

# Federal Trade Commission

“Some Thoughts on the Evolving Nature of Data Security and Privacy Protection”

J. Thomas Rosch  
Commissioner, Federal Trade Commission

before  
International Association of Privacy Professionals  
Practical Privacy Series  
Washington, DC

December 4, 2012

Good morning. I am pleased to be here today to discuss some of my thoughts on data security and privacy. As many of you may know, my seven-year term as Commissioner of the Federal Trade Commission recently ended this past September, and once my replacement is confirmed and sworn in, I will be leaving the Commission. In light of this timing, I thought it therefore might be appropriate for me to sum up my thoughts on data security and privacy, and to explain how my thinking on these issues has evolved over the last several years.

## Data Security and Privacy Breaches

My first brush with data security and privacy protection actually occurred a few years before I rejoined the Commission. In 2002, I represented Eli Lilly when the Commission – in its very first data security case – brought an action against Eli Lilly for misrepresenting the step8.5(i)r66.2

---

<sup>1</sup> 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 Chief of Staff, Beth Delaney, for her invaluable assistance in preparing these remarks.

that they took to protect consumers' sensitive data. It is a case that has an interesting fact pattern. For a little over a year, Lilly provided consumers with a "Medi-messenger" e-mail reminder service whereby consumers could design and receive personal e-mail messages to remind them to take or refill their medication. Once a consumer registered for Medi-messenger, the reminder messages were automatically e-mailed from Lilly to the subscriber at the e-mail address she or he had provided, and according to the subscriber's requested schedule. These reminders were individualized e-mails and did not identify any other subscribers to the service.

In June 2001, quite ironically, in the process of terminating this Medi-messenger service, a Lilly employee created a new computer program to access Medi-messenger subscribers' e-mail addresses and to send e-mail messages announcing the end of this service. This e-mail message unfortunately included all recipients' e-mail addresses in the "To:" line of the message, thereby unintentionally disclosing to each individual subscriber the e-mail addresses of all 669 Medi-messenger subscribers. To make matters worse, because these recipients had signed up for this service through Lilly's Prozac.com website, this inadvertent disclosure of email addresses actually translated into the inadvertent disclosure of people taking Prozac.

Lilly's privacy policies had informed consumers that Lilly recognized the importance of keeping sensitive information private and that it took measures to do so. In light of the email address incident, the FTC complaint therefore alleged that Lilly's claim of privacy and confidentiality was deceptive because Lilly failed to maintain or implement internal measures

---

<sup>2</sup> In particular, the complaint alleged that Lilly failed to: provide appropriate training for its employees regarding consumer privacy and information security; provide appropriate oversight and assistance for the employee who sent out the e-mail, who had no prior experience in creating, testing, or implementing the computer program used; and implement appropriate

I still think the basis for bringing this case ~~deceptive~~ *deceptive* representation about security practices – is correct. However, I must admit I am still disappointed that I wasn't able to convince the Commission that this one particular ~~unadvertent~~ *unadvertent* disclosure didn't equate to a deceptive representation about reasonable data security practices.

It is interesting to consider how ~~the~~ *the* Lilly case would be framed today if the company had not made explicit representations about its security practices. My personal recollection

---

checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the e-mail. Lilly's failure to implement appropriate measures also violated a number of its own written security procedures. *See In the Matter of Eli Lilly and Co.*, FTC File No. 012-3214 (May 10, 2002) (complaint), available at <http://www.ftc.gov/os/2002/05/elilillycmp.htm>

<sup>3</sup> 15 U.S.C. § 45(n) (2004).

Privacy Protection Act – recognize this and regulate certain aspects of the collection, sharing and retention of most of this information.<sup>4</sup>

However, I am not sure that the disclosure of an email address associated with the prescription drug Prozac – to other email addresses that are also associated with that website – is the type of tangible injury that is necessary for an unfairness claim, according to what the Commission told Congress in 1980 and again in 1982.<sup>5</sup> a threshold issue, the injury itself may have been considered substantial to some consumers, but not all. How do we measure that type of injury? It is not financial in nature, but rather goes to revealing personal information about someone. When we step away from tangible injury, and move toward injury that makes people – some people – “uncomfortable,” we start down a slippery slope. Where does it stop? This incident only involved email addresses – not names, addresses, other personal identifiers, or even confirmation that the addressee took Prozac. The only thing that was disclosed was that a

---

<sup>4</sup> The Commission has successfully challenged practices that violate these statutes. *Aid Corp.*, FTC File No. 072-3121 (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); *Settlement One Credit Corp.*, FTC File No. 082-3208 (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).

