Federal Trade Commission

DO NOT TRACK: PRIVACY IN AN INTERNET AGE

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

at the

Loyola Chicago Antitrust Institute Forum
Chicago, Illinois
October 14, 2011

I am pleased to have been asked to speak to you today about the concept of "Do Not Track" and the various methods that have been proposed to implement it. This has been a controversial topic as of late – generating attention not only from the Commission and the media, but also from Congress, the online industry, and a host of consumer advocacy groups. Congress has proposed several pieces of legislation that relate to the concept of Do Not Track. And the online industry (including trade associations) has pursued divergent attempts at self-regulation. At the same time, some, such as consumer advocacy groups, have complained that these efforts do not go far enough while others – and I include myself in this group – are concerned that these attempts at protecting consumer privacy may instead thwart innovation and real, informed consumer choice. This afternoon, I would like to share some thoughts regarding

[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 Beth Delaney, David Koehler and Monica Kumar for their invaluable assistance in preparing these remarks.

these developments.

Because I have already spoken and written about my reservations about the general concept of Do Not Track, I will not discuss them in depth here today.[2] However, to set the stage for today's remarks, let me highlight a couple distinctions that I draw when examining issues related to consumer privacy.

First, as a threshold matter, I see a distinction between the issues associated with "data collection" (such as the types of information collected; the means through which it is collected; whether, and with whom, it is shared; and how long it is retained) as compared to the issues associated with "data security" (the obligation to keep secure information that has been collected from consumers). Practices that threaten data security are pernicious, and the Commission has successfully challenged them.[3]

Second, I draw a distinction between "sensitive" consumer information and non-sensitive

---

[2] For example, as I discussed in an earlier speech, before we proceed down the road toward championing a "Do Not Track" system, we should gather competent and reliable evidence about what kind of tracking is occurring. We also need to know more than we know now about what types of "tracking" consumers really care about. Specifically, we need to gather reliable evidence about the practices that most concern consumers. I believe that it is possible to gather that evidence and that the FTC is probably in the best position to do so. *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Information and Privacy: In Search of a Data-Driven Policy, Remarks Before the Technology Policy Institute Aspen Forum (Aug. 22, 2011), *available at* http://www.ftc.gov/speeches/rosch/110822aspeninfospeech.pdf.

[3] *See, e.g., Lookout Servs., Inc.*, FTC File No. 1023076 (June 15, 2011) (consent order) (alleging failure to reasonably and appropriately secure employees' and customers' personal information, collected and maintained in an online database); *CVS Caremark Corp.*, FTC File No. 0723119 (June 18, 2009) (consent order) (alleging failure to implement reasonable policies and procedures for secure disposal of personal information); *BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order) (alleging failure to take reasonable and appropriate security measures to protect sensitive consumer financial information with respect to credit and debit card purchases); *Eli Lilly and Co.*, FTC File No. 0123214 (May 8, 2002) (consent order) (alleging failure to provide appropriate training for employees regarding consumer privacy and information security).

consumer information. I think we all can recognize that certain information should be deemed "sensitive," whether it be your personal health and medical records, your personal financial records, personally identifiable information collected from children, or other highly personal information about individuals, such as their sexual preference. Consumer harm certainly occurs when such information is not treated with the proper deference. Indeed, federal statutes – such as the Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, and Children's Online Privacy Protection Act – recognize this and regulate certain aspects of the collection, sharing and retention of most of this information.[4]

Sensitive consumer information should be treated differently than other types of consumer information. For example, I think that – for purposes of behavioral tracking and advertising – sensitive personal information like medical and health records, financial data, information collected from children, and other highly personal information should only be collected from consumers after they have explicitly given their permission for its collection and use. In other words, the collection, use, sharing and retention of "sensitive" information could only occur after consumers "opted in" to these practices.[5]

On the other hand, there is some consumer data – such as consumer preferences;

---

[4] The Commission has successfully challenged practices that violate these statutes. *Rite Aid Corp.*, FTC File No. 0723121 (Nov. 12, 2010) (consent order) (in conjunction with HHS; alleging failure to establish policies and procedures for the secure disposal of consumers' sensitive health information) (HIPAA); *SettlementOne Credit Corp.*, FTC File No. 0823208 (Feb. 9, 2011) (proposed consent agreement) (alleging that credit report reseller failed to implement reasonable safeguards to control risks to sensitive consumer information) (GLBA); *United States v. Playdom, Inc.*, Case No. SACV 11-0724-AG(ANx) (C.D. Cal. May 24, 2011) (consent order) (alleging failure to provide notice and obtain consent from parents before collecting, using, and disclosing children's personal information) (COPPA).

