THE FTC'S CRUSADE AGAINST DATA SECURITY BREACHES: LOOKING BACK, LOOKING FORWARD

by

MICHAEL D. SCOTT*

Final Version
Printout Date: May 13, 2014

* The author is professor of law at Southwestern Law School in Los Angeles, where he teaches a variety of technology law courses, including Cyberlaw and Information Privacy Law. He is author of seven legal titles in the information technology law field, including SCOTT ON INFORMATION TECHNOLOGY LAW (3rd ed. Aspen 2007) and SCOTT ON OUTSOURCING LAW & PRACTICE (Aspen 2006). The author would like to thank the Southwestern Law School faculty for their useful comments on earlier versions of this article.

Abstract

The Federal Trade Commission has taken the lead in the online privacy arena. It initially promoted self-regulation, but eventually realized that self-regulation was not working. Thereafter it began taking legal action against entities that violated the terms of their own privacy policies as deceptive trade practices. Eight years ago, the Commission began filing complaints under its unfairness doctrine against companies that experienced data security breaches. Until recently, those complaints were all settled by consent orders.

Looking back, this article analyzes the earlier data security breach cases under the carefully developed requirements of the unfairness doctrine, and argues that these actions were improperly filed. It further argues that the complaints and consent orders in these cases have provided no real guidance as to what a company should do (or not do) to avoid being the target of an unfairness action if it is the victim of a security breach. It also looks at new areas of FTC enforcement, including cases against information resellers whose clients did not properly secure the acquired data, and a case against a cell phone provider for weakening the security of its operating system.

Looking forward, this article analyzes two pending cases challenging the FTC's authority in this area and one trial court's ruling, and discusses congressional concern about the use of the unfairness doctrine and the FTC's plans to extend its asserted authority into the regulation of "big data."

Data security and the prevention of identity theft and other forms of misuse of personal data are too important to be left to the whim of the FTC or any other government agency. Companies need to know what is expected of them, so that they can implement appropriate technologies and put in place proper procedures to provide an adequate level of protection for sensitive personal data.

Table of Contents

I. Introduction

II. Early FTC Online Privacy Activities

III. FTC's Pursuit of Websites for Deceptive Acts or Practices

IV. FTC's Change of Tactics: Applying the "Unfairness" Principle to Data Security Breaches
- A. Evolution of the Unfairness Doctrine
  - 1. 1980 Unfairness Statement
  - 2. 1994 Amendment to the FTC Act
- B. The FTC's 2000 Report and Data Security
- C. A Data Security Breach As An "Unfair Act or Practice"
  - 1. Data Security Breaches
  - 2. BJ's Wholesale Club
  - 3. DSW, Inc.
  - 4. CardSystem Solutions, Inc.
- D. Applying the Unfairness Doctrine to Data Security Breaches
  - 1. Injury to Consumers
    - a. Substantial Injury
    - b. Cost-Benefit Analysis
    - c. Consumers' Ability to Avoid Injury
  - 2. Violation of an Established Public Policy
- E. The FTC Has Provided No Meaningful Guidance on What It Considers Unfair in the Data Security Breach Context
- F. Claims for Failure to Adequately Police Security Practices of their Customers
- G. HTC America – A Further Expansion of FTC Authority

V. Looking Forward
- A. Respondents Fight Back
  - 1. FTC v. LabMD
  - 2. FTC v. Wyndham Hotels
- B. Congress Chimes In
- C. Hints of FTC's Future Plans for the "Unfairness" Doctrine

VI. Conclusion

Everyone recognizes that there are imperfections and deficiencies in the state of privacy on the Internet, but let us not make the search for the perfect the enemy of the good.[1]

I. Introduction

The Federal Trade Commission ("FTC") has taken the lead in the United States in regulating privacy issues online.[2] The Commission began studying online privacy issues in 1995.[3] It initially supported industry self-regulation as the preferred method for dealing with online privacy.[4] However, various FTC surveys of websites showed that self-regulation was not working.[5] The FTC became concerned that, without strong privacy protection, there would be an erosion of confidence in the Web and a concomitant negative impact on the growth of electronic commerce.[6] As a result, over the last decade the agency has

---

[1] Privacy Online: Fair Information Practices in the Electronic Marketplace, Hearings Before the Senate Comm. on Commerce, Science, and Transportation, 106th Cong., 2d Sess., Dissenting opinion of FTC Commissioner Orson Swindle, at 26 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/swindledissent.pdf (last visited Nov. 17, 2013) [hereinafter "Swindle Dissent"].

[2] Privacy Online: Fair Information Practices in the Electronic Marketplace, Hearings Before the Senate Comm. on Commerce, Science, and Transportation, 106th Cong., 2d Sess. (May 2000) (statement of Robert Pitofsky, Chairman, Federal Trade Commission) ("Since 1995, the Commission has been at the forefront of the public debate concerning online privacy."), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited Nov. 17, 2013) [hereinafter "2000 FTC Report"].

[3] *See* Federal Trade Comm'n, Privacy Online: A Report to Congress 2 (June 1998) ("In April 1995, staff held its first public workshop on Privacy on the Internet, and in November of that year, the Commission held hearings on online privacy as part of its extensive hearings on the implications of globalization and technological innovation for competition and consumer protection issues."), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited Nov. 17, 2013) [hereinafter "1998 FTC Report"]. *See also* FTC Staff Report: The FTC's First Five Years Protecting Consumers Online (Dec. 1999), *available at* http://www.ftc.gov/os/1999/12/fiveyearreport.pdf (last visited Nov. 17, 2013).

[4] 2000 FTC Report, *supra* note 2, at i ("Throughout, the Commission's goal has been to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online.").

[5] *See* 1998 FTC Report, *supra* note 3, at 41. *See also* 2000 FTC Report, *supra* note 2, at ii-iii; Federal Trade Comm'n, Self-Regulation and Privacy Online: A Report to Congress 12 (July 1999), *available at* http://www.ftc.gov/os/1999/9907/privacy99.pdf (last visited Nov. 17, 2013) [hereinafter "1999 FTC Report"].

[6] *See* 2000 FTC Report, *supra* note 2, at 3 ("These findings suggest that consumers will continue to distrust online companies and will remain wary of engaging in electronic commerce until meaningful and effective consumer privacy protections are implemented in the online marketplace. If such

become increasing active in protecting consumer privacy rights online.[7]

Section 5 of the Federal Trade Commission Act[8] empowers the Commission to "prevent persons, partnerships, or corporations" from using "unfair or deceptive acts or practices in or affecting commerce."[9] Pursuant to those powers, the Commission has aggressively pursued websites that have violated their own privacy policies.[10] In 2003 the agency made a "dramatic shift"[11] in its enforcement efforts by filing complaints against organizations that had experienced data security breaches. Some of these companies had made representations concerning the security of their computer systems, which the agency attacked as

---

protections are not implemented, the online marketplace will fail to reach its full potential."). *See also* Letter from Mozelle W. Thompson, Federal Trade Comm'n, to Sen. John McCain (Apr. 24, 2002) (73% of online consumers who refused to purchase online did so because of privacy concerns), *available at* http://www.ftc.gov/os/2002/04/sb2201thompson.htm (last visited Nov. 17, 2013). It was estimated that $1.9 billion in e-commerce sales was lost in 2006 because of consumer concerns about Internet security. *See Gartner Says Nearly $2 Billion Lost in E-Commerce Sales in 2006 Due to Security Concerns of U.S. Adults* (Nov. 27, 2006), *available at* http://www.gartner.com/it/page.jsp?id=498974 (last visited Nov. 17, 2013).