<sup>5</sup> 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), available at <http://www.ftc.gov/bcp/policystmt/ad-unfair.htm> [hereinafter *Unfairness Policy Statement*]; 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.

certain email address had signed up for the Medi-Messenger service. I am concerned about the lack of certainty that is caused by this slippery slope. In contrast, a statute such as HIPAA specifically sets forth the conditions for which ~~data~~ personal information must be protected and offers certainty in that it delineates the particular pieces of personal information that are covered and how they must be treated.

I recently abstained from voting in the *DesignerWare* and rent-to-own cases for this very lack of certainty. *DesignerWare* licensed software to rent-to-own stores, including franchisees of Aaron's, ColorTyme, and Premier Rental Purchase, to help them track and recover rented computers.

As alleged in our complaint, *DesignerWare*'s software contained a "kill switch" that the rent-to-own stores could use to disable a computer if it was stolen, or if the renter failed to make timely payments. *DesignerWare* also had an add-on program known as "Detective Mode" that purportedly helped rent-to-own stores locate rented computers and collect late payments. *DesignerWare*'s software also collected data that allowed the rent-to-own operators to secretly track the location of rented computers, and thus the computers' users. When Detective Mode was activated, the software could log keystrokes, capture screen shots and take photographs using a computer's webcam. It also presented a fake software program registration screen that tricked consumers into providing their personal contact information.

---

<sup>6</sup> Data gathered by *DesignerWare* and provided to rent-to-own stores using Detective Mode revealed private and confidential details about computer users, such as user names and passwords for email accounts, social media websites, and financial institutions; Social Security numbers; medical records; private emails to doctors; bank and credit card statements; and webcam pictures of children, partially undressed individuals, and intimate activities at home.

The FTC's complaint contained allegations that some of these practices were deceptive and others were unfair. I abstained from voting in this case because although I agreed that the companies had harmed consumers, I believed that all the conduct should have been framed as either deceptive representations or deceptive omissions.

\* \* \*

Beginning in 2006, when I arrived as Commissioner, and continuing for the first few years of my term, the staff was in the midst of bringing a series of cases that involved the failure of companies to take reasonable measures to protect the security of the sensitive personal information on their computer networks. These cases sometimes alleged deception and other times alleged unfairness. Some complaints involved allegations of both deception and unfairness. The standard operating procedure was to bring these cases administratively and to accept an administrative consent that enjoined the companies from engaging in these unreasonable security practices. Each administrative consent also required the company to undergo biennial security audits for 20 years.

As these cases kept coming up to the Commission, I struggled with a couple of issues. First, why were these companies able to avoid paying any consumer restitution, disgorgement or civil penalties? None of these settlements involved any money. Second, I became concerned

---

<sup>7</sup> *In the Matter of CardSystems Solutions, Inc.*, FTC File No. 052-3148 (Sept. 8, 2006) (decision and order); *In the Matter of DSW, Inc.*, FTC File No. 012-3196 (Dec. 15, 2005) (stipulated final order); *In the Matter of BJ's Wholesale Club, Inc.*, FTC File No. 042-3160 (Sept. 20, 2005) (decision and order); *In the Matter of Guidance Software, Inc.*, FTC File No. 062-3057 (Apr. 3, 2007) (decision and order); *In the Matter of LifeIsGood Retail, Inc.*, FTC File No. 072-3046 (Apr. 18, 2008) (decision and order); *In the Matter of Reed Elsevier*, FTC File No. 081-0133 (June 5, 2009) (decision and order); *In the Matter of TJX Companies*, FTC File No. 072-3055 (Aug. 1, 2008) (decision and order).

with the lack of efficiency in bringing these cases on a one-by-one basis. Many of these cases seemed to involve virtually the exact same type of data vulnerability. I wondered whether there wasn't there a better way to put all01 nnw [herr there anine basnotico pnd ge way ]TJ T\*ually]TJ T\* ro exay irity. -.001 Tw [(w2asn't the2ck ofsecur wh pr4(

---

<sup>8</sup> 15 U.S.C. § 45(I).

