Dissenting Statement of Commissioner J. Thomas Rosch
Issuance of Federal Trade Commission Report
Protecting Consumer Privacy in an Era of Rapid Change:
Recommendations for Businesses and Policymakers
March 26, 2012

Introduction

I agree in several respects with what the "final" Privacy Report says. Specifically, although I disagree that the consumer has traditionally ever been given any "choice" about information collection practices (other than to "take-it-or-leave-it" after reviewing a firm's privacy notice), I agree that consumers ought to be given a broader range of choices if for no other reason than to customize their privacy protection. However, I still worry about the constitutionality of banning take-it-or-leave-it choice (in circumstances where the consumer has few alternatives); as a practical matter, that prohibition may chill information collection, and thus impact innovation, regardless whether one's privacy policy is deceptive or not.[1]

I also applaud the Report's recommendation that Congress enact "targeted" legislation giving consumers "access" to correct misinformation about them held by a data broker.[2] I also support the Report's recommendation that Congress implement federal legislation that would require entities to maintain reasonable security and to notify consumers in the event of certain security breaches.[3]

---

[1] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("Report") at 50-52.

[2] *Id.* at 14, 73.

[3] *Id.* at 26. I also support the recommendation that such legislation authorize the Commission to seek civil penalties for violations. However, despite its bow to "targeted" legislation, the Report elsewhere counsels that the Commission support privacy legislation generally. *See, e.g., id.* at 16. To the extent that those recommendations are not defined, or narrowly targeted, I disagree with them.

Finally, I concur with the Report insofar as it recommends that information brokers who compile data for marketing purposes must disclose to consumers how they collect and use consumer data.[4] I have long felt that we had no business counseling Congress or other agencies about privacy concerns without that information. Although I have suggested that compulsory process be used to obtain such information (because I am convinced that is the only way to ensure that our information is complete and accurate),[5] a voluntary centralized website is arguably a step in the right direction.

Privacy Framework

My disagreement with the "final" Privacy Report is fourfold. First, the Report is rooted in its insistence that the "unfair" prong, rather than the "deceptive" prong, of the Commission's Section 5 consumer protection statute, should govern information gathering practices (including "tracking"). "Unfairness" is an elastic and elusive concept. What is "unfair" is in the eye of the beholder. For example, most consumer advocacy groups consider behavioral tracking to be unfair, whether or not the information being tracked is personally identifiable ("PII") and regardless of the circumstances under which an entity does the tracking. But, as I have said, consumer surveys are inconclusive, and individual consumers by and large do not "opt out" from tracking when given the chance to do so.[6] Not surprisingly, large enterprises in highly

---

[4] *Id*. at 14, 68-70.

[5] *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Information and Privacy: In Search of a Data-Driven Policy, Remarks at the Technology Policy Institute Aspen Forum (Aug. 22, 2011), *available at* http://www.ftc.gov/speeches/rosch/110822aspeninfospeech.pdf.

[6] *See* Katy Bachman, *Study: Internet User Adoption of DNT Hard to Predict*, adweek.com, March 20, 2012, *available at* http://www.adweek.com/news/technology/study-internet-user-adoption-dnt-hard-predict-139091 (reporting on a survey that found that what Internet users say they are going to do about using a

concentrated industries, which may be tempted to raise the privacy bar so high that it will disadvantage rivals, also support adopting more stringent privacy principles.[7]

The "final" Privacy Report (incorporating the preliminary staff report) repeatedly sides with consumer organizations and large enterprises. It proceeds on the premise that behavioral tracking is "unfair."[8] Thus, the Report expressly recommends that "reputational harm" be considered a type of harm that the Commission should redress.[9] The Report also expressly says that privacy be the default setting for commercial data practices.[10] Indeed, the Report says that the "traditional distinction between PII and non-PII has blurred,"[11] and it recommends "shifting the burdens away from consumers and placing obligations on businesses."[12] To the extent the

---

Do Not Track button and what they are currently doing about blocking tracking on the Internet, are two different things); s*ee also* 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" (Dec. 1, 2010), *available at* http://www.ftc.gov/speeches/rosch/101201privacyreport.pdf.

[7] *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Do Not Track: Privacy in an Internet Age, Remarks at Loyola Chicago Antitrust Institute Forum (Oct. 14, 2011), *available at* http://www.ftc.gov/speeches/rosch/111014-dnt-loyola.pdf; *see also* Report at 9.