[7] *See* §§ III-V *infra*. The FTC's role as privacy enforcer is not without its detractors. *See, e.g.,* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies,* 54 Hastings L.J. 877, 887-88 (2003) ("In many ways, this agency is an illogical choice for protection of citizens' privacy. . . . Reliance on the FTC as a primary enforcer of citizen privacy is misplaced.").

[8] *See generally* Federal Trade Commission Act, 15 U.S.C. §§ 41 *et seq*.

[9] Section 5 of the current FTC Act provides, in pertinent part:

> (1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.
> (2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, [except certain specified financial and industrial sectors] from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

Id. § 45.

[10] *See, e.g., In re* Geocities, Agreement Containing Consent Order, Aug. 13, 1998, *available at* http://www.ftc.gov/os/1998/9808/geo-ord.htm (last visited Nov. 17, 2013). *See also* In the Matter of Petco Animal Supplies, Inc., File No. 032 3221 (Nov. 8, 2004), *available at* http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf (last visited Nov. 30, 2013); Federal Trade Comm'n v. Doubleclick, Inc., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); Federal Trade Comm'n v. Intuit, Inc. 138 F. Supp. 2d 1272 (C.D. Cal. 2001).

[11] Goodwin Proctor LLP, *Data Security Breaches – The DSW and Other Recent FTC Actions Expand Requirements for Safeguarding Customer Data. What Can You Do To Reduce Your Exposure?,* at 1 (Dec. 6, 2005), *available at* http://www.martindale.com/computer-data-services/article_Goodwin-Procter-LLP_202800.htm (last visited Nov. 17, 2013).

deceptive trade practices.[12] But most of the other companies had made no such representations, yet were sued by the Commission under Section 5 of the Act for "unfair" trade practices.[13]

This article will look at the FTC's current strategy on data security cases and will analyze whether the Commission has exceeded its authority in pursuing the victims of malicious computer attacks who have made no misrepresentations as to the security of their systems or engaged in any other deceptive conduct.

The article will also look ahead at pending litigation challenging the FTC's authority in this area, at serious criticism being leveled against the Commission for misuse of its Section 5 authority, and at the FTC's plans to expand its reach under the "unfairness" doctrine to "big data" companies and their privacy and security activities.[14]

II. Early FTC Online Privacy Activities

The FTC initially sought to deal with online privacy issues by encouraging industry self-regulation.[15] It argued that the growth of the Internet in general, and electronic commerce in particular, mandated against sweeping regulations that might inhibit their growth.[16] Commentators believed that market forces would punish those companies who did not adequately protect consumer privacy, while rewarding companies that protected privacy with increased sales.[17] The main element of self-regulation

---

[12] *See* § III *infra*.

[13] *See* § IV *infra*. A list of the Commission's data security-related enforcement actions to date can be found at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Nov. 30, 2013).

[14] *See* § V.B *infra*.

[15] *See generally* 1999 FTC Report, *supra* note 5, at 6 ("[S]elf-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."); 1998 FTC Report, *supra* note 3, at i-ii.

[16] *Id.*

[17] *See, e.g.,* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 131 (1997) ("Individual responsibility, not regulation, is the principal and most effective form of privacy protection in most settings. The law should serve as a gap-filler, facilitating individual action in those situations in which the lack of competition has interfered with private privacy protection. In those situations, the law should only provide limited, basic privacy rights. . . . The purpose of these rights is to facilitate--not interfere with--the development of private mechanisms and individual choice as a means of valuing and protecting privacy"). *See also* 2000 FTC Report, *supra* note 2, Statement of Commissioner Thomas B. Leary Concurring in Part and Dissenting in Part, at 4 ("The Report does not explain why an adequately informed body of consumers cannot discipline the marketplace to provide an appropriate mix of substantive privacy provisions.") [hereinafter "Leary Statement"].

was the posting of privacy policies by websites that collected personal information, and FTC enforcement of those privacy policies.[18]

By 2000, however, the Commission realized that industry self-regulation was not working[19] and that "substantially greater incentives" would be required to protect consumer privacy online.[20] In its 2000 Report, the Commission indicated that while it had the power under section 5 of the FTC Act to pursue deceptive practices, such as a website's failure to abide by a stated privacy policy (i.e., breach of contract claims),[21] it could not require companies to adopt privacy policies in the first place.[22] Accordingly, the Commission proposed legislation that would provide it with the authority to issue and enforce specific privacy regulations.[23]

However, with the election of President George W. Bush, and a change in leadership at the Commission, there was also a change in the agency's position. The new FTC Chairman, Timothy Muris, announced that the agency would expand enforcement of existing laws rather than pursuing new legislation.[24] Muris indicated that the Commission was "primarily a law enforcement agency" which "best carries out its consumer protection mission" through "aggressive enforcement of the basic laws of consumer protection."[25] He further indicated that in his opinion, "the

---

[18] *See* Federal Trade Comm'n, Consumer Privacy on the World Wide Web, Prepared Statement Before the House Comm. on Commerce, Subcomm. on Telecom., Trade and Consumer Protection (July 21, 1998), *available at* http://www.ftc.gov/os/1998/07/privac98.htm (last visited Nov. 17, 2013).

[19] 2000 FTC Report, *supra* note 2, at ii.

[20] *Id.* at ii-iii.

[21] *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur,* 53 Vand. L. Rev. 2041, 2057 (2000) ("The FTC's promotion of privacy policies is instructively viewed as an attempt to cause websites to make quasi-contractual statements in writing. The more contractual these statements are, the more enforceable they will be.").

[22] 2000 FTC Report, *supra* note 2, at 34 ("As a general matter, however, the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web sites"). *But see* Julia Gladstone, The U.S. Privacy Balance and the European Privacy Directive: Reflections on the United States Privacy Policy, 7 Willamette J. Int'l L. & Disp. Reso. 10, 28 (2000) ("Upon the recommendation of the FTC many web sites now publish their privacy policies . . . .").

[23] 2000 FTC Report, *supra* note 2, at 36-38.