Commission has found the act or practice to be unfair or deceptive. This determination of unlawfulness must also have been made in a final, litigated order, not a consent order.

I thought that litigating a few of these data breach cases and writing Commission decisions that would support later Section 205 actions would kill two birds with one stone. It would be an effective method to put industry members on notice about their obligations. Then, the Commission eventually could pursue civil penalties in appropriate cases.

For a variety of reasons, that proposal was never able to be implemented. The first obstacle of course is that you have to have a company that prefers to administratively litigate the matter rather than settle with the FTC. That didn't happen. Second, around that time, legislation was being proposed that would provide for the imposition of civil penalties in data breach cases. That possibility took some of the heat off of my proposal. It seemed quite promising at the time, although as we all know, it has not panned out.<sup>9</sup> The staff developed a series of high profile matters that involved data security vulnerabilities that also triggered obligations under other statutory regimes, and these statutes and rules did allow the FTC to pursue civil penalties.

---

<sup>9</sup> *United States v. Choicepoint*, FTC File No. 052-3069 (N.D. Ga. Jan. 26, 2006) (stipulated final judgment); *United States v. ValueClick, Inc.*, FTC File No. 072-3111 and 072-3158 (Mar. 17, 2008) (stipulated final judgment); *United States v. Rental Research Services, Inc.*, FTC File No. 072-3228 (Mar. 5, 2009) (stipulated final judgment); *The Matter of CVS Caremark Corp.*, FTC File No. 072-3119 (June 23, 2009) (decision and order); *FTC v. LifeLock, Inc.*, FTC File No. 072-3069 (Mar. 9, 2010) (stipulated final judgment).



## The New Privacy Paradigm

Beginning in December 2010, I started to become uncomfortable with the new “privacy paradigm” proposed first by staff in its preliminary Privacy Report<sup>10</sup> and then later by the Commission, in its final Privacy Report, issued in March 2012.<sup>11</sup> My primary disagreement with this new privacy paradigm is that it uses the “unfair” prong, rather than the “deceptive” prong, of the Commission’s Section 5 consumer protection statute, to frame how the FTC should govern information gathering practices (including “tracking”).<sup>12</sup> I am uncomfortable about centering the agency’s policy recommendations and law enforcement initiatives on unfairness.

“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 information (“PII”) and regardless of the circumstances under which an entity does the tracking. But, as I and others have said, consumer surveys are inconclusive, and individual consumers historically have not “opt outed” from tracking when given the chance to do so.<sup>13</sup>

---

<sup>10</sup> See Fed. Trade Comm’n, Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Dec. 2010), available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>

<sup>11</sup> Fed. Trade Comm’n, FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> [hereinafter *FTC Privacy Report*].

<sup>12</sup> *Id.*

<sup>13</sup> See Katy Bachman, *Study: Internet User Adoption of DNT Hard to Predict*, *adweek.com*, Mar. 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 Do Not Track button and what they are currently doing about blocking tracking on the Internet, are two different things); see also Concurring Statement of Commissioner J. Thomas Rosch,

The Commission's final Privacy Report (like the staff's preliminary privacy report) repeatedly sides with consumer organizations and large enterprises. It proceeds on the premise that behavioral tracking is "unfair."<sup>14</sup> Thus, the Report expressly recommends that "reputational harm" be considered a type of harm that the Commission should redress.<sup>15</sup> The Report also expressly says that the "best practices include making privacy the 'default setting' for commercial data practices."<sup>16</sup> Indeed, the Report says that the "traditional distinction between PII and non-PII has blurred,"<sup>17</sup> and it recommends "shifting burdens away from consumers and placing obligations on businesses."<sup>18</sup>

That is not how the Commission itself has traditionally proceeded. To the contrary, as I have noted, 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.<sup>19</sup>

---

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>

<sup>14</sup> *FTC Privacy Report*, *supra* note 12, at 8 and n.37.

<sup>15</sup> *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.

<sup>16</sup> *Id.* at i.

<sup>17</sup> *Id.* at 19.

<sup>18</sup> *Id.* at 23, *see also id.* at 24.

<sup>19</sup> *See supra* note 6.