[5] In addition, prior to opting in, consumers would need to be provided with disclosures about the full extent of collection, use, sharing and retention of such information.

browsing history; information that is not personally identifiable; demographic and age information – that I don't think necessarily deserves the same stringent protection.[6] The collection, use, sharing and retention of these more benign types of information arguably do not lead to the types of consumer injury associated with the collection, use, sharing and retention of "sensitive" information.[7] And, as I have mentioned before, the collection and use of this type of data can help fuel innovation, underwrite the costs of providing free content to users, and streamline the user's experience on the Internet.

I. Commission Efforts

As many of you are aware, the Commission officially entered the "Do Not Track" fray when it issued a December 2010 preliminary staff report, "*Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*," which

---

[6] I do acknowledge that some have argued persuasively that if enough "benign" information is collected and compiled about a particular individual, the resulting profile could raise privacy concerns. *See, e.g.*, Emily Steel, A *Web Pioneer Profiles People By Name*, WALL ST. J., Oct. 25, 2010, http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

[7] To the extent that the Commission has used a "harm" model based on the potential for physical or financial harm, or intangible harm constituting a violation of a special statute, that model may be a useful and legitimate framework. The Commission has challenged practices threatening physical harm under Section 5 of the FTC Act. *See Int'l Harvester Co.*, 104 F.T.C. 949 (1984). Moreover, it has challenged practices threatening intangible harm under special statutes enacted by Congress, specifically the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, and the Do Not Call amendments to the Telemarketing Sales Rule. However, the Commission could overstep its bounds if it were to begin considering "reputational harm" or "the fear of being monitored" or "other intangible privacy interests" generally when analyzing consumer injury. The Commission has specifically advised Congress that absent deception, it will not ordinarily enforce Section 5 against alleged intangible harm. Letter from the Fed. Trade Comm'n 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, *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

recommended implementation of a do-not-track mechanism so consumers could choose whether to allow the tracking of certain data, such as their online searching and browsing activities, in order to serve them targeted advertising.[8]

This "recommendation," however, was not a unanimous one, and both former Commissioner Kovacic and I expressed our serious reservations about this course of action.[9] Nonetheless, we agreed with the Commission's decision to issue the staff's Report in order to continue the dialogue on consumer privacy issues and to solicit comment on a proposed new framework for how companies should protect consumers' privacy. This dialogue has continued: the Commission has testified before Congress several times on issues related to privacy and the concept of Do Not Track,[10] and some of the members of the Commission have given speeches

---

[8] FTC Press Release, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), *available at* http://www.ftc.gov/opa/2010/12/privacyreport.shtm. The Report contained a list of questions for comment, and the public comment period ended February 18th. *See* FTC Press Release, FTC Extends Deadline for Comments on Privacy Report Until February 18 (Jan. 21, 2011), *available at* http://www.ftc.gov/opa/2011/01/privacyreport.shtm.

[9] Concurring Statement of Comm'r William E. Kovacic, Issuance of Preliminary FTC Staff Report "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," *appended to* FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change* 109 app. (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; Concurring Statement of Comm'r 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.

[10] "Privacy and Data Security: Protecting Consumers in the Modern World," Testimony Before the Senate Committee on Commerce, Science, and Transportation (June 29, 2011), *available at* http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf; "Internet Privacy, the Views of the FTC, FCC, and NTIA," Testimony Before the House Subcommittee on Commerce, Manufacturing, and Trade and House Subcommittee on Communications and Technology (July 14, 2011), *available at* http://www.ftc.gov/os/testimony/110714internetprivacytestimony.pdf. *See also* Statement of Comm'r J. Thomas Rosch, Dissenting in Part from "Privacy and Data Security: Protecting

and public statements expressing their views on the topic.[11] Also, I imagine the general concept of Do Not Track will also be discussed in any future reports issued by staff on the proposed privacy framework.

While the Commission's work on this issue appears to have been limited to "thinking deep thoughts" – namely, identifying the possible benefits and down sides of implementing potential Do Not Track mechanisms – there is one notable exception. In a recent Notice of Proposed Rulemaking for the COPPA Rule, the Commission recently proposed amending the definition of "personal information" to add other identifiers that link a child's activities across different sites or services.[12] The effect of this amendment would be to require parental notification and consent prior to the collection and use of persistent identifiers for purposes such as behaviorally targeting advertising to a child. Effectively, this would require parents to "opt

---

Consumers in the Modern World" (June 29, 2011), *available at* http://www.ftc.gov/speeches/rosch/110629privacytestimony.pdf; Statement of Comm'r J. Thomas Rosch, Dissenting in Part from "Internet Privacy: The Views of the FTC, FCC, and NTIA" (July 14, 2011), *available at* http://www.ftc.gov/os/2011/07/110714roschdissentingstatement.pdf.