[24] Devin Gensch, *Putting Enforcement First,* The Recorder, Nov. 7, 2001, at 5. *See also* Remarks of Timothy J. Muris, The Privacy 2001 Conference (Oct. 4, 2001), *available at* http://www.ftc.gov/speeches/muris/privisp1002.htm (last visited Nov. 17, 2013).

[25] Prepared Statement of FTC Chairman Timothy J. Muris, Challenges Facing the Federal Trade Commission, Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection, House Comm. on Energy and Commerce (Nov.

particular issue of broad based, Internet only legislation is still premature at this moment."[26]

III. FTC's Pursuit of Websites for Deceptive Acts or Practices

One of the pillars of Chairman Muris's privacy enforcement efforts was to pursue websites for deceptive trade practices.[27] The first FTC case involving Internet privacy was *In re GeoCities*.[28] The complaint[29] focused on two activities that the agency claimed were deceptive trade practices.

First, the complaint alleged that GeoCities had misrepresented "the uses and privacy of the information it collect[ed]" from consumers, namely, that the website had "sold, rented or otherwise marketed and disclosed" personal data "to third parties who have used this information for purposes other than those for which members have given permission," contrary to the website's stated privacy policy.[30]

Second, it alleged that GeoCities had made "misrepresentations involving sponsorship" when it stated that it personally collected and maintained children's personal information for an online club.[31] Instead, the complaint alleged that third parties were collecting and maintaining this personal data from children.[32]

7, 2001), *available at* http://energycommerce.house.gov/reparchives/107/hearings/11072001Hearing403/print.htm (last visited Nov. 17, 2013).

[26] *Id.*

[27] 15 U.S.C. §45(a). *Deceptive practices* are defined as "material representations or omissions likely to mislead a reasonable consumer." Federal Trade Comm'n v. Tashman, 318 F.3d 1273, 1277 (11th Cir. 2003). *See* Steven Hetcher, *supra* note 21, at 2058 ("[I]t is clear that once websites provide privacy policies, the FTC will be in a position to exercise its deceptive practices jurisdiction if those policies are not followed. By encouraging websites to provide privacy policies in the first place, the FTC has created a situation in which it is now able to extend its enforcement jurisdiction onto the Internet.").

[28] Press Release, *FTC, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case: Commission Establishes Strong Mechanisms for Protecting Consumers' Privacy Online* (Aug. 13, 1998), *available at* http://www.ftc.gov/opa/1998/9808/geocitie.htm (last visited Nov. 17, 2013).

[29] *See In re* GeoCities, Complaint (Feb. 5, 1999), *available at* http://http://www.ftc.gov/os/1999/02/9823015cmp.htm (last visited Nov. 17, 2013) [hereinafter "GeoCities Complaint"].

[30] *Id.* ¶¶ 12-16.

[31] *Id.* ¶ 18.

[32] *Id.* ¶ 19.

The FTC claimed that GeoCities' conduct constituted "unfair or deceptive acts or practices" in violation of section 5 of the Act. The case quickly settled with a Consent Order.[33]

The *Geocities* Consent Order[34] required GeoCities to clearly post a privacy notice "telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information."[35] This Consent Order became the blueprint for a series of complaints filed against websites that, *inter alia,* failed to comply with their own posted privacy policies.[36]

Since *Geocities*, the Commission has brought a number of cases against companies for violating their own, published privacy policies.[37] These actions generally alleged that the companies made implicit or explicit promises to protect sensitive consumer information, but failed to do so (either because hackers[38] were able to gain unauthorized access to consumers' personal information[39]

---

[33] *In re* Geocities, Decision and Order (Feb. 5, 1999), *available at* http://www.ftc.gov/os/1999/02/9823015.htm (last visited Nov. 17, 2013) [hereinafter "Consent Order"].

[34] *Id.*

[35] *Id.* § IV. These requirements reflected the Commission's earlier pronouncement that website privacy policies should reflect the Fair Information Practice Principles (FIPPs), including the Notice/Awareness Principle, the Choice/Consent Principle, and the Access/Participation Principle. *See generally* 2000 FTC Report, *supra* note 4, at n.1. For a further discussion of these Principles, see § IV.B. infra.

[36] In addition, the provisions of the Consent Order relating to the collection and use of information from children formed the basis for the 1998 Children's Online Privacy Protection Act (COPPA), Pub. L. No. 105 -277, Div. C, tit. XIII, § 1301, 112 Stat. 2681-2728 (1998), *codified at* 15 U.S.C. §§ 6501-06, and its implementing regulations. 16 C.F.R. Part 312 (Apr. 21, 2000).

[37] Recent cases include *Facebook, Inc.,* No. C-4365 (F.T.C. Aug. 10, 2012), *available at* http://www.ftc.gov/os/caselist/0923184/120810facebookcmpt.pdf (last visited Nov. 29 2013); *Myspace, Inc.,* No. C-4369 (F.T.C. Sept. 11, 2012), *available at* http://ftc.gov/os/caselist/1023058/120911myspacecmpt.pdf (last visited Nov. 29, 2013).

[38] A *hacker* is "[an] unauthorized individual[] who attempt to penetrate information systems; browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way." Gov't Accountability Off., Information Security: Computer Hacker Information Available on the Internet (GAO/T-AIMD-96-108) (June 5, 1996), *available at* http://www.gao.gov/archive/1996/ai96108t.pdf (last visited Nov. 20, 2013).

[39] *See In re* Guidance Software, Inc., File No. 0623057, Agreement Containing Consent Order (Nov. 16, 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf (last visited Nov. 17, 2013); *In re* Nations Title Agency Inc., FTC Docket No. C-4161, Decision and Order (June 20, 2006), *available at* http://www.ftc.gov/os/caselist/0523117/0523117NationsTitleDecisionandOrder.pdf (last visited Nov. 17, 2013); *In re* Petco Animal Supplies, Inc., FTC Docket No. C-4133, Decision and Order (Mar. 4, 2005), *available at* http://www.ftc.gov/os/caselist/0323221/050308do0323221.pdf (last visited Nov. 17, 2013); *In re* MTS Inc., d/b/a Tower

or the company intentionally disclosed the information to others[40]), making their privacy representations either deceptive or unfair.[41] The consent orders settling these cases required the companies, *inter alia,* to comply with their own privacy policies, as well as to implement "reasonable security measures" to safeguard customer data from unauthorized disclosure.[42]

The Commission has also used its Section 5 powers to pursue deception claims against online companies for a variety of

---

Records/Books/Video, FTC Docket No. C-4110, Decision and Order (May 28, 2004), *available at* http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf (last visited Nov. 17, 2013); *In re* Guess?, Inc., FTC Docket No. C-4091 (July 30, 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf (last visited Nov. 17, 2013); *In re* Microsoft Corp., FTC Docket No. C-4069, Decision and Order (Dec. 20, 2002), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftdecision.pdf (last visited Nov. 17, 2013); *In re* Eli Lilly & Co., FTC Docket No. C-4047, Decision and Order (May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elilillydo.htm (last visited Nov. 17, 2013).

