Concurring Statement of Commissioner 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
December 1, 2010

INTRODUCTION

The Commission issues this Report today 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. I concur in the decision to issue the Report and seek critical comment on the issues it raises, but write separately to explain my serious reservations about the proposal advanced in the Report.

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 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]

---

[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.

[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

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, 8-9), 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.

As a hortatory exercise, the Report is less problematic.[4] Many, if not all, of the "best

---

be disclosed by virtue of the transaction itself. *See also* Report at vi, 41, 52-54.

[3] The Report mentions "access" and "security" as aspirational privacy goals. *See* Report at 7. However, with the possible exception of the Children's Online Privacy Protection 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.

[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, 40, 41, 44-52. 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).

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, 52-53, 57-63. 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 48-49 (respecting self-regulation as applicable to a "legacy system"). That possibility may be blunted by ensuring 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 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

[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 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." Report at 33-34.

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 25-28. 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 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, 2, 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

---

[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.

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, 31-32), generally when analyzing consumer injury. The Commission has specifically advised Congress that absent deception, it will not enforce Section 5 against alleged intangible harm.[9]

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 consumer information, including the sharing of non-sensitive information like behavioral tracking information, with third parties. *See* Report at 76-77. The Report is ambiguous as to whether this requirement would apply no matter

---

[7] The Report asserts there has been an "enormous growth in data processing and storage capabilities" (Report at 24), and that there has been a proliferation of affiliates, information brokers and other information aggregators. *See* Report at 21, 23-25, 46, 69. 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 In re 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, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction, *reprinted in In re Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

how clear and conspicuous the disclosure of the prospect of material change was. *Compare* Report at 15, 76-77 *with* Report at 39, 77. 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 61), 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 support a Do Not Track mechanism if it is technically feasible. However, I think consumers should have to "opt in" to use such a mechanism just as they have opted in to get on the Do Not Call Registry. Making access to the Do Not Track mechanism depend upon consumers opting in would not only parallel the Do Not Call model: it would give the Commission a much more reliable estimate of the percentage of consumers who really wish to prevent this type of tracking.

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.