[11] *See, e.g.*, Julie Brill, Comm'r, Fed. Trade Comm'n, Privacy: From the Woods to the Weeds, Address Before the International Association of Privacy Professionals (Sept. 15, 2011), *available at* http://www.ftc.gov/speeches/brill/110915privacywoods.pdf; Jon Leibowitz, Op.-Ed., *Internet Business Must Respect Users' Privacy*, BLOOMBERG, June 2, 2011, http://www.bloomberg.com/news/2011-06-02/internet-businesses-must-respect-users-privacy-jon-leibowitz.html; Jon Leibowitz, Op.-Ed., *'Do Not Track' Rules Would Help Web Thrive*, U.S. NEWS & WORLD REP., Jan. 3, 2011, http://www.usnews.com/opinion/articles/2011/01/03/ftc-chairman-do-not-track-rules-would-help-web-thrive-jon-leibowitz; J. Thomas Rosch, Op.-Ed., *The Dissent: Why One FTC Commissioner Thinks Do Not Track is Off-Track*, ADVERTISING AGE, March 24, 2011.

[12] The Commission's Notice of Proposed Rulemaking can be found at 76 Fed. Reg. 59,804 (Sept. 27, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf.

in" to tracking on behalf of their children.[13] Public comment has been requested on this proposal as well as a variety of other proposed amendments to the COPPA Rule.

At the same time that the FTC has been analyzing these issues, Congress and the online industry have actively been attempting to implement – to varying degrees – the Do Not Track concept. Let's review the bidding.

II. Recent Legislative Proposals

Congress has attempted to address the Do Not Track concept through proposed legislation in one of two ways: (1) directly, by instructing the FTC to develop a specific Do Not Track mechanism; or (2) indirectly, through broader privacy bills that consider Do Not Track concerns. Two recent legislative proposals specifically take Do Not Track head on, directing the FTC to develop a Do Not Track mechanism.[14] In February, Representative Jackie Speier (D-CA) introduced the "Do Not Track Me Online Act,"[15] which would require the FTC to issue rules: (a) establishing standards for "an online opt-out mechanism;" (b) requiring mandatory disclosures regarding the collection, use, and sharing of information; and (c) allowing consumers to otherwise prohibit the collection or use of a broad array of information transmitted online

---

[13] However, operators' use of persistent identifiers for purposes such as user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, protecting against fraud or theft, and other activities necessary to maintain the technical functioning of a site or service would not require parental consent.

[14] A third Do Not Track bill is directed exclusively at children. Representatives Ed Markey (D-MA) and Joe Barton (R-TX) introduced the "Do Not Track Kids Act of 2011," H.R. 1895, 112th Cong. (2011), which would amend the Children's Online Privacy Protection Act (COPPA) to prevent tracking on children's web sites without parental consent, create a teen privacy bill of rights, and establish an "eraser button" to allow deletion of online information about a minor.

[15] H.R. 654, 112th Cong. (2011) [hereinafter Speier bill].

including online browsing activity, unique identifiers, and personal information[16] such as name, postal address, email address, telephone number, government issued identification number, or financial account numbers and passwords.[17]

Senator Jay Rockefeller (D-WV) introduced the "Do-Not-Track Online Act of 2011" in May.[18] It would require the FTC to issues rules: (a) establishing a mechanism whereby consumer can simply and easily opt out of having their personal information collected online – including on mobile devices; and (b) prohibiting the collection of personal information from consumers who have opted out.[19] The Senate bill does not define "personal information."

Three additional bills address broader privacy concerns but ultimately reach similar issues regarding the collection and use of online consumer information, albeit without providing for a specific Do Not Track mechanism. Representative Bobby Rush (D-IL) reintroduced the "BEST PRACTICES" Act in February to provide baseline privacy standards for collecting and sharing personal information on the Internet.[20] In particular, this House bill would require that companies collecting personal information must provide: (a) clear and prominent notice

---

[16] The bills discussed herein use a variety of terms and varying definitions for the "personal information," "personally identifiable information," or "covered information" that is regulated by each bill. For the sake of simplicity in comparison, I refer to each as "personal information" in the text of my remarks.

[17] Speier bill, *supra* note 15, at §§ 2(3)(A), 3(a)-(b).

[18] S. 913, 112th Cong. (2011) [hereinafter Rockefeller bill].

[19] *Id.* at § 2(a)(1)-(2).