Another line of cases arising from the *Geocities* Consent Order relates to the improper collection and use or disclosure of information from children. Because this article does not address the FTC's enforcement efforts concerning the privacy of children's information online, these cases will not be discussed.

[40] *See, e.g., In re* Vision I Properties LLC, d/b/a/ Cartmanager Int'l, FTC File No. 0423068, Agreement (Mar. 10, 2005), *available at* http://www.ftc.gov/os/caselist/0423068/050310agree0423068.pdf (last visited Nov. 17, 2013); *In re* Gateway Learning Corp., FTC Docket No. C-4120, Decision and Order (Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf (last visited Nov. 17, 2013).

[41] In most of these cases, the complaint contained a "catch-all" allegation that the respondent's failure to comply with its own website privacy policy was either a deceptive or an unfair act or practice, but the acts upon which the complaint was grounded were the respondent's failure to comply with its own privacy policy. *See, e.g., In re* Petco Animal Supplies, Inc., FTC Docket No. C-4133, Complaint (Mar. 4, 2005), *available at* http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf (last visited Nov. 17, 2013), where the complaint alleged that through the privacy policies posted on the website, the "respondent represented, expressly or by implication that the personal information it obtained from consumers through www.PETCO.com was maintained in an encrypted format and therefore was inaccessible to anyone but the customer providing the information." *Id.* ¶6. The concluding paragraph of the complaint alleged generally that: "The acts and practices of the respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act." *Id.* ¶15. Importantly, nowhere in any of these complaints was it alleged that the failure of the respondents to implement reasonable security measures was itself either a deceptive or an unfair act or practice.

[42] These provisions of the consent orders relating to the implementation of reasonable security measures foretold the settlement terms that the Commission would later impose upon respondents charged with engaging in "unfair" trade practices. However, at the time of these earlier consent orders, there was no indication that the Commission would attempt to impose these provisions on companies other than those that had violated their own privacy policies.

Internet-related claims unrelated to a violation of published privacy policies. These include claims against:

1. spyware[43] and adware[44] distributors that surreptitiously downloaded software onto unsuspecting users' computers,[45]
2. those who made materially deceptive representations in marketing a spyware removal product,[46]
3. those who made fraudulent claims in selling prescription drugs online,[47]
4. a credit reporting company that failed to verify the identity of persons to whom it was disclosing confidential consumer information and failed to monitor unauthorized activities,[48]
5. a company that markets video cameras designed to allow consumers to monitor their homes remotely,[49]
6. a company that failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers,[50]

---

[43] *Spyware* "includes 'adware' and other programs that 'secretly install on your computer without your permission or knowledge' and may cause 'pop ups,' banner advertisements, and other extraneous ads, send 'spam' e-mail messages, hijack search engine links or home pages, trace online activity, allow others to remotely access a computer, record private information or steal passwords. It also includes 'adware, keyloggers, Trojans, hijackers, dialers, viruses, spam, and general ad serving.'" Federal Trade Comm'n v. MaxTheater, Inc., 2005 WL 3724918, at *2 (E.D. Wash. Dec. 6, 2005).

[44] *Adware* is "[a] type of 'spyware' that uses collected information to display targeted advertisements. . . ." Federal Trade Comm'n v. Seismic Entertainment Productions, Inc., 2004 WL 2403124, at *1 (D.N.H. Oct. 21, 2004).

[45] See, e.g., In the Matter of Aaron's, Inc., Complaint, Oct. 22, 2013, *available at* http://www.ftc.gov/os/caselist/1223264/131022aaronscmpt.pdf (last visited Nov. 17, 2013); *In re* Zango, Inc. f/k/a/ 180Solutions, Inc., Complaint, Mar. 7, 2007, *available at* http://www.ftc.gov/os/caselist/0523130/0523130c4186complaint.pdf (last visited Nov. 17, 2013); Federal Trade Comm'n v. MaxTheater, Inc., 2005 WL 3724918, at *2 (E.D. Wash. Dec. 6, 2005); Federal Trade Comm'n v. Seismic Entertainment Productions, Inc., 2004 WL 2403124 (D.N.H. Oct. 21, 2004).

[46] Federal Trade Comm'n v. Trustsoft, Inc., 2005 WL 1523915 (S.D. Tex. June 14, 2005).

[47] Federal Trade Comm'n v. Rennert, Complaint (filed D. Nev. July 6, 2000), *available at* http://www.ftc.gov/os/2000/07/iogcomp.htm (last visited Nov. 17, 2013).

[48] United States v. Choicepoint, Inc., Case No. 106-CV-0198, Stipulated Final Judgment and Order (N.D. Ga. Jan. 26, 2005), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf (last visited Nov. 17, 2013).

[49] In the Matter of TRENDnet, Inc., Complaint, Sept. 4, 2013, *available at* http://www.ftc.gov/os/caselist/1223090/130903trendnetcmpt.pdf (last visited Nov. 21, 2013).

7. a reverse auction site that used improper promotional activities to solicit users of a competitive auction site,[51] and
8. unauthorized charges in connection with "phishing."[52]

Most of these complaints included general allegations that the conduct was either a deceptive or an unfair act or practice,[53] but the focus was always on the deceptiveness of the targeted practices.

IV. FTC's Change of Tactics: Applying the "Unfairness" Principle to Data Security Breaches

Since 2005, the FTC has filed a large number of complaints against companies that experienced data security breaches without any violation of published privacy policies. The Commission has claimed in each of these cases that the respondent failed to adopt "reasonable security measures" to protect sensitive data, and that such failures *alone* amounted to an unfair act or practice in violation of Section 5 of the FTC Act.

While the concept of "unfairness" has developed within the FTC and the courts over the last three decades, it has had a checkered history.[54] Generally the doctrine has been limited to

---

[50] In the Matter of HTC America Inc., Complaint, July 2, 2013, available at http://www.ftc.gov/os/caselist/1223049/130702htccmpt.pdf (last visited Nov. 21, 2013).

[51] Federal Trade Comm'n v. ReverseAuction.com, Complaint (filed D.D.C. Jan. 6, 2000), *available at* http://www.ftc.gov/os/2001/01/reversecmp.htm (last visited Nov. 17, 2013).

[52] Federal Trade Comm'n v. Hill, No. H 03-5537 (filed S.D. Tex. Dec. 3, 2003), *available at* http://www.ftc.gov/os/caselist/0323102/040322cmp0323102.pdf (last visited Nov. 17, 2013); Federal Trade Comm'n v. C.J., No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), *available at* http://www.ftc.gov/os/2003/07/phishingcomp.pdf (last visited Nov. 17, 2013). *Phishing* is a high-tech scam that use spam or pop-up messages "to lure personal information (credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information) from unsuspecting victims. *See* FTC Consumer Alert, How Not to Get Hooked by a "Phishing" Scam 1 (Oct. 2006), *available at* http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf (last visited Nov. 17, 2013).