[8] Report at 8 & n.37.

[9] *Id*. at 2. The Report seems to imply that the Do Not Call Rule would support this extension of the definition of harm. *See id*. ("unwarranted intrusions into their daily lives"). However, it must be emphasized that the *Congress* granted the FTC underlying authority under the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, to promulgate the Do Not Call provisions and other substantial amendments to the TSR. The Commission did not do so unilaterally.

[10] *Id*.

[11] *Id*. at 19.

[12] *Id*. at 23, *see also id.* at 24.

Report seeks consistency with international privacy standards,[13] I would urge caution. We should always carefully consider whether each individual policy choice regarding privacy is appropriate for this country in all contexts.

That is not how the Commission itself has traditionally proceeded. To the contrary, the Commission represented in its 1980, and 1982, Statements to Congress that, absent deception, it will not generally enforce Section 5 against alleged intangible harm.[14] In other contexts, the Commission has tried, through its advocacy, to convince others that our policy judgments are sensible and ought to be adopted. And, as I stated in connection with the recent *Intel* complaint, in the competition context, one of the principal virtues of applying Section 5 was that that provision was "self-limiting," and I advocated that Section 5 be applied on a stand-alone basis only to a firm with monopoly or near-monopoly power.[15] Indeed, as I have remarked, absent such a limiting principle, privacy may be used as a weapon by firms having monopoly or near-monopoly power.[16]

---

[13] *Id*. at 9-10. This does not mean that I am an isolationist or am impervious to the benefits of a global solution. But, as stated below, there is more than one way to skin this cat.

[14] *See* Letter from the FTC 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 (Dec. 17, 1980), *reprinted in International Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984) ("Unfairness Policy Statement") *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm; Letter from the FTC to Hon. Bob Packwood and Hon. Bob Kasten, Committee on Commerce, Science and Transportation, United States Senate, *reprinted in* FTC Antitrust & Trade Reg. Rep. (BNA) 1055, at 568-570 ("Packwood-Kasten letter"); and 15 U.S.C. § 45(n), which codified the FTC's modern approach.

[15] *See* Concurring and Dissenting Statement of Commissioner J. Thomas Rosch, *In re Intel Corp*., Docket No. 9341 (Dec. 16, 2009), *available at* http://www.ftc.gov/os/adjpro/d9341/091216intelstatement.pdf.

[16] *See* Rosch, *supra* note 7 at 20.

There does not appear to be any such limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" as the watchdog over these practices not only in the online world but in the offline world.[17] That is not only paternalistic, but it goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).[18] I would instead stand by what we have said and challenge information collection practices, including behavioral tracking, only when these practices are deceptive, "unfair" within the strictures of Section 5(n) and our commitments to Congress, or employed by a firm with market power and therefore challengeable on a stand-alone basis under Section 5's prohibition of unfair methods of competition.

Second, the current self-regulation and browser mechanisms for implementing Do Not Track solutions may have advanced since the issuance of the preliminary staff Report.[19] But, as the final Report concedes, they are far from perfect,[20] and they may never be, despite efforts to create a standard through the World Wide Web Consortium ("W3C") for the browser mechanism.[21]

---

[17] *See* Report at 13.

[18] Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312.

[19] Report at 4, 52.

[20] *Id*. at 53, 54; *see esp. id*. at 53 n.250.

[21] *Id*. at 5, 54.

More specifically, as I have said before, the major browser firms' interest in developing Do Not Track mechanisms begs the question of whether and to what extent those major browser firms will act strategically and opportunistically (to use privacy to protect their own entrenched interests).[22]

In addition, the recent announcement by the Digital Advertising Alliance (DAA) that it will honor the tracking choices consumers make through their browsers raises more questions than answers for me. The Report is not clear, and I am concerned, about the extent to which this latest initiative will displace the standard-setting effort that has recently been undertaken by the W3C. Furthermore, it is not clear that all the interested players in the Do Not Track arena – whether it be the DAA, the browser firms, the W3C, or consumer advocacy groups – will be able to come to agreement about what "Do Not Track" even means.[23] It may be that the firms professing an interest in self-regulation are really talking about a "Do Not Target" mechanism, which would only prevent a firm from serving targeted ads, rather than a "Do Not Track" mechanism, which would prevent the collection of consumer data altogether. For example, the DAA's Self-Regulatory Principles for Multi-Site Data do not apply to data collected for "market research" or "product development."[24] For their part, the major consumer advocacy groups may

---

[22] *See* Rosch, *supra* note 7 at 20-21.