[20] Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 611, 112th Cong. (2011) [hereinafter Rush bill]. The bill was previously introduced as H.R. 5777, 111th Cong. (2010).

identifying who is collecting the information and how it will be used; and (b) a mechanism for consumers to opt out of having any of their "covered information" collected.[21] Moreover, the Rush bill would require express opt-in consent for: (a) disclosing personal information to third parties (except for certain joint marketing and service providers who are contractually bound to protect the information); (b) collecting, using, or disclosing sensitive information; (c) monitoring "all or substantially all" Internet browsing activity; or (d) any material change to privacy practices regarding previously personal information or sensitive information.[22]

Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the "Commercial Privacy Bill of Rights Act of 2011" in April.[23] This Senate bill would require the FTC to issue rules requiring companies that collect personal information to: (a) provide notice of their collection and use practices; and (b) provide an opt-out mechanism when using personal information in an unauthorized manner.[24] The Kerry-McCain bill would require an opt-in mechanism for: (a) collecting, using, or sharing of sensitive information; or (b) the use or sharing with third parties of previously collected personal information after a material change to

---

[21] Rush bill, *supra* note 20, at §§ 101, 102(a), 103. The Rush bill's definition of "covered information" includes an individual's name, postal address, email address, telephone number, government issued identification number, financial account numbers and passwords, unique persistent identifiers, or other related information. *Id.* at § 2(4).

[22] *Id.* at §§ 104, 105. The Rush bill defines "sensitive information" as including an individual's medical history, race or ethnicity, religious beliefs, sexual orientation, financial records, precise geolocation information, unique biometric data, or Social Security number. *Id.* at § 2(8)(A).

[23] S. 799, 112th Cong. (2011) [hereinafter Kerry-McCain bill].

[24] *Id*. at §§ 201, 202. The Kerry-McCain bill defines "personally identifiable information" as including an individual's first and last name, postal address, email address, telephone numbers, government issued identification number, financial account numbers and passwords, unique identifier information, or other related information. *Id*. at §§ 3(5).

privacy practices and where the use or sharing creates a risk of economic or physical harm.[25]

The day after the introduction of the Kerry-McCain bill in the Senate, Representatives Cliff Stearns (R-FL) and Jim Matheson (D-UT) introduced the "Consumer Privacy Protection Act of 2011" in the House.[26] This bill would require that, before collecting any personal information from a consumer, a company must provide: (a) notice regarding how the information will be collected and used; and (b) an opportunity to opt of the sale or disclosure of information.[27] Such an opt out, however, would not be required if the information is being transferred to an "information-sharing affiliate," defined as an affiliate that is either under common control of the covered entity or is contractually obligated to comply with the entity's privacy policy.[28] Unlike the Rush and Kerry-McCain bills, there are no circumstances for which the Stearns-Matheson bill would require opt-in consent.

In addition to transparency and opportunities for consumers to control aspects of the collection and use of their personal or sensitive information, these bills have a number of important things in common. First, some of the bills acknowledge the distinction between data collection and data security. For example, although the primary focus of the broad privacy bills

---

[25] *Id*. at § 202(a)(3). The Kerry-McCain bill defines "sensitive personally identifiable information" as including an individual's health records, religious affiliation, or personally identifiable information posing significant risk of economic or physical harm if lost, compromised, or disclosed without authorization. *Id*. at § 3(6).

[26] H.R. 1528, 112th Cong. (2011) [hereinafter Stearns-Matheson bill].

[27] *Id*. at §§ 4(a)-(b), 6(a). The Stearns-Matheson bill defines "personally identifiable information" as including an individual's first and last name, postal address, email address, telephone number, government issued identification number, financial account numbers, or other related information. *Id*. at § 3(8).

[28] *Id*. at §§ 3(7), 6(a).

consider the collecting and sharing of consumer information, both the Rush and Kerry-McCain bills each specifically require data security safeguards for collected data and obligations to retain personal or sensitive consumer information only so long as necessary to fulfill a legitimate business purpose or to comply with a legal requirement.[29] Both of these bills would provide for civil penalties for violations of the data security and retention provisions. Although less detailed, the Stearns-Matheson bill similarly requires "an information security policy . . . that is designed to prevent unauthorized disclosures or release" of personally identifiable information.[30]

Second, the bills make distinctions between sensitive personal information on the one hand and other information on the other. Indeed, presumably consistent with consumer expectations, all of the legislative proposals generally provide exceptions for first-party information collection related to the transaction or service.[31] Similarly, some of the bills proposed exclude aggregated or anonymized information.[32] The Rush and Kerry-McCain bills, however, draw the distinction that I have mentioned between sensitive and non-sensitive information, and require express opt-in consent regarding the collection, use, or sharing of sensitive information, such as an individual's medical records, religious affiliation, or

---

[29] *See* Rush bill, *supra* note 20, at §§ 301-303; Kerry-McCain bill, *supra* note 23, at §§ 301-302.

[30] Stearns-Matheson bill, *supra* note 26, at § 8.