[53] *See, e.g., In re* Zango, Inc., Complaint, *supra* note 44, at ¶¶ 16-18 (claims for deceptive failure to adequately disclose adware, unfair installation of adware and unfair uninstall practices).

[54] *See* J. Howard Beales III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (June 2003), *available at* http://www.ftc.gov/speeches/beales/unfair0603.shtm (last visited Nov. 26, 2013) (hereinafter "Beales").

activities relating to the advertising, marketing and sale of products or services.[55]

The question is whether the unfairness doctrine, as it currently exists, should be extended to activities unrelated to the advertising, marketing or sale of products or services, and in particular, whether the doctrine should be applied *sua sponte* by the Commission to companies that have suffered data security breaches.

A. Evolution of the Unfairness Doctrine

The Federal Trade Commission was established in 1915.[56] Its purpose "was to prevent unfair methods of competition in commerce as part of the battle to 'bust the trusts.'"[57] Congress expanded its authority over the ensuing decades. In 1938, Congress passed the Wheeler-Lea Amendment,[58] which amended the FTC Act to prohibit "unfair or deceptive acts or practices" in addition to "unfair methods of competition" -- "thereby charging the FTC with protecting consumers directly, as well as through its antitrust efforts."[59]

FTC jurisdiction over "unfair" acts or practices was added to Section 5 of the FTC Act in 1938.[60] The FTC did not use the "unfairness" prong of Section 5 extensively until 1972. In that year, a U.S. Supreme Court decision encouraged the Commission to

---

[55] *See, e.g.*, Federal Trade Comm'n, Dot Com Disclosures 1 (May 2000), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom (last visited Nov. 17, 2013).

[56] The agency was created by the Federal Trade Commission Act (Act of Sept. 26, 1914, ch. 311, § 5, 38 Stat. 717, 719 (*codified as amended at* 15 U.S.C. §§ 41-58 (1994)). The Commission consists of a five-member board with broad authority to regulate unfair and deceptive business practices. No more than three of the FTC members can be from the same political party, and they are appointed for overlapping seven-year terms. *Id.*

[57] About the Federal Trade Commission, *available at* http://www.ftc.gov/ftc/about.shtm (last visited Nov. 17, 2013). Yet, even at this early date, Congress recognized how vague the concept of "unfairness" was. *See* H.R. Conf. Rep. No.1142, 63rd Cong., 2d Sess. 19 (1914) ("It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again. If Congress were to adopt the method of definition, it would undertake an endless task."). *See also* Senate Report No. 597, 63rd Cong., 2d Sess. 13 (1914).

[58] Pub. L. No. 75-447, §§ 3, 52 Stat. 111, 111 (1938) (*codified as amended at* 15 U.S.C. § 45(a)(1)).

[59] Beales, *supra* note 54.

[60] Wheeler-Lea Amendment of 1938, Pub. L. No. 75-447, §§ 3, 52 Stat. 111, 111 (1938) (*codified as amended at* 15 U.S.C. § 45(a)(1)).

apply unfairness to protect consumers in the area of advertising.[61] In *Federal Trade Commission v. Sperry & Hutchinson Co.*,[62] the Court noted that the consumer, as well as the competitor, needed protection from unfair trade practices, stating:

> Thus, legislative and judicial authorities alike convince us that the Federal Trade Commission does not arrogate excessive power to itself if, in measuring a practice against the elusive, but congressionally mandated standard of fairness, it, like a court of equity, considers public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws.[63]

In a footnote in the decision,[64] the Court cited approvingly the criteria for unfairness that the Commission had set forth in an earlier proposed rule relating to cigarettes advertising and labeling.[65] The factors set forth in the Cigarette Rule were:

1. Whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise -- whether, in other words, it is within at least the penumbra of some common law, statutory, or other established concept of unfairness.
2. Whether it is immoral, unethical, oppressive, or unscrupulous.
3. Whether it causes substantial injury to consumers (or competitors or other business people).[66]

This Supreme Court's decision, and the 1975 Magnuson-Moss Warranty-Federal Trade Commission Improvement Act,[67]

---

[61] *See* Dorothy Cohen, *Unfairness in Advertising Revisited,* J. of Marketing 73, 73 (Winter 1982).

[62] 405 U.S. 233 (1972).

[63] *Id.* at 244. This language has been criticized as "suggesting almost unlimited agency authority. . . ." Robert A. Skitol, *How BC and BCP Can Strengthen Their Respective Policy Missions Through New Uses of Each Other's Authority,* 72 Antitrust L.J. 1167, 1168 (2005).

[64] *S&H,* 405 U.S. at 244 n.5.

[65] Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8355 (July 2, 1964) [hereinafter "Cigarette Rule"].

[66] *Id.*

[67] Pub. L. 93–637, 88 Stat. 2183 (Jan. 4, 1975), *codified at* 15 U.S.C. §§ 2301 *et seq.* (as amended).

which provided the FTC with rulemaking authority,[68] resulted in an "ensuing decade of 'over-exuberance' as the agency tested the outer limits of its powers."[69] The FTC's actions were widely criticized,[70] and the matter came to a head in 1980.

1. 1980 Unfairness Statement

In 1980 Congress enacted the Federal Trade Commission Improvement Act,[71] which "prohibited application of the unfairness doctrine in several specified proceedings and curtailed its use in rulemaking for at least three years while Congress engaged in oversight hearings."[72]

Later that year, the Consumer Subcommittee of the Senate Committee on Commerce, Science, and Transportation held oversight hearings on the unfairness doctrine. In connection with those hearings, the Commission wrote a letter[73] to the ranking

> In 1975 the Magnuson-Moss Act provided the Commission with rulemaking authority, permitting the FTC to establish trade regulation rules that specify unfair or deceptive acts or practices that are prohibited. This Act neither defined nor clarified the concept of unfairness.

Cohen, *supra* note 61, at 74.

[69] Skitol, *supra* note 63, at 1169. *See also* Ernest Gellhorn, *Trading Stamps, S&H, and the FTC's Unfairness Doctrine,* 1983 Duke L.J. 903, 906 ("The progeny of *S&H* has been a series of unsound decisions, persistent and unwise use of FTC resources, and imposition of costly and unnecessary requirements on retailers and advertisers.").

[70] *See, e.g.,* Teresa M. Schwartz, *Regulating the Unfair Practices Under the FTC Act: The Need for a Legal Standard of Unfairness,* 11 Akron L. Rev. 1 (1977); William Erxleben, *The FTC's Kaleidoscopic Unfairness Statute: Section 5,* 10 Gonz. L. Rev. 333 (1975).

[71] Pub. L. No. 96-252, 94 Stat. 374 (May 28, 1980), *codified as amended* in scattered sections of 15 U.S.C. (1982).

[72] Gellhorn, *supra* note 69, at 942.