[23] Tony Romm, *What Exactly Does 'Do Not Track' Mean?*, Politico, Mar. 13, 2012, *available at* http://www.politico.com/news/stories/0312/73976.html; *see also* Report at 4 (DAA allows consumer to opt out of "targeted advertising").

[24] *See Self-Regulatory Principles for Multi-Site Data,* Digital Advertising Alliance, Nov. 2011, at 3, 10, 11, *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf; *see also* Tanzina Vega, *Opt-Out Provision Would Halt Some, but Not All, Web Tracking*, New York Times, Feb. 26, 2012, *available at* http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-

not be interested in a true "Do Not Track" mechanism either. They may only be interested in a mechanism that prevents data brokers from compiling consumer profiles instead of a comprehensive solution. It is hard to see how the W3C can adopt a standard unless and until there is an agreement about what the standard is supposed to prevent.[25]

It is also not clear whether or to what extent the lessons of the Carnegie Mellon Study respecting the lack of consumer understanding of how to access and use Do Not Track will be heeded.[26] Similarly, it is not clear whether and to what extent Commissioner Brill's concern that consumers' choices, whether it be "Do Not Collect" or merely "Do Not Target," will be honored.[27] Along the same lines, it is also not clear whether and to what extent a "partial" Do Not Track solution (offering nuanced choice) will be offered or whether it is "all or nothing." Indeed, it is not clear whether consumers can or will be given complete and accurate information about the pros and the cons of subscribing to Do Not Track before they choose it. I find this last

---

web-tracking.html?pagewanted=all.

[25] *See* Vega, *supra* note 24.

[26] *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, Carnegie Mellon University CyLab, Oct. 31, 2011, *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf; *see also Search Engine Use 2012*, at 25, Pew Internet & American Life Project, Pew Research Center, Mar. 9, 2012, *available at* http://pewinternet.org/~/media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf ("[j]ust 38% of internet users say they are generally aware of ways they themselves can limit how much information about them is collected by a website").

[27] *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Big Data, Big Issues, Remarks at Fordham University School of Law (Mar. 2, 2012) *available at* http://ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

question especially vexing in light of a recent study that indicated 84% of users polled prefer targeted advertising in exchange for free online content.[28]

Third, I am concerned that "opt-in" will necessarily be selected as the *de facto* method of consumer choice for a wide swath of entities that have a first-party relationship with consumers but who can potentially track consumers' activities across unrelated websites, under circumstances where it is unlikely, because of the "context" (which is undefined) for such tracking to be "consistent" (which is undefined) with that first-party relationship:[29] 1) companies with multiple lines of business that allow data collection in different contexts (such as Google);[30] 2) "social networks," (such as Facebook and Twitter), which could potentially use "cookies," "plug-ins," applications, or other mechanisms to track a consumer's activities across the Internet;[31] and 3) "retargeters," (such as Amazon or Pacers), which include a retailer who delivers an ad on a third-party website based on the consumer's previous activity on the retailer's website.[32]

---

[28] *See* Bachman, *supra* note 6.

[29] Report at 41.

[30] *Id.* Notwithstanding that Google's prospective conduct seems to fit perfectly the circumstances set forth on this page of the Report (describing a company with multiple lines of business including a search engine and ad network), where the Commission states "consumer choice" is warranted, the Report goes on to conclude on page 56 that Google's practices do not require affirmative express consent because they "currently are not so widespread that they could track a consumer's every movement across the Internet."

[31] *Id.* at 40. *See also supra* note 30. That observation also applies to "social networks" like Facebook.

[32] *Id.* at 41.