[31] *See, e.g.*, Kerry-McCain bill, *supra* note 23, at § 202(a)(3)(A)(i); Rockefeller bill, *supra* note 18, at § 2(b)(1); Speier bill, *supra* note 15, at § 3(d)(1); Rush bill, *supra* note 20, at §§ 2(5)(A), 103(e); Stearns-Matheson bill, *supra* note 26, at §§ 4(a)(1), 6(a)(1).

[32] *See* Rush bill, *supra* note 20, at 501(a) (exempting aggregate information or "covered information or sensitive information from which identifying information has been removed"); Stearns-Matheson bill, *supra* note 26, at 3(8)(c) (exempting "anonymous or aggregate data, or any other information that does not identify a unique living individual" from "personally identifiable information").

information that, if disclosed, poses a significant risk of economic or physical harm.[33]

Third, the majority of the legislative proposals incorporate some manner of self-regulation. The Rush, Kerry-McCain, and Stearns-Matheson privacy bills all propose participation in approved and monitored self-regulation programs as a "safe harbor" from the legislation.[34] For example, the Rush bill would provide a safe harbor that would exempt companies from certain opt-in consent requirements, provided those companies participate in a universal opt-out program operated by self-regulatory bodies approved and monitored by the Commission.[35] Similarly, although neither the Speier nor Rockefeller bill proposes self-regulation, the Rockefeller bill directs the Commission, in designing standards and rules for the implementation for an opt-out mechanism, to take into consideration the mechanisms that have been proposed by industry thus far.[36]

III. The Online Industry's Implementation of Do Not Track

As things now stand, there is a handful of different mechanisms that purport to give consumers the choice to eliminate behavioral advertising, and some that purport to eliminate

---

[33] *See* Rush bill, *supra* note 20, at §§ 2(8)(A), 104(b); Kerry-McCain bill, *supra* note 23, at §§ 3(6), 202(a)(3). Although the Speier bill separately defines "sensitive information" (including medical history, race or ethnicity, religious beliefs, sexual orientation, financial records, precise geolocation information, unique biometric data, and Social Security number), the bill does not include specific provisions regarding the treatment of such information except for providing that anyone collecting sensitive information cannot be excluded from the status as a covered entity regulated under the bill. Speier bill, *supra* note 15, at 2(2)(B)(iii), 4(A).

[34] *See* Rush bill, *supra* note 20, at § 401; Kerry-McCain bill, *supra* note 23, at § 501; Stearns-Matheson, *supra* note 26, at § 9.

[35] Rush bill, *supra* note 20, at § 401.

[36] *See* Rockefeller bill, *supra* note 18, at § 2(c)(3)(A).

both tracking and targeted advertising.[37] The most prominent options developed to date are browser-related mechanisms associated with Microsoft's Internet Explorer 9, Mozilla's Firefox, and Google's Chrome,[38] and the self-regulatory regime set up by the Digital Advertising Alliance. I will discuss each of these in turn.

Microsoft's Internet Explorer 9 offers a "Do Not Track" mechanism which uses third-party domain blocking to prevent certain third-party websites from establishing contact or accessing the consumer's computer. The opt-in mechanism involves the use of "white lists" or "black lists," known as Tracking Protection Lists or "TPLs." These allow consumers to decide which third-party websites they will allow to access, and therefore potentially track, their online activity. In order to opt in, the user goes to the browser's "Safety" settings, where there is the option to create a personalized TPL (based on script and tracking cookie information from previously visited websites) or to subscribe to one of five already-created TPLs.[39]

Although consumers are given the choice to create their own TPL, it may be difficult for them to do so in an informed manner because they do not have access to complete details about

---

[37] The World Wide Web Consortium (W3C) has organized a Tracking Protection Working Group to standardize the "Do Not Track" opt-out tools already a part of Firefox, Internet Explorer and Safari. *See* W3C's New 'Do Not Track' Group Aims for Better Web Privacy, Sept. 9, 2011, *available at* http://www.webmonkey.com/2011/09/the-w3c-accepts-do-not-track-project-for-better-web-privacy/. The W3C process is notable in that (1) it is open to a broad group of stakeholders, including publishers, browser makers, the advertising industry, analytics companies, and public-interest groups; (2) it is primarily a public, on-the-record process; (3) any standards it produces are voluntary; and (4) it is coordinated by a standards body that has experience in navigating competition issues in standard-making.

[38] Apple has also implemented Do Not Track in their Safari browser; however, that mechanism is not discussed in these remarks.

