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

INTRODUCTION

In December 2010, the Commission issued a preliminary staff privacy report ("Report") in order to continue the dialogue on issues related to consumer privacy and to solicit comment on a proposed new framework for how companies should protect consumers' privacy. Although I concurred in the decision to issue the Report and seek critical comment on the issues it raised, I have serious reservations about some of the proposals advanced in the Report, including the concept of "Do Not Track."

As a guide to Congress about what privacy protection law should look like,[1] the Report is flawed. First, insofar as the Report suggests that a new framework for consumer privacy should replace "notice" (or "harm") as the basis for Commission challenges relating to consumer privacy protection, that is unnecessary. A privacy notice that is opaque or fails to disclose material facts (such as the fact that consumer information may be shared with third parties) is deceptive under Section 5. That is particularly true if the sharing of the information may cause tangible harm. Moreover, Section 5 liability could not be avoided by eschewing a privacy notice

[1] The Report acknowledges that it is intended to "inform policymakers, including Congress, as they develop solutions, policies, and potential laws governing privacy." *See* Report at i, 2.

altogether both because that would generally be competitive suicide and because that course would be deceptive in that it would entail a failure to disclose material facts.[2]

Second, insofar as the Report suggests that "notice and choice" has ever been a basis for law enforcement at the Commission (*see* Report at iii, 8-11), that suggestion is unfounded. Although the Commission has on several occasions challenged privacy notices that it considered deceptive, it has never challenged a firm's failure to offer a particular kind of "choice." For example, the Commission has never challenged an opt-out mechanism on the ground that it should have been an opt-in mechanism. Indeed, if the notice has been adequate, consumers have generally not had any choice other than to "take or leave it," and that choice has never been considered to be a Section 5 violation unless what was represented in the notice was different than what was actually done in practice.[3]

In short, to the extent that privacy notices have been buried, incomplete, or otherwise ineffective – and they have been – the answer is to enhance efforts to enforce the "notice" model, not to replace it with a new framework.

---

[2] The duty to disclose "material" facts would be triggered when the information was collected, used, or shared in a manner that "is likely to affect the consumer's conduct or decision with regard to a product or service." *See* FTC Policy Statement on Deception, *appended to Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174, 175 (1984). In some cases, disclosure would not have to be express. For example, using consumer information to provide order fulfillment would be disclosed by virtue of the transaction itself. *See also* Report at vi, 41, 52-53.

[3] The Report mentions "access" and "security" as aspirational privacy goals. *See* Report at 7. However, with the possible exceptions of the Children's Online Privacy Protection Act and the Fair Credit Reporting Act, the Report does not suggest that Congress has ever enacted a special statute mandating "access," and the Report does not cite any instance in which "lack of access" has been a basis for a Commission law enforcement action. Moreover, except for the special statutes identified, the Report does not identify any special statute enacted by Congress that mandates "security" as such. The Commission has brought cases under the "unfairness" prong of Section 5 for failure to have reasonable security measures in place, but there was financial harm threatened in those cases.

As a hortatory exercise, the Report is less problematic.[4] Many, if not all, of the "best practices" suggested are desirable. However, I disagree with the Report insofar as it suggests that even when the privacy notice is inadequate, the defect may be cured if consumers are offered some "meaningful choice" mechanism – whether it be opt in or opt out. *See* Report at 41, 52, 56-68. If firms are offered that alternative, that might disincentivize them from adopting acceptable privacy notices in the first place. That would be undesirable. Moreover, the Report takes no position as to whether the choice mechanism should be an opt-in or opt-out mechanism. *Id*. Because that question is left open, the Report can be read to portend that the final Report will suggest an opt-in option. More fundamentally, the self-regulation that is championed in this area (*see* Report at 8) may constitute a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival that may constrain the exercise of undue power. *See* Report at 48 (respecting self-regulation as applicable to a "legacy system"). That possibility may be blunted by insuring that smaller rivals participate in the adoption of self-regulatory rules, but that may not be practical.

ANALYSIS

The Report repeatedly acknowledges that the increasing flow of information provides important benefits to consumers and businesses.[5] Report at i, iv, 21, 33-35. Yet, despite the

---

[4] The Report asserts that there are a number of "best practices" that private firms should adopt from the get-go in order to protect privacy. *See* Report at v, 39, 40-41, 43-52. Most of these practices are desirable in the abstract. But that does not mean that firms should be mandated *de jure* (*i.e*., by legislation) to adopt them or that firms should be required to do so *de facto* (*i.e.*, that large, well-entrenched firms engaging in "self-regulation" should dictate what the privacy practices of their competitors should be).