These entities might have to give consumers "opt-in" choice now or in the future: 1) regardless whether the entity's privacy policy and notices adequately describe the information collection practices at issue; 2) regardless of the sensitivity of the information being collected; 3) regardless whether the consumer cares whether "tracking" is actually occurring; 4) regardless of the entity's market position (whether the entity can use privacy strategically – *i.e.*, an opt-in requirement – in order to cripple or eliminate a rival); and 5) conversely, regardless whether the entity can compete effectively or innovate, as a practical matter, if it must offer "opt in" choice.[33]

Fourth, I question the Report's apparent mandate that ISPs (like Verizon, AT&T and Comcast), with respect to uses of deep packet inspection, be required to use opt-in choice.[34] This is not to say there is no basis for requiring ISPs to use opt-in choice without requiring opt-in choice for other large platform providers. But that kind of "discrimination" cannot be justified, as the Report says, because ISPs have "are in a position to develop highly detailed and comprehensive profiles of their customers."[35] So does any large platform provider who makes available a browser or operating system to consumers.[36]

Nor can that "discrimination" be justified on the ground that ISPs may potentially use that data to "track" customer behavior in a fashion that is contrary to consumer expectations. There is no reliable data establishing that most ISPs presently do so. Indeed, with a business

---

[33] *See id.* at 60 ("Final Principle").

[34] *Id*. at 56 ("the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection").

[35] *Id*.

[36] *Id*.

model based on subscription revenue, ISPs arguably lack the same incentives as do other platform providers whose business model is based on attracting advertising and advertising revenue: ISPs assert that they track data only to perform operational and security functions; whereas other platform providers that have business models based on advertising revenue track data in order to maximize their advertising revenue.

What really distinguishes ISPs from most other "large platform providers" is that their markets can be highly concentrated.[37] Moreover, even when an ISP operates in a less concentrated market, switching costs can be, or can be perceived as being, high.[38] As I said in connection with the *Intel* complaint, a monopolist or near monopolist may have obligations which others do not have.[39] The only similarly situated platform provider may be Google, which, because of its alleged monopoly power in the search advertising market, has similar power. For any of these "large platform providers," however, affirmative express consent should be required only when the provider *actually* wants to use the data in this fashion, not just when it *has the potential* to do so.[40]

---

[37] Federal Communications Commission, *Connecting America: The National Broadband Plan, Broadband Competition and Innovation Policy, Section 4.1, Networks, Competition in Residential Broadband Markets* at 36, *available at* http://www.broadband.gov/plan/4-broadband-competition-and-innovation-policy/.

[38] Federal Communications Commission Working Paper, *Broadband decisions: What drives consumers to switch – or stick with – their broadband Internet provider* (Dec. 2010), at 3, 8, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1206/DOC-303264A1.pdf.

[39] *See* Rosch, *supra* note 15.

[40] *See, e.g.*, Report at 56.

Conclusion

Although the Chairman testified recently before the House Appropriations Subcommittee chaired by Congresswoman Emerson that the recommendations of the final Report are supposed to be nothing more than "best practices,"[41] I am concerned that the language of the Report indicates otherwise, and broadly hints at the prospect of enforcement.[42] The Report also acknowledges that it is intended to serve as a template for legislative recommendations.[43] Moreover, to the extent that the Report's "best practices" mirror the Administration's privacy "Bill of Rights," the President has specifically asked either that the "Bill of Rights" be adopted by the Congress or that they be distilled into "enforceable codes of conduct."[44] As I testified before the same subcommittee, this is a "tautology;" either these practices are to be adopted voluntarily by the firms involved or else there is a federal requirement that they be adopted, in

---

[41] Testimony of Jon Leibowitz and J. Thomas Rosch, Chairman and Comm'r, FTC, *The FTC in FY2013: Protecting Consumers and Competition*: *Hearing on Budget Before the H. Comm. on Appropriations Subcomm. on Financial Services and General Government*, 112 th Cong. 2 (2012), text from CQ Roll Call, available from: LexisNexis® Congressional.

[42] One notable example is found where the Report discusses the articulation of privacy harms and enforcement actions brought on the basis of *deception*. The Report then notes "[l]ike these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions." Report at 8. The accompanying footnote concludes that "even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm." *See also infra* note 43.

[43] *Id*. at 16 ("to the extent Congress enacts any of the Commission's recommendations through legislation"); *see also id*. at 12-13 ("the Commission calls on Congress to develop baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate").

[44] *See* Letter from President Barack Obama, *appended to* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

which case there can be no pretense that they are "voluntary."[45] It makes no difference whether the federal requirement is in the form of enforceable codes of conduct or in the form of an act of Congress. Indeed, it is arguable that neither is needed if these firms feel obliged to comply with the "best practices" or face the wrath of "the Commission" or its staff.

[45] *See* FTC Testimony, *supra* note 41.