[39] Microsoft points to five TPLs. There are, however, several other TPLs in use beyond the five that Microsoft includes.

the information collection, use and sharing practices of the websites they may or may not want to block. The already-created TPLs are furnished in large part by self-interested parties, such as consumer advocacy groups or industry trade associations, who have their own views on whether and to what extent consumers should allow "tracking" of their non-sensitive data. Microsoft does nothing to inform consumers about consequences of opting-in to a TPL. Furthermore, the user does not know which sites are on the already-created TPLs – only after the user selects and downloads a particular TPL can they see which sites have been blacklisted or whitelisted.

Mozilla offers another browser-based approach to "Do Not Track" in its latest version of Firefox. This mechanism, if enabled, sends an HTTP "Do Not Track" header along with the user's request to access a website. The website receives the Do Not Track request and is supposed to honor it. Although this approach does not interfere with the functionality of websites or their content, the mechanism is basically unenforceable – it relies entirely on the good faith of the recipient third party to honor the Do Not Track request. Furthermore, the mechanism, activated by a single click in the "Tell websites I do not want to be tracked" box of the "advanced" settings, does not fully inform users of the consequences of their choice. Recently, Mozilla released a "Field Guide"[40] which purports to inform consumers of the types of tracking that are occurring and the consequences of opting out. However, any usefulness that these disclosures might offer is undercut by the fact that they are not proximate to the choice mechanism. In addition, it is not clear how complete or accurate are the descriptions of the tracking that is now occurring or the consequences of opting out. Finally, despite being the

[40] *Mozilla Publishes Developer Guide on DNT; Releases DNT Adoption Numbers*, MOZILLA PRIVACY BLOG (Sept. 8, 2011), http://blog.mozilla.com/privacy/2011/09/08/mozilla-publishes-developer-guide-on-dnt-releases-dnt-adoption-numbers/.

simplest Do Not Track mechanism to enable, only five percent of Firefox 4 users have enabled the feature to date.[41] This rate of implementation by users makes me wonder whether or not consumers are actually aware of the existence of this Do Not Track mechanism – or alternatively, how concerned consumers actually are about being tracked.

The third browser-based Do Not Track mechanism is offered by Google, which has a plug-in called "Keep My Opt-Outs" that can be downloaded to the Chrome browser.[42] "Keep My Opt-Outs" purports to allow a user to "permanently opt out of ad tracking from all companies that offer opt-outs through the industry self-regulation programs,"[43] and offers automatic updates to include new companies as they continue to join self-regulatory programs. As such, the plug-in comes to grips with two major problems faced by some other Do Not Track mechanisms: the impermanence of cookie-based solutions, which disappear when the consumer clears his or her cookies, and the need to stay up-to-date with new ad platforms as they join the self-regulatory programs. The web page containing the download for the plug-in mentions some of the negative consequences of installation: the ads that the consumer sees may be less relevant and diverse and may also result in less profitable ads for the consumer's favorite websites.[44]

However, the Google mechanism appears to only limit the consumer from receiving

---

[41] *Id.*

[42] Google has made the code for the extension available to the public on an open-source basis so that developers can adapt it for use with other browsers.

[43] *Keep Your Opt-Outs*, GOOGLE PUBLIC POLICY BLOG (Jan. 24, 2011), http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.

[44] *See Keep My Opt-Outs*, GOOGLE CHROME WEB STORE, https://chrome.google.com/webstore/detail/hhnjdplhmcnkiecampfdgfjilccfpfoe (last updated July 30, 2011).

targeted advertising. "Keep My Opt-Outs" does not stop websites from otherwise tracking a consumer's online activity, and cookies continue to be installed on the consumer's computer. In addition, since the plug-in only prevents "ad" tracking and serving by companies that are members of self-regulatory programs, such as the Digital Advertising Alliance, the scope of the mechanism is limited – consumers would still be tracked and served advertising by any companies that were not members of a self-regulatory program.

The final mechanism uses cookies to effectuate the choice mechanism.[45] The Digital Advertising Alliance (DAA), the self-regulatory body comprised of the nation's largest media and marketing associations, launched its self-regulatory program for online behavioral advertising in 2010.[46] The program requires that member companies engaged in online behavioral advertising provide "enhanced notice" to consumers about collection and use practices, and offer a choice mechanism with respect to the collection and use of data ***for online behavioral advertising purposes***.[47] For most program participants, this "enhanced notice"

---

[45] *See Frequently Asked Questions about Online Behavioral Advertising and the Consumer Opt Out Page: About the Consumer Opt out Page and what it does – and doesn't – do*, THE SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING (DIGITAL ADVERTISING ALLIANCE), http://www.aboutads.info/how-interest-based-ads-work#about-opt-out (last visited Oct. 7, 2011) ("Online companies use cookies to remember users' preferences about the collection and use of data for online behavioral advertising. [The DAA's] 'opt out cookies' help the participating companies to 'recognize' users who have opted out of receiving such advertising and to respect that choice.").