I am particularly concerned about the Commission treading into areas where the alleged injury is to “reputation,” or where the conduct is merely alleged to be “creepy.” Implementing some of the recommendations in the final Privacy Report would install “Big Brother” (in the form of the Commission or the Congress) as the watchdog over these practices not only in the online world but in the offline world<sup>20</sup>. 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)<sup>21</sup> would instead stand by what we have said and challenge information collection practices, including behavioral tracking, only when these practices are deceptive or “unfair” within the strictures of Section 5(n) and our commitments to Congress.

#### “Do Not Track”

For today’s purposes, when I refer to “Do Not Track” mechanisms I mean a method by which an Internet user can make a choice whether or not to allow the collection and use of data regarding their online activities – things like search and browsing<sup>22</sup>. Some have likened the concept of “tracking” to being followed around a store as you shop. However, computer technology allows online tracking to be more comprehensive, pervasive and detailed than the tracking that can occur offline.

One of my objections in my dissent from the Commission’s final Privacy Report was to what I viewed as the overly optimistic description in the Report of the status of browser

---

<sup>20</sup> See *FTC Privacy Report*, *supra* note 12, at 13.

<sup>21</sup> Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312.

<sup>22</sup> The concept of Do Not Track was presented in the preliminary Staff Privacy Report, issued in December 2010<sup>22</sup> *see supra* note 11.

mechanisms and self-regulatory efforts regarding the concept of “Do Not Track.” More specifically, the Report asserted that both the development of browser mechanisms and the evolution of self-regulation regarding “Do Not Track” had advanced substantially since the issuance of the staff’s preliminary privacy report in December 2010. Indeed, some were quoted as predicting that consumers could use these Do Not Track mechanisms by the end of 2012.

I was a “doubting Thomas.” As the final Privacy Report was being issued, a browser-based opt-out mechanism to prevent tracking was being touted by the major browser firms’ agreed to implement a browser-based mechanism<sup>23</sup> and the Digital Advertising Alliance (DAA) committed to following the instructions that consumers made using such mechanisms<sup>24</sup>. This later evolved into a general agreement to develop a common Do Not Track mechanism based on the technical standard adopted by the W3C (World Wide Web Consortium) standard-setting organization. My doubts about that “agreement” were twofold.

First, I was concerned that at least one of those major browser firms would act strategically and opportunistically to use privacy to protect its own entrenched competitive

---

<sup>23</sup> Kenneth Corbin, *Obama Backs 'Consumer Bill of Rights' for Online Privacy*, CIO, Feb. 23, 2012, available at <http://www.cio.com/article/700735/Obama-Backs-Consumer-Bill-of-Rights-for-Online-Privacy>.

<sup>24</sup> Julia Angwin, *Web Firms to Adopt 'No Track' Button*, Wall St. J., Feb. 23, 2012, available at <http://online.wsj.com/article/SB10001424052970203960804577239774264364692.html>

<sup>25</sup> Edward Wyatt, *White House, Consumers in Mind, Offers Online Privacy Guidelines*, N.Y. Times, Feb. 23, 2012, available at [http://www.nytimes.com/2012/02/23/business/white-house-outlines-online-privacy-guidelines.html?\\_r=1](http://www.nytimes.com/2012/02/23/business/white-house-outlines-online-privacy-guidelines.html?_r=1); see also Press Release, Digital Advertising Alliance, *White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumers Online Privacy* (Feb. 23, 2012), available at <http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf>

---

<sup>26</sup> I have raised this argument before.

website's choice to honor (or not) a Do Not Track signal received from a browser.<sup>27</sup> Moreover, since that signal was an "all or nothing" signal, the W3C option – at least insofar as it has developed to date – did not offer the consumer the option of exercising a "nuanced" choice (allowing collection in some circumstances, but not others).

Worse, I was concerned that the major browser firms and the recipient websites and online services did not mean the same thing when it came to defining the meaning of "Do Not Track." It appeared that the browser firms and some of the websites would interpret it to really mean "Do Not Collect" data. But it appeared that the balance of the websites interpreted "Do Not Track" to mean simply "Do Not Target" advertising to consumers. That difference became clear when the Digital Advertising Alliance (DAA), a coalition of industry trade association members (which acted as a voluntary "self-regulatory" group), insisted on carving out an exception for data collected for "research" or "product development" purposes.<sup>28</sup> Under such circumstances, I was hard put to see how the W3C could fashion even a technical standard when

