring and Dissenting Statement of Commissioner J. Thomas Rosch, *In the Matter of Intel Corp.*, Docket No. 9341 (Dec. 16, 2009), *available at* http://www.ftc.gov/os/adjpro/d9341/091216intelstatement.pdf.

[29] *See* Rosch, Remarks at Loyola, *supra* note 7 at 20.

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 prohibition of unfair methods of competition.

---

[30] *See* Report at 13.

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