[73] *See* Federal Trade Comm'n, FTC Policy Statement on Unfairness, Letter from Michael Pertschuk, Chairman, Federal Trade Comm'n to Hon. Wendell H. Ford, Chairman, and Hon. John C. Danforth, Ranking Minority Member, S. Comm. on Commerce, Science, and Transportation, Consumer Subcomm. (Dec. 17, 1980), *reprinted in* International Harvester, Inc., 104 F.T.C. 949, 1070-76 (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm (last visited Nov. 29, 2013) [hereinafter "Unfairness Statement"].

For a discussion of the policy developments that led to the preparation of the Unfairness Statement, *see* Neil W. Averitt, *The Meaning of "Unfair Acts or Practices" in Section 5 of the Federal Trade Commission Act,* 70 Geo. L.J. 225 (1981); Timothy J. Muris & J. Howard Beales, III, *The Limits of Unfairness Under the Federal Trade Commission Act,* Association of Nat'l Advertisers Publication (1991) (also discusses the Commission's use of unfairness subsequent to 1980).

members of the Committee in which it "narrow[ed] the unfairness doctrine."[74] The letter stated:

> We recognize that the concept of consumer unfairness is one whose precise meaning is not immediately obvious, and also recognize that this uncertainty has been honestly troublesome for some businesses and some members of the legal profession. This result is understandable in light of the general nature of the statutory standard.[75]

The *Unfairness Statement* noted, however, that:

> The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time.[76]

The *Unfairness Statement* noted that by 1964 the agency had identified three factors to be considered in applying the unfairness doctrine:

> 1. whether the practice injures consumers;
> 2. whether it violates established public policy; and
> 3. whether it is unethical or unscrupulous.[77]

The *Unfairness Statement* stated that the Commission now agreed to abandon the third element, and "pledged to proceed only

---

[74] Gellhorn, *supra* note 69, at 956.

[75] Unfairness Statement, 104 F.T.C. at 1071.

[76] *Id.* at 1072.

[77] *Id.* These factors were adapted from the factors set forth in the Cigarette Rule, *supra* note 62. In *Federal Trade Comm'n v. Sperry & Hutchinson,* 405 U.S. 233, 244-45 n.5 (1972), the Supreme Court appeared to "put its stamp of approval on the Commission's evolving use of a consumer unfairness doctrine not moored in the traditional rationales of anticompetitiveness or deception." American Financial Servs. Ass'n v. Federal Trade Comm'n, 767 F.2d 957, 968 (D.C. Cir. 1985). However, "the FTC's use of its unfairness doctrine has substantially evolved since *Sperry*." Letter from Timothy J. Muris, Chairman of the Federal Trade Comm'n to the U.S. Dept. of Transportation (June 6, 2003), *available at* http://www.ftc.gov/os/2003/06/dotcomment.htm (last visited Nov. 17, 2013).

if either the unjustified consumer injury test or the violation of public policy test was satisfied."[78]

In 1984, the Commission formally adopted its 1980 *Unfairness Statement* as the standard that it would apply in proceedings that challenged specific acts or practices as unfair.[79]

2. 1994 Amendment to the FTC Act

In 1994, Congress amended the FTC Act by effectively codifying the agency's definition of unfairness from the *Unfairness Statement*. Section 5(n) now states:

> The Commission shall have no authority under this section or section 18 to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[80]

B. The FTC's 2000 Report and Data Security

The issue of data security[81] predates the Internet. Data security is one of the lynchpins of what is generally referred to as the *Fair Information Practice Principles*.[82] The Fair Information Practice Principles were first articulated in a report by the

---

[78] Gellhorn, *supra* note 69, at 942.

[79] *In re* International Harvester Co., 104 F.T.C. 949, 1060-62 (1984).

[80] Federal Trade Commission Act Amendments of 1994 (H.R. 2243), *codified at* 15 U.S.C. § 45(n).

[81] The term *data security* means "[p]rotection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure." Comm. on Nat'l Security Sys., National Information Assurance (IA) Glossary 21 (Instruction No. 4009 (June 2006)), *available at* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf (last visited Nov. 17, 2013).

[82] There are five Fair Information Practice Principles: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. *See* 1998 FTC Report, *supra* note 3, at 7. It is the fourth principle that is relevant to this discussion. *See also* 2000 FTC Report, *supra* note 2, at iii ("Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers").

Department of Health, Education and Welfare in 1973.[83] Since then, "a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies."[84]

One of the Fair Information Practice Principles, referred to as the *Security Principle,* as articulated in various FTC documents over the last several decades, provides general guidance as to what data security should include, but nothing specific. In particular, as noted in the 1998 FTC Report:

> Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.[85]

"Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers."[86] The Fair Information Practice Principles were promoted[87] by the Commission as appropriate benchmarks for companies in self-regulating their promulgation

---

[83] *See* DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973).

[84] 1998 FTC Report, *supra* note 3, at 48 n. 27. A series of reports setting forth the core fair information practice principles include: The Privacy Protection Study Comm'n, Personal Privacy in an Information Society (1977); Organization for Economic Cooperation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980); Information Infrastructure Task Force, Information Policy Comm., Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information (1995); Dept. of Commerce, Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (1995); The European Union Directive on the Protection of Personal Data (1995); and the Canadian Standards Ass'n, Model Code for the Protection of Personal Information: A National Standard of Canada (1996).

[85] 1998 FTC Report, *supra* note 3, at 10.

[86] *Id.* at 11.

[87] The Commission has stated that "[a]s a general matter, however, the Commission lacks authority to require firms to adopt information practice policies." 2000 FTC Report, *supra* note 2, at 34.

and use of online privacy policies.[88] They were also the basis for the Consent Order in the *Geocities* case,[89] and were implemented in the Children's Online Privacy Protection Act of 1998.[90]

In December 1999, the Commission established the Advisory Committee on Online Access and Security.[91] The Advisory Committee was asked, *inter alia,* to "consider the parameters of 'reasonable access' to personal information collected from and about consumers online and 'adequate security' for such information."[92] The Advisory Committee submitted its Final Report on May 15, 2000.[93]

In its Final Report, the Advisory Committee indicated that:

1. "[S]ecurity is a process, and that no single standard can assure adequate security, because technology and security threats are constantly evolving."[94]
2. "[E]ach Web site [should] have a security program to protect personal data that it maintains, and that the program [should] specify its elements and be 'appropriate to the circumstances.'"[95]
3. "The 'appropriateness' standard, which would be defined through case-by-case adjudication, takes into account changing security needs over time as well as the particular circumstances of the Web site, including the risks it faces, the costs of protection, and the type of the data it maintains."[96]

The FTC in its 2000 Report called for the passage of broad privacy protection legislation that would (i) "set forth a basic level of privacy protection for all visitors to consumer-oriented commercial Web sites to the extent not already provided by the

---

[88] Federal Trade Comm'n, Prepared Statement on Consumer Privacy on the World Wide Web, Before the Subcomm. on Telecomm., Trade & Consumer Protection, House Comm. on Commerce (July 21, 1998), *available at* http://www.ftc.gov/os/1998/9807/privac98.htm (last visited Nov. 17, 2013).

