Statement of Commissioner J. Thomas Rosch, Dissenting in Part
Privacy and Data Security: Protecting Consumers in the Modern World
Testimony before the
Senate Committee on Commerce, Science, and Transportation
June 29, 2011

The root problem with the concept of "Do Not Track" is that we, and with respect, the Congress, do not know enough about most tracking to determine how to achieve the five attributes identified in today's Commission testimony, or even whether those attributes can be achieved.[1] Considered in a vacuum, the proposed Do Not Track attributes set forth in today's testimony can be considered innocuous, indeed even beneficial. However, the concept of Do Not Track cannot be considered in a vacuum. The promulgation of five attributes, standing alone, untethered to actual business practices and consumer preferences, and not evaluated in light of their impact upon innovation or the Internet economy, is irresponsible. I therefore respectfully dissent to the portions of the testimony that discuss and describe certain conclusions about the concept of Do Not Track.[2]

---

[1] As described in today's and prior testimony, the five attributes are:

First, any Do Not Track system should be implemented universally, so that consumers do not have to repeatedly opt out of tracking on different sites. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be deleted if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes. Finally, an effective Do Not Track system would go beyond simply opting consumers out of receiving targeted advertisements; it would opt them out of collection of behavioral data for all purposes other than product and service fulfillment and other commonly accepted practices.

[2] The concept of Do Not Track was presented in the preliminary Staff Privacy Report, issued in December 2010. *See* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. At that time, the Commission requested public comment on the issues raised in that preliminary report.

It is easy to attack practices that threaten data security. There is a consensus in both the United States and Europe that those practices are pernicious, and the Commission has successfully challenged them.[3] It is also easy to attack practices that compromise certain personally identifiable information ("PII") like one's social security number, confidential financial or health data, or other sensitive information, such as that respecting children. The consensus about those practices in the United States is reflected in federal statutes like the Health Insurance Portability and Accountability Act ("HIPAA"), the Gramm-Leach-Bliley Act ("GLBA"), and the Children's Online Privacy Protection Act ("COPPA"), and the Commission has likewise successfully challenged practices that violate those statutes.[4] On the other hand, some of the "tracking" that occurs routinely is benign, such as tracking to ensure against advertisement repetition and other tracking activities that are essential to ensuring the smooth operation of websites and internet browsing. But we do not know enough about other kinds of

---

[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).

[4] *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).

"tracking" – or what consumers think about it – to reach any conclusions about whether most consumers consider it good, bad or are indifferent.

More specifically, it is premature to endorse any particular browser's Do Not Track mechanism. One type of browser mechanism proposed to implement Do Not Track involves the use of "white lists" and "black lists" to allow consumers to pick and choose which advertising networks they will allow to track them.[5] These lists are furnished by interested third parties in order to prevent the types of tracking that consumers supposedly do not want.[6] It is clear from these "lists" what the interested third parties think about the tracking on the lists (or not on the lists). However, it is not clear whether most consumers share those views, or even understand the basis upon which the "list" was created. Another proposed browser Do Not Track mechanism operates by sending a Do Not Track header as consumers surf the Internet. This mechanism would only eliminate tracking to the extent that the entities receiving the Do Not Track header understand and respect that choice. Theoretically at least, this mechanism could block all tracking if it does not offer customization and preserve the ability to customize.[7] This

---

[5] Many, if not all, browsers currently allow consumers to customize their browser to prevent the installation of, or delete already installed, cookies that are used for tracking.

[6] Some Tracking Protection Lists (TPLs) allow any criterion to be used to decide which sites go on a TPL and which do not. In some cases, consumers may have the option to create their own TPL. However, as discussed below, neither the FTC, nor consumer advocates, nor consumers themselves, know enough about the tracking, collection, retention and sharing practices of online entities.

[7] In addition, it is not clear how the "recipient" of the Do Not Track header would respond to such a request when the consumer has otherwise indicated that he or she wishes to have the recipient customize the consumer's experience.

is important because there may be some tracking that consumers find beneficial and wish to retain.

Beyond that, consumers (including consumers that are surveyed by interested third parties) are generally not fully informed about the consequences – both bad and good – of subscribing to a Do Not Track mechanism.[8] They are not always told, for example, that they may lose content (including advertising) that is most pertinent and relevant to them. Neither are they told that they may lose free content (that is paid for by advertising). Nor are they told that subscribing to a Do Not Track mechanism may result in more obtrusive advertising or in the loss of the chance to "sell" the history of their internet activity to interested third parties. Indeed, they are not even generally told what kinds of tracking are going to be eliminated. On the other hand, consumers are not told that tracking may facilitate the compilation of a consumer "profile" through the aggregation of information by third parties to whom it is sold or with whom it is shared (such as insurance companies engaged in "rating" consumers). One reason that consumers are not told about the latter consequence is that we do not know enough about what information is being collected and sold to third parties to know the extent to which such aggregation is occurring.

[8] That is not to say that current technology cannot facilitate these disclosures. However, it is critical that advertisers and publishers take the opportunity to explain to consumers what their practices are and why they might be beneficial.

One thing is certain though: consumers cannot expect simply to "register" for a Do Not Track mechanism as they now register for "Do Not Call."[9] That is because a consumer registering for Do Not Call needs to furnish only his or her phone number. In the context of the Do Not Call program, each telephone already has a unique identifier in the form of a telephone number. In contrast, there is no such persistent identifier for computers. For example, Internet Protocol ("IP") addresses can and do change frequently. In this context, creating a persistent identifier, and then submitting it to a centralized database, would raise significant privacy issues.[10] Thus, information respecting the particular computer involved is essential, and that kind of information cannot be furnished without compromising the very confidential information that consumers supposedly do not want to share. In addition, multiple users of the same computer or device may have different preferences, and tying a broad Do Not Track mechanism to a particular computer or device does not take that into consideration.

This is not to say that a Do Not Track mechanism is not feasible. It is to say that we must gather competent and reliable evidence about what kind of tracking is occurring before we embrace any particular mechanism. We must also gather reliable evidence about the practices most consumers are concerned about. Nor is it to say that it is impossible to gather that

---

[9] *See* Prepared Statement of the Federal Trade Commission on Do Not Track Before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, Dec. 2, 2010, *available at* http://www.ftc.gov/os/testimony/101202donottrack.pdf.

[10] A new identifier would be yet another piece of PII that companies could use to gather data about individual consumers.

evidence. The Commission currently knows the identities of several hundred ad networks representing more than 90 percent of those entities engaged in the gathering and sharing of tracking information. It is possible to serve those networks with compulsory process, which means that the questions about their information practices (collection, tracking, retention and sharing) must be answered under oath. That would enable the Commission to determine and report the kinds of information practices that are most frequently occurring. Consumers could then access more complete and reliable information about the consequences of information collection, tracking, retention and sharing. Additionally, the Commission could either furnish, or, depending on technical changes that may occur, facilitate the furnishing of, more complete and accurate "lists" and consumers would then have the ability to make informed choices about the collection, tracking, retention and sharing practices they would or would not permit.

This course is not perfect. For one thing, it would take time to gather this information. For another thing, it would involve some expense and burden for responding parties (though no more than that to which food and alcohol advertisers who currently must answer such questionnaires are exposed). Consumers would also be obliged to avail themselves of the information provided by the Commission. But I respectfully submit that this course is superior to acting blindly, which is what I fear we are doing now.