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.

existing legal and self-regulatory frameworks.[3] The second day-long roundtable, held on January 29, 2010 in Berkeley, California, examined how technology affects consumer privacy, including its potential to weaken and/or strengthen privacy protections. This roundtable also explored privacy implications of several evolving technologies, like social networking, cloud computing, and mobile computing.[4] The third and final roundtable, held in March 2010 in Washington, DC, addressed Internet architecture and privacy issues, and included panel discussions focusing on health and other sensitive consumer information. This roundtable concluded with a panel that discussed the cumulative lessons learned from all three roundtables and possible directions forward.[5] Public comment periods followed each of the roundtables.[6]

The roundtables and public comment process culminated in the December 2010 issuance of a preliminary staff report entitled, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers."[7] As indicated by its title, the preliminary Report proposes a new framework to protect consumer privacy; it also suggests

---

[3] FTC Press Release, FTC Releases Agenda for First Privacy Roundtable and Announces Date of Second Roundtable (Nov. 17, 2009), *available at* http://www.ftc.gov/opa/2009/11/privacyrt.shtm.

[4] FTC Press Release, FTC Releases Agenda for Second Roundtable on Consumer Privacy and More Information for Third Roundtable (Jan. 21, 2010), *available at* http://www.ftc.gov/opa/2010/01/roundtable.shtm.

[5] FTC Press Release, FTC Releases Agenda for Final Roundtable on Consumer Privacy (Mar. 10, 2010), *available at* http://www.ftc.gov/opa/2010/03/privacy.shtm.

[6] Public comments *available at* http://www.ftc.gov/os/comments/privacyroundtable/index.shtm.

[7] 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 (hereinafter "Report").

implementation of a "do-not-track" mechanism so consumers can choose whether to allow the tracking of certain data, such as their online searching and browsing activities, in order to serve them targeted advertising. The Report contained a list of questions for comment, and the public comment period ended February 18th.[8]

I agreed with the Commission's decision to issue the 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, but I wrote separately to explain my serious reservations about some of the proposals advanced in the Report.

Since the issuance of the preliminary Staff Report in December, the Commission has been asked several times by Congress to testify on issues related to privacy and the concept of "Do Not Track." These hearings have provided further opportunity for discussion about the "Do Not Track" concept, and I have written separate statements (and an op-ed piece) to explain the serious reservations I have about the implementation of "Do Not Track."[9] I would like to take this opportunity today to highlight some of the overarching issues that I think are important in this debate.

---

[8] 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] *See* Statement of Commissioner J. Thomas Rosch, Dissenting in Part, 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 of the House Committee on Energy and Commerce (July 14, 2011), *available at* http://www.ftc.gov/os/2011/07/110714roschdissentingstatement.pdf; 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), *available at* http://www.ftc.gov/speeches/rosch/110629privacytestimony.pdf; J. Thomas Rosch, "The Dissent: Why One FTC Commissioner Thinks Do Not Track is Off-Track," ADVERTISING AGE, March 24, 2011.

II. Challenges Presented

As a preliminary matter, for purposes of discussing a privacy framework, I draw 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). There is a consensus in both the United States and Europe that practices that threaten data security are pernicious, and the Commission has successfully challenged them.[10] My remarks today are focused on the issues surrounding data collection, use, and retention, in particular, as they relate to the concept of "Do Not Track."

First, I think we need to examine whether all data should be treated equally. As a preliminary step in determining how to regulate information flows, it might be helpful to recognize that there is a qualitative range in the types of information that are being collected from consumers. I think that we can probably all agree 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. It is indisputable that

---

[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 information security).

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.

However, I do not think that all other types of information that might be collected, tracked or otherwise compiled – like consumer preferences, browsing history, information that is not personally identifiable, demographic and age information – necessarily deserves the same deference and protection. Indeed, some of the "tracking" that occurs routinely is completely innocuous, such as tracking to ensure against advertisement repetition and other tracking activities that are essential to ensuring the smooth operation of web sites and internet browsing.

---

[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.

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.[13] On the other hand, some have argued persuasively that if enough "benign" information is collected and compiled about a particular individual, the resulting profile could raise privacy concerns.[14]

Second, I am not convinced that we are in possession of accurate information about how consumers feel about the collection, use, sharing and retention of "sensitive" versus "less sensitive" information. Nor do we know enough yet about the scope of "tracking" and "profiling" to reach any conclusions about how to regulate these practices. These practices are opaque – we do not know the range of information that is being tracked or how that information is being used, shared or retained. As a result, we can not know how consumers feel about these practices: we don't even fully understand these practices. As I pointed out in my separate

---

[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, *available at* http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

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 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. The Commission currently knows the identities of several hundred advertising networks and related entities that represent more than 90 percent of the behavioral tracking and advertising industry. The Commission could serve those entities with compulsory process, and direct them to answer under oath questions about their information practices (collection, use, sharing and retention).