[89] *See* Consent Order, note 33 *supra*.

[90] Pub. L. No. 105 to 277, Div. C, tit. XIII, § 1301, 112 Stat. 2681-2728 (1998), *codified at* 15 U.S.C. §§ 6501-06, and its implementing regulations (16 C.F.R. Part 312 (Apr. 21, 2000)).

[91] *See* Notice of Establishment of the Federal Trade Commission Advisory Committee on Online Access and Security, *available at* http://www.ftc.gov/acoas (last visited Nov. 17, 2013).

[92] 2000 FTC Report, *supra* note 2, at 28.

[93] *See* Final Report of the Federal Trade Comm'n Advisory Committee on Online Access and Security (May 15, 2000), *available at* http://www.ftc.gov/acoas/papers/acoasfinal1.pdf (last visited Nov. 17, 2013) [hereinafter "ACOAS"].

[94] *Id.* at 19.

[95] *Id.* at 26.

[96] *Id.* at 25.

COPPA," (ii) apply the Fair Information Practice Principles to online data privacy generally,[97] and (iii) give the Commission specific authority to "promulgate more detailed standards pursuant to the Administrative Procedure Act."[98] It indicated that:

> The Commission recognizes that the implementation of these practices may vary with the nature of the information collected and the uses to which it is put, as well as with technological developments. For this reason, the Commission recommends that any legislation be phrased in general terms and be technologically neutral. Thus the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency in promulgating its rules and regulations.
>
> Such rules and regulations could provide further guidance to Web sites by defining fair information practices with greater specificity. For example, after soliciting public comment, the implementing agency could expand on what constitutes "reasonable access" and "adequate security" in light of the implementation issues and recommendations identified and discussed by the Advisory Committee. . . .
>
> . . . The Commission hopes and expects that the industry and customers would participate actively in developing regulations under the new legislation. . . .[99]

There was a strong dissent to the 2000 Report by Commissioner Orson Swindle, who objected to the Commission's seeming abandonment of self-regulation in favor of "extensive government regulation."[100]

> The Commission owes it to Congress – and the public – to comment more specifically on what it has in mind before it recommends legislation that requires all consumer-oriented commercial Web sites to comply with

---

[97] *See, e.g.,* 2000 FTC Report, *supra* note 2, at iii.

[98] *Id.* at ii, 36, 37. While the Report refers to "the implementing authority" generally, it is clear from the context of the Report that the Commission considered itself to be the appropriate agency to implement the Fair Information Practice Principles. *See, e.g.,* Swindle Dissent, *supra* note 1, at 1 ("The majority recommends that Congress give rulemaking authority to an 'implementing agency' (presumably the Commission). . . ."). The Administrative Procedure Act is at 5 U.S.C. § 553.

[99] 2000 FTC Report, *supra* note 2, at 37-38.

[100] Swindle Dissent, *supra* note 1, at 1.

> breathtakingly broad laws whose details will be filled in later during the rulemaking process.
>
> Most disturbing, the Privacy Report is devoid of any consideration of the costs of legislation in comparison to the asserted benefits of enhancing consumer confidence and allowing electronic commerce to reach its full potential.[101]

He concluded by warning:

> The current recommendation, however, defies not just logic but also fundamental principles of governance. In recognition of some of the complexities of regulating privacy – particularly Access and Security – the Commission asks Congress to require all commercial consumer-oriented Web sites to comply with extensive, yet vaguely phrased, privacy requirements and to give the Commission (or some other agency) a blank check to resolve the difficult policy issues later. This would constitute a troubling devolution of power from our elected officials to unelected bureaucrats.[102]

Commissioner Thomas B. Leary also dissented to portions of the Report, including the provisions relating to data security.[103] He argued that the legislative recommendation in the Report was "too broad because it suggests the need for across-the-board substantive standards when, in most cases, clear and conspicuous notice alone should be sufficient."[104]

Leary also took issue with the Commission's claim that the fair information practices are "widely-accepted" in either the online or offline worlds.[105] Leary indicated that the Report failed to explain what was meant by "'reasonable' standards"[106] and expressed concern that the legislation, as proposed in the Report, "could in many cases lead to vast expense for trivial benefit and which provides an ominous portent for the content of any substantive rules." He noted that "[i]n some cases, involving particular kinds of information or particular uses, the risk of harm may be so great that specific substantial standards are required.

---

[101] *Id.* at 1-2.
[102] *Id.* at 27.
[103] *See* Leary Statement, *supra* note 17.
[104] *Id.* at 1.
[105] *Id.* at 5-6.
[106] *Id.* at 6.

This is a legislative judgment. Congress can, and already does pass industry-specific legislation to deal with these situations."[107]

Over 13 years have passed since the Commission pushed for specific legislation to provide broad consumer privacy protection, and Congress thus far has declined to act. Starting in 2005, the FTC decided to move forward on its own without any new, specific privacy laws or delegation of authority from Congress. Instead, the Commission chose to proceed pursuant to the "unfairness" prong of Section 5 of the FTC Act.

C. A Data Security Breach As An "Unfair Act or Practice"

For the last 8 years, the FTC has applied the unfairness doctrine to situations in which a company has suffered a data security breach. The Commission has held no hearings, solicited no public comments, engaged in no rulemaking, nor issued any policy statements or guidelines on when, if ever, the unfairness doctrine can, or should, be applied to data security breaches.[108] Instead, the agency merely began filing complaints against companies that suffered such breaches.

The application of the unfairness doctrine to data security breaches constitutes a significant shift in how the Commission has used the doctrine previously. For example, in 2003, J. Howard Beales III, then-Director of the FTC Bureau of Consumer Protection indicated that:

> As codified in 1994, in order for a practice to be unfair, the injury it causes must be (1) substantial, (2) without offsetting benefits, and (3) one that consumers cannot reasonably avoid. Each step involves a detailed, fact-specific analysis that must be carefully considered by the Commission. *The primary purpose of the Commission's*

---

[107] *Id.* at 7, *citing* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.;* Telecommunications Act of 1996, 47 U.S.C. §§ 222 *et seq.;* Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710 *et seq.;* Cable Communications Policy Act of 1984, 47 U.S.C. §§ 551 *et seq.;* and Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq*.

[108] In fact, prior statements from FTC officials seemed to indicate that the Commission itself believed that its power in the online privacy area was limited to deceptive trade practices. *See, e.g.,* Jeffrey Benner, *FTC Powerless to Protect Privacy,* Wired Mag., May 31, 2001 ("'The agency's jurisdiction is (over) deception,' Lee Peeler, the FTC's associate director for advertising practices, said, 'If a practice isn't deceptive, we can't prohibit them from collecting information. The agency doesn't have the jurisdiction to enforce privacy. It has the authority to challenge deceptive practices.'"), *available at* http://www.wired.com/politics/security/news/2001/05/44173 (last visited Nov. 17, 2013).