---

<sup>27</sup> Cf. Dan Goodin, *Apache Webserver Updated to Ignore Do Not Track Setting in IE 10*, *Ars Technica*, Sept. 10, 2012, available at <http://arstechnica.com/security/2012/09/apache-webserver-updated-to-ignore-do-not-track-setting-in-ie-10/>

<sup>28</sup> For example, the DAA's Self-Regulatory Principles for Multi-Site Data do not apply to data collected for "market research" or "product development." Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data*, at 3, 10 and 11 (Nov. 2011), available at <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>; also Tanzina Vega, *Opt-Out Provision Would Halt Some, but Not All, Web Tracking*, *N.Y. Times*, Feb. 26, 2012, available at <http://www.nytimes.com/2012/02/27/technology/opt-provision-would-halt-some-but-not-all-web-tracking.html?pagewanted=all>

---

<sup>29</sup> Tony Romm, *What Exactly Does 'Do Not Track' Mean?*, Politico, Mar. 13, 2012, available at <http://www.politico.com/news/stories/0312/73976.html>.

<sup>30</sup> *See also* Letter from Commissioner J. Thomas Rosch, Fed. Trade Comm'n, *World*

transactions.) Moreover, because Microsoft has a huge installed base, at least in the United States (accounting for most of the browsers installed as original equipment in desktop and laptop computers), it has been suggested that Microsoft has acted more strategically and opportunistically to disadvantage rivals (particularly Google) than out of concern for consumer privacy.<sup>33</sup>

Second, the development and implementation of this standard puts the “scope” of the choice in the hands of those *other than* consumers. The major browser firms and the recipient websites and online services, not consumers, will continue to have the final say regarding what “Do Not Track” means. And that will remain the *status quo* no matter what technical standard

---

<sup>33</sup> Kelly Clay, *Is Microsoft Going After Google With IE10?*, Forbes, June 4, 2012, available at <http://www.forbes.com/sites/kellyclay/2012/06/04/microsoft-going-after-google-with-ie10/>

<sup>34</sup> Jim Edwards, *Here's the Gaping Flaw in Microsoft's 'Do Not Track' System For IE10*, Business Insider, Aug. 29, 2012, available at <http://www.businessinsider.com/heres-the-gaping-flaw-in-microsofts-do-not-track-system-for-ie-10-2012-8> (“The hole is that the DNT is merely a signal telling advertisers about users’ preferences to not be tracked—it’s *not* a mechanism that actually blocks web ads from dropping tracking “cookies” onto browsers’ desktops and devices.”) (emphasis in original).



---

<sup>35</sup> Press release, Digital Advertising Alliance, Digital Advertising Alliance (DAA)

---

<sup>38</sup> *See supra*

Commission used the same ill-defined language in its March 2012 Privacy Report, that would import an “opt-in” requirement in a broad swath of contexts.<sup>41</sup> In addition, as I have also pointed out before, it is difficult, if not impossible, to reliably determine “consumer expectations” in any particular circumstance.<sup>42</sup>

Fourth, even if we were to assume that there is the sort of harm anticipated by Section 5(n), I do not see any support at all for the recommendations made in the Staff Report, much less the kind of rigorous cost-benefit analysis that should be conducted before the Commission embraces such recommendations. Nor do I think that they can be justified on the ground that technological change will occur so rapidly with respect to facial recognition technology that the Commission cannot adequately keep up with it when, and if, a consumer’s data security is compromised or facial recognition technology is used to build a consumer profile. On the contrary, the Commission has shown that it can and will act promptly to protect consumers when that occurs.

#### Deception, Rather Than Unfairness

As you may have figured out from my remarks, I believe that the “deception” prong of “unfairness or deceptive acts or practices” language of Section 5 is the better course for pursuing both the public policy and enforcement goals of our consumer protection mission when it comes to privacy, and even in most data breach cases. First, it is important to focus on the fact that “deception” includes both affirmative misrepresentations as well as failures to disclose material

---

<sup>41</sup> See 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* (Mar. 26, 2012) available at <http://ftc.gov/speeches/rosch/120326privacyreport.pdf>

<sup>42</sup> *Id.*

---

<sup>43</sup> Letter from the FTC to Hon. Jon D. Dingell, Committee on Energy and Commerce, United States House of Representatives, FTC Policy Statement on Deception at 2 (Oct. 4, 1983), appended to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984) Policy Statement on Deception, available at