[5] "In particular, [workshop] panelists discussed benefits specific to business models such as online search, online behavioral advertising, social networking, cloud computing, mobile technologies, and health services. Participants noted that search engines provide customers with

acknowledgment of these benefits, the Report, as written, leaves room in any final report for a prohibition against dissemination to third parties of non-sensitive information generally, and of information collected through behavioral tracking specifically.

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).[6]

Second, the Report asserts that the "notice" model that the Commission has used in the past no longer works (*see* Report at iii, 19-20) and that the Commission should instead adopt the

---

instant access to tremendous amounts of information at no charge to the consumer. Online advertising helps to support much of the content available to consumers online and allows personalized advertising that many consumers value. Social networking services permit users to connect with friends and share experiences online, in real time. These platforms also facilitate broader types of civic engagement on political and social issues." *See* Report at 33-34.

[6] *See, e.g.*, Thomas M. Lenhard 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.

new framework proposed in the Report. Although the Report repeatedly asserts that this new framework "builds upon" the traditional Commission law enforcement model (*see* Report at v, 38-39, 40), it in fact would replace that model. To be sure, many, if not most, privacy policy disclosures are prolix and incomprehensible. But the appropriate remedy for opacity is to require notices to be clear, conspicuous and effective. If a consumer is provided with clear and conspicuous notice prior to the collection of information, there is no basis for concluding that a consumer cannot generally make an informed choice.[7] In addition, 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.[8] 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" (*see* Report at iii, 20, 31), 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.[9]

---

[7] The Report asserts there has been an "enormous growth in data processing and storage capabilities" (*see* Report at 24), and that there has been a proliferation of affiliates, information brokers and other information aggregators. *See* Report at 21, 23-24, 45-46, 68. But the Report does not explain how or why this phenomenon cannot be addressed by clear and conspicuous disclosures to consumers that their information may be aggregated in that fashion.

[8] 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. *See* Report at 10-12. However, the Commission has not challenged practices threatening intangible harm under Section 5.

[9] Letter from the Federal Trade Commission to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate,

Third, as stated, the Report takes the position that an opt-in requirement may be triggered whenever there is a "material" change in the handling of the "other" information, including the sharing of non-sensitive information like behavioral tracking information, with third parties. *See* Report at 75-76. The Report is ambiguous as to whether this requirement would apply no matter how clear and conspicuous the disclosure of the prospect of material change was. *Compare* Report at 15, 75-76 *with* Report at 39, 76. Arguably, there is no warrant for requiring more than an opt-out requirement if that was what was initially required, when the disclosure of the material change and the ability to opt out is made clearly and conspicuously and the consumer actually receives the disclosure.

Fourth, insofar as the Report could be read as suggesting a ban on "take it or leave it" options (*see* Report at 60), again, clear and conspicuous disclosure is the most appropriate way to deal with such an option. I question whether such a ban would be constitutional and am also concerned about the impact of a ban on innovation.

Finally, if the traditional "notice" law enforcement model is to be augmented by some "choice" mechanism, I continue to have many questions about the proper implementation of a Do Not Track concept. 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.[10] Considered in a vacuum, the proposed Do Not Track attributes set

---

Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction, *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

[10] 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

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.[11]

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.[12] It is also easy to attack practices that compromise certain personally identifiable information ("PII") like one's social security number, confidential

---

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.

[11] 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.

[12] *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).

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.[13] 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 "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.[14] These lists are furnished by interested third parties in order to prevent the types of tracking that consumers supposedly do not want.[15] It is clear from

---

[13] *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).

[14] 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.

[15] 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

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.[16] This 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.[17] 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,

---

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.

[16] 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.

[17] 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.

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.

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."[18] 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.[19] 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

---

[18] *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.

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

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 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.

CONCLUSION

To the extent we have exercised our authority under Section 5, the "notice" model for privacy law enforcement has served this Commission long and well. Not only is there no warrant for discarding it now in favor of a proposed new framework that is as yet theoretical and untested, but in my judgment it would also be bad public policy to do so. To the contrary, if there is anything wrong with the "notice" model, it is that we do not enforce it stringently enough. Moreover, as the Bureau of Consumer Protection concedes, there are many benefits to the sharing of non-sensitive consumer information, and they may be endangered by the aspirational proposals advanced in the Report, however hortatory they may be.