[46] The program is intended to implement their "Self-Regulatory Principles for Online Behavioral Advertising," which were released in July 2009. *See Self-Regulatory Principles for Online Behavioral Advertising*, THE SELF-REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING (DIGITAL ADVERTISING ALLIANCE) (July 2009), http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

[47] As a baseline, DAA only requires that companies give consumers the option of opting out of targeted advertising. While some companies may go above and beyond this threshold requirement and allow consumers to opt out of all tracking, it is not specifically required by the

involves the use of an icon located on or near the advertisement itself, which takes users to a page containing the required disclosures and an opt-out mechanism.[48]

The disclosure regime could use improvement, however, in several respects. First, some have suggested that the icon may not be prominent enough to actually prompt consumers to click on it for the required disclosures and the instructions on opting out. Second, assuming a consumer finds the icon and clicks on it, the presentation and organization of the disclosures that appear vary depending upon the entity that is serving the icon.[49] While users are informed eventually about some of the consequences of adopting the mechanism (in particular, loss of ad relevance and the effect on the economics of Internet advertising), it takes some perseverance and more than one or two "clicks" to reach this pertinent information. And finally and perhaps

---

DAA. *See Self-Regulatory Principles for Online Behavioral Advertising Implementation Guide*, DIGITAL ADVERTISING ALLIANCE 9-10 (Oct. 2010), http://www.aboutads.info/resource/download/OBA%20Self-Reg%20Implementation%20Guide%20-%20Full%20Text.pdf ("As a Third Party that operates across multiple unaffiliated sites, you should . . . provide consumers with the ability to exercise choice with respect to collection and use of data for OBA purposes . . . .").

[48] *Id*. at 8-11. *See also id*. at 3: "Advertising Option Icon: The program promotes the use of an icon and accompanying language, to be displayed in or near online advertisements or on Web pages where data is collected and used for behavioral advertising. Advertising Option Icon indicates that the advertising is covered by the self-regulatory program, and by clicking on it consumers will be able to link to a clear disclosure statement regarding the data collection and use practices associated with the ad as well as an easy-to-use opt-out mechanism."

[49] The icon is served by three entities – Evidon, TRUSTe, and DoubleVerify – as well as by individual companies. These entities have discretion in how information is presented. *See, e.g.*, *Navigating Online Consumer Privacy*, MEDIA CONTACTS (June 2011), *available at* http://www.mediacontacts.com/wp-content/uploads/MC_Insight_Privacy_June11b.pdf ("The DAA has certified a few technology providers, such as Evidon (formerly Better Advertising Project), DoubleVerify, and TRUSTe, to offer a turnkey solution for implementing OBA compliance. All these solutions utilize the 'Advertising Option Icon.' This icon is integrated into the advertising creative and serves to notify the consumer that the ad they are being served is behaviorally targeted to them. On websites, the icon is integrated into the footer of any pages collecting behavioral data and serves a similar purpose of notice in the ad.").

most importantly, the "choice" mechanism is merely an ad preference manager dressed as a "Do Not Track" mechanism; for the most part, it only allows consumers to manage their behavioral advertising interest categories or to opt out of receiving targeted advertising. It does not, however, stop data collection or the placement of cookies on consumers' computers.[50]

IV. Analysis

There appear to be at least four overarching shortcomings with the current industry or "self-regulatory" Do Not Track mechanisms proposed thus far. The first is that some of the mechanisms only allow consumers the ability to opt out of behavioral advertising, but not all "tracking," and there is a failure to alert consumers to this fact. A recent study conducted by Stanford researchers indicates that there is consumer confusion on this issue and that consumers – perhaps because of the moniker "Do Not Track" – think that they are opting out of being tracked, not just opting out of receiving targeted advertising.[51] Both the Google "Keep My Opt-Outs" and the DAA self-regulatory program suffer from this shortcoming and neither one adequately informs the consumer of the limited scope of the opt out.

Second, with regard to some of the Do Not Track mechanisms, although their disclosures

---

[50] While some companies allow consumers to opt out of all data collection and use, none of the disclosures seem to adequately explain to consumers what exactly they are opting out of. Preliminary research suggests that most users do not understand the function of DAA opt-outs, and mistakenly believing that opting out will stop data collection altogether. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising* at 16-18 (Aug. 16, 2010), *available at* http://www.aleecia.com/authors-drafts/tprc-behav-AV.pdf; Aleecia M. McDonald, *Position Paper for the W3C Do Not Track Workshop* (Apr. 2011), *available at* http://www.w3.org/2011/track-privacy/papers/AleeciaMcDonald.pdf.