Second, once this information is gathered, information collection, use, sharing and retention practices can be categorized. While the process of collecting this data will inform the types of categories, for illustrative purposes, I offer a few examples. One category would be tracking that is obviously technical in nature, such as tracking to prevent the repetitive serving of the same advertising, or tracking to prevent fraud. Another category might consist of "first party" tracking (as described by FTC Staff in its Online Behavioral Advertising Report) whereby

the web site uses the information to improve the consumer's experience on the web site but does not share the data with others. A third category could involve instances where there is tracking across web sites and this compilation of tracking data is used to serve targeted advertising to consumers through a network of web sites. If advertising networks and their related entities then share that tracking information with other third parties, that behavior might require a separate category. Categories could also be developed based upon the types of information that is collected – for example, tracking mechanisms that collect sensitive information would be categorized separately. We should also take into consideration the sharing of information that enables the creation of a "profile" of a particular individual and whether that profile contains sensitive information, or seemingly benign information that when aggregated, ultimately becomes so personalized as to be considered sensitive. Gathering this information and categorizing it would be beneficial in many ways.

Third, I would suggest that it could be used to create "white lists" and "black lists" based on categories. Such lists could be used by the Do Not Track mechanisms being implemented by the browsers. As things now stand, there are a handful of mechanisms that purport to eliminate behavioral advertising, and some that purport to eliminate both tracking and targeted advertising.[17] 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

[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.

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. There is no doubt in my mind that most consumers do not want to take chances with their privacy. They want to zealously guard against identity theft and the use by others of truly personal information like health information, financial information, information about their sexual preferences and practices, and other highly sensitive information. For that kind of information, an opt-in option may be perfectly appropriate. On the other hand, as economist Steve Salop recently reminded us, there is no reliable data on what percentage of consumers insist on this high level of protection against behavioral tracking. 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.

That is why I have so vigorously supported clear, complete and accurate notices to consumers about what information sellers will and will not protect before consumers are obliged to make their choices. I consider the Commission's insistence that such notices be given to be our most significant contribution to consumer protection.[20]

---

[20] 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, made unsupported claims about what percentage of consumers favored protecting themselves against behavioral tracking (as opposed to pure privacy breaches), and suggested that "notice" might be replaced by a new and untested paradigm.

This course is not perfect. I acknowledge that various criticisms have been leveled at this process. To begin with, it would take time to gather this information from industry members. For example, the FTC needs to obtain approval from the Office of Management and Budget when sending out information requests to more than nine respondents. Consumers would also be obliged to avail themselves of the information provided by the Commission. I do not consider these to be legitimate criticisms nor insurmountable obstacles: we should have reliable information of this kind before we proceed further, and accuracy is more important than speed.

Additionally, it has been said that there are too many firms tracking and selling consumer behavior and hence too many potential recipients of questionnaires respecting the practices that are occurring. I do not consider this a legitimate objection either: as I noted earlier, there are approximately 300 advertising networks and related entities that represent the vast majority of this industry. Using statistical tools we could obtain relevant, representative information about the data collection, use, sharing and retention practices of this industry. We are in no position to advise Congress on legislation or engage in crafting self-regulatory guidelines unless we are in possession of reliable information of this kind.

Moreover, this course would involve some expense and burden for responding parties (though no more than that to which members of the food, alcohol and tobacco industries who currently must answer such questionnaires are exposed).

Finally, some have pointed out that such questionnaires will only take "a snapshot in time"; they will not disclose what information practice these entities will engage in prospectively. I do not think that this is a show-stopper either: our recent consent decree with Google Inc. demonstrates that the Staff has the enforcement tools necessary to address issues that arise when companies' information practices violate the terms of their privacy policies.

I understand that this will not be an easy path. But I respectfully submit that this course is superior to acting blindly, which is what I fear we are doing now with respect to our premature endorsement of "Do Not Track."

IV. Conclusion

Finally, as these suggestions are put into practice, the resulting choices will enable policy-makers to proceed on the basis of reliable information about the information practices that consumers really care about, on the one hand, and those they do not, on the other hand. To the extent that additional safeguards are needed, this process would also provide legislators with useful information.