Federal Trade Commission

INFORMATION AND PRIVACY:
IN SEARCH OF A DATA-DRIVEN POLICY

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

at the

Technology Policy Institute Aspen Forum
Aspen, Colorado
August 22, 2011

I am pleased to have been asked to participate on this panel today. From my standpoint, this topic couldn't be more timely. While privacy has been a priority for the Federal Trade Commission for the last several years, privacy issues – in particular, those relating to policy – have received even more attention from the Commission recently.

I. Background

As many of you may know, beginning in December 2009, the FTC held a series of "Privacy Roundtables" in Washington, DC and northern California.[2] The first roundtable focused on the risks and benefits of information-sharing practices, consumer expectations regarding these practices, behavioral advertising, information brokers, and the adequacy of

[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] FTC Press Release, FTC to Host Public Roundtables to Address Evolving Consumer Privacy Issues (Sept. 15, 2009), *available at* http://www.ftc.gov/opa/2009/09/privacyrt.shtm.

[8] FTC Press Release, FTC Extends Deadline for Comments on Privacy Report Until February 18 (Jan. 21, 2011), *available at* http:/

[10] *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 informa

consumer harm occurs when such information is not treated with the proper deference. Indeed, federal statutes – such as the Health Insurance Portability and Accountability Act (HIPAA), 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.[11] I think that – for purposes of behavioral tracking and advertising – sensitive information like this 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 information defined as "sensitive" could only occur after consumers "opted in" to these practices.[12] Alternatively, for some types of sensitive information, it may be desirable to prohibit entirely its collection and use for behavioral tracking and advertising.

[11] Likewise, 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).

[12] 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.

[13] 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 Federal Trade Commission 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).

[14] *See, e.g.*, Emily Steel, "A Web Pioneer Profiles People By Name," W.S.J., Oct. 25, 2010,

statement accompanying the issuance of the Staff's preliminary Privacy Report, the information we at the FTC (Staff as well as Commissioners) have is based on imperfect consumer surveys and the preconceived notions of interested industries or consumer groups.[15]

Beyond that, consumers (including consumers that are surveyed by interested third parties) are generally not fully informed about the benefits or consequences of subscribing to a Do Not Track mechanism.[16] 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

---

[15] First, based on testimony by some workshop participants, the Report asserts that the use being made of online and offline consumer information is contrary to consumer understanding. *See* Report at 25-26, 29. The Report also alleges that "consumer surveys have shown that a majority of consumers are uncomfortable with being tracked online." *Id*. at 29. Although some consumers may hold that view (which would be sufficient to make the practice of behavioral tracking a "material" fact), as the Report itself acknowledges it is inaccurate to assert that consumer surveys establish that "a majority of consumers" feel that way. *Id.* at 29 n.72. As others have observed, consumer surveys vary considerably in this respect. Of course, many consumers do not opt in to behavioral tracking when asked. But an even higher percentage do not opt out when given the chance to do so (and there is no solid evidence that this is because they have not been able to make an informed choice). *See, e.g.*, Thomas M. Lenard and Paul H. Rubin, *Privacy and the Commercial Use of Personal Information: The Case of Customer Proprietary Network Information*, Progress on Point, at 6 (Aug. 2007) ("[I]n testimony before the FTC on the experience of one firm, a witness indicated that, when the default was opt-in, 85 percent of consumers chose not to provide their data. In contrast, 95 percent chose to provide their data when the default was opt-out"), *available at* http://www.pff.org/issues-pubs/pops/pop14.15lenardrubinCPNIprivacy.pdf.

[16] 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.

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). As noted above, 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.

III. A Possible Solution

First, before we proceed down the road toward championing a "Do Not Track" system, we should gather competent and reliable evidence about what kind o

the web site use

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

advertising networks they will allow to track them.[18] These lists are furnished by interested third parties in order to prevent the types of tracking that consumers supposedly do not want.[19] 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.

Fourth, based on these categories, instead of relying on third parties, the FTC could design disclosures and other consumer education materials in order to enable consumers to make fully-informed decisions when they select a Do Not Track option. We are the experts when it comes to determining what constitutes full and complete disclosure, and we will have the benefit of having collected the underlying information from the advertising networks. Consumers need to be informed of the consequences of the option they are selecting before they do so. Those consequences may weigh in favor of a more customized Do Not Track mechanism, which could cover some or all of the categories. Or, the consequences of choosing of Do Not Track mechanism (for example, the loss of relevancy, the loss of free content, the replacement of current advertising with even more obtrusive advertising, and the loss of an opportunity to sell or franchise the right to track oneself) may weigh in favor of allowing track. In any event, the consumer could make that informed choice.

I am a big fan of consumer choice. But only if it is informed consumer choice. I am not

---

[18] 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.

[19] 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.