[51] Jonathan Mayer, *Tracking the Trackers: Early Results*, STANFORD LAW SCHOOL: CENTER FOR INTERNET AND SOCIETY (July 12, 2011), http://cyberlaw.stanford.edu/node/6694. *See also Stanford Study Shows Online Consumer Privacy Tools Flawed*, SILICONVALLEY.COM, July 21, 2011, http://www.siliconvalley.com/ci_18524333.

may be sufficient to warn consumers that one of the consequences of opting out will be that the consumer will lose access to relevant targeted advertising, most of the notices do not warn of other possible consequences of opting out. For example, I remain concerned about the possibility that "across-the-board" opting out by consumers may reduce the overall financing that supports free content across the Internet, and accordingly, result in a decrease in innovation. There is limited disclosure on this point. For example, only one program – the Google plug-in – alerts consumers that engaging the mechanism might result in less profitable advertising for their favorites websites. The DAA program explains how Internet advertising funds free content, but that information is not presented clearly and prominently. None of the mechanisms specifically alert consumers that the result of selecting a mechanism may also result in more obtrusive advertising, although perhaps that fact may be surmised by the notice that they will receive less relevant advertising.

The third shortcoming is that the "proof is in the pudding." I do not see much evidence that these mechanisms are really working to alert consumers about the existence of tracking and online behavioral advertising. For example, the rates of adoption are very low. As I mentioned earlier, only five percent of Firefox users have enabled the feature. With respect to the DAA program, a recently published press release stated that more than "80 million U.S. internet users [were] served ads with Ad Choices icon" and that "the 50 billionth impression of the Advertising Choices Icon" was served on behalf of the licensees of the DAA. However, these numbers just represent ads that consumers may or may not see. The press report provides no indication as to whether consumers are clicking on the icon to get more information, and actually notes that "[e]ven as the program's growth and the number of companies . . . have accelerated, the opt-out

rate on impressions served . . . remains extremely low."[52] A corollary to this is the question whether the DAA opt-out mechanism actually functions in the way that DAA members represent that it will. There has been a recent study conducted by the CyLab at Carnegie Mellon University suggesting – again with regard to the DAA self-regulatory program – that the program does not always function as represented.[53]

The fourth shortcoming may be even more serious and incurable. The current proposals all involve, to some degree, well-entrenched firms (whether as implementers or participants). Those firms may favor barriers to consumer tracking in order to create or raise entry barriers to rivals instead of solely to protect consumers against behavioral tracking. Let me set the table a bit. Some of the participating firms offer advertising that is not display advertising, which arguably is heavily dependent on behavioral tracking. Moreover, some of those firms offer their advertising through vehicles that are not as accessible to rivals offering display advertising. Those firms may be tempted to sail under the consumer protection banner when their predominant interest is instead to disadvantage rivals that are more heavily dependent on advertising reliant on behavioral advertising. Former Commissioner Kovacic has remarked that

---

[52] Press Release, Evidon, Evidon Passes 50 Billion Impressions Served, 80 Million Unique Users (Aug. 4, 2011), *available at* http://blog.evidon.com/2011/08/04/evidon-passes-50-billion-impressions-served-80-million-unique-users-press-release/.

[53] Saranga Komanduri et al., *AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements*, CYLAB at CARNEGIE MELLON UNIVERSITY (Mar. 30, 2011), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11005.pdf. *See also* Jacqui Cheng, *Study Finds 12.5% of Companies Violating Own Do-Not-Track Policies*, (July 2011), http://arstechnica.com/tech-policy/news/2011/07/study-finds-not-all-voluntary-do-not-track-efforts-are-going-smoothly.ars.

we are a better antitrust agency for having a consumer protection mission.[54] That is surely true to a point. But we cannot be blinded so much by our zeal to protect consumers from behavioral tracking that we lose sight of our competition mission. There is probably nothing worse than to have firms with an anti-competitive agenda designing consumer protection initiatives.

V. Conclusion

Where does all of this leave us? From what I have seen thus far, Do Not Track is clearly a difficult technical issue – both as a matter of definition and implementation – without a perfect – or even a pragmatic – solution. In short, I have reservations about whether any of the self-regulatory programs, including the DAA program, really do present consumers with a mechanism that will both fully inform them before they make a choice about whether to allow tracking of their non-sensitive information or not and whether they can and will really exercise that choice. I would suggest the jury is still out about both questions. Accordingly, I would suggest further that it would be premature to put all of our eggs in the self-regulatory basket – either as part of an industry solution or legislative solution – to resolve the Do Not Track question.

---

[54] *See, e.g.*, William E. Kovacic, *Competition Policy, Consumer Protection, and Economic Disadvantage*, 25 WASH. U. J. LAW & POL'Y 101, 114 (2007) (observing that "[c]onsumer protection laws are important complements to competition policy").