> *modern unfairness authority continues to be to protect consumer sovereignty by attacking practices that impede consumers' ability to make informed choices.*[109]

Some commentators have questioned whether the mere fact that a party has suffered a data security breach constitutes an "unfair act or practice" without a showing of some overt act on the part of the respondent.[110]

Until 2012, all of the actions brought for data security breaches quickly settled, thereby providing no judicial opinions on the efficacy or legality of the Commission's actions under the unfairness doctrine. However, since 2012, two respondents have fought back,[111] claiming that the unfairness doctrine should not be used in data security breach cases. Indeed it is unclear whether the unfairness doctrine should be applied at all in this context, particularly where the company that is the victim of the data security breach has engaged in no acts that could be deemed "unfair" – as that term has been interpreted by the Commission and the courts.[112]

More troublesome has been the lack of any rulemaking proceedings, policy statements or guidelines from the Commission explaining what conduct it deems "reasonable," and therefore not actionable under the unfairness doctrine, and what conduct it deems "unreasonable," and hence actionable. As stated by one lawyer:

> [T]he FTC seems to have found a heretofore unknown, federal, general obligation to maintain security for personally identifiable data.[113]

1. Data Security Breaches

A data security breach "generally refers to an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security

---

[109] Beales, *supra* note 54 (emphasis added).

[110] *See, e.g.,* Holly K. Towle, *Let's Play "Name that Security Violation!",* 11 Cyberspace Lawyer, Apr. 2006, at 11 (*also available at* http://www.klgates.com/newsstand/Detail.aspx?publication=3220 (last visited Nov. 17, 2013)).

[111] These cases are discussed in detail in Section V.A *infra*.

[112] "'Unfair' is a particularly imprecise and flexible term, so, not surprisingly, its meaning has evolved over time." Thomas B. Leary, Unfairness and the Internet, *available at* http://www.ftc.gov/speeches/leary/unfairness.shtm (last visited Nov. 17, 2013) [hereinafter "Leary Speech"].

[113] Towle, *supra* note 110.

numbers (SSN) or financial information such as credit card numbers."[114] Data security breaches can take many forms and do not necessarily lead to any consumer injury.[115]

There are a variety of activities that may give rise to data security breaches. Breaches can result from intentional actions, including hacking,[116] employee theft,[117] theft of equipment (such as laptop computers[118] and hard drives[119]), and deception or misrepresentation to obtain unauthorized data.[120] They can also arise from negligent conduct by the organization that suffered the security breach, including the loss of laptop computers or hard disks,[121] loss of data tapes,[122] unintentional exposure of data on the Internet,[123] and improper disposal of data.[124] Security breaches can

---

[114] Government Accountability Off., Personal Information: Data Breaches Are Frequent, But Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown, at 2 (GAO-07-737) (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf?source=ra (last visited Nov. 17, 2013) [hereinafter "GAO Report"]. *Personally identifiable information* "refer[s] to any information that can be used to distinguish or trade an individual's identity – such as name, Social Security number, driver's license number, and mother's maiden name. . . ." *Id.* at 2 n.2.

[115] The GAO reported that in a study of the 24 largest data security breaches reported in the media from January 2000 through June 2005, it found that only four included evidence of subsequent fraudulent activities. *Id.* at 6. The vast majority (18) showed no clear evidence of any identity theft, and the remaining two lacked sufficient information to make any determination. *Id.*

[116] In early 2007, TJX Companies reported unauthorized intrusions into its computer systems that may have led to the disclosure of credit card information and driver's license numbers on 45.7 million customers. *See, e.g.,* Dan Kaplan, *45.7 Million-Victim TJX Companies Breach Could Lead to Federal Notification Law,* SC Mag., Mar. 29, 2007, *available at* http://scmagazine.com/us/news/article/647277/457-million-victim-tjx-companies-breach-lead-federal-notification-law (last visited Nov. 17, 2013). *See also* Bell v. Acxiom Corp., 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (unpublished).

[117] *See, e.g.,* Towle, *supra* note 110.

[118] *See, e.g.,* Robert Ellis Smith, *Laptop Hall Of Shame,* Forbes.com, Sept. 7, 2006, *available at* http://www.forbes.com/columnists/2006/09/06/laptops-hall-of-shame-cx_res_0907laptops.html (last visited Nov. 17, 2013).

[119] *See, e.g.,* Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705 (S.D. Ohio 2007); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006).

[120] *See, e.g.,* Federal Trade Comm'n, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress, available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm (last visited Nov. 17, 2013).

[121] *See, e.g.,* Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007).

[122] Paul Shread, *Bank's Tape Loss Puts Spotlight on Backup Practices* (Feb. 28, 2005), *available at* http://www.enterprisestorageforum.com/continuity/news/article.php/3486036 (last visited Nov. 17, 2013).

[123] *See, e.g., Data Exposure Response* (Jan. 25, 2007), *available at* http://www.twu.edu/response/index.asp (last visited Nov. 17, 2013).

also arise from an organization's installation and use of software, which the organization reasonably believes to be secure, but which contains vulnerabilities that render it insecure.[125]

In 2005-06, the Commission filed complaints against three companies – BJ's Wholesale Club, DSW, Inc. and CardSystems Solutions, Inc. – that suffered data security breaches, and were alleged to have engaged in unfair trade practices. These three cases established the pattern for FTC data security breach cases that is still being used today Each of these cases is discussed in detail below.

2. BJ's Wholesale Club

In 2005, a wi-fi system[126] at a BJ's Wholesale Club store in Miami was used by thieves to gain access to the store's on-site computers. The wi-fi system only connected the on-site computers to inventory scanning devices, but the thieves were able to use default user IDs and passwords to download bank card information and make fraudulent purchases with BJ's customers' credit and debit cards. The resultant losses from fraudulent transactions using counterfeit credit cards allegedly totaled around $13 million.[127]

The FTC filed a complaint[128] against BJ's for an unfair act or practice due to its failure to provide "reasonable security" for its computer network, alleging that BJ's:

---

[124] *See, e.g.,* Debra Black, *Rogers Pins Data Dump on Sales Firm,* thestar.com, Apr. 9, 2007, *available at* http://www.thestar.com/article/200900 (last visited Nov. 17, 2013).

[125] *See* Michael D. Scott, *Tort Liability for the Vendors of Insecure Software: Has the Time Finally Come?,* 67 Md. L. Rev. 425 (2008), *available at* http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3320&context=mlr (last visited Nov. 20, 2013). *See also* In the Matter of HTC America Inc., Complaint, July 2, 2013, *available at* http://www.ftc.gov/os/caselist/1223049/130702htccmpt.pdf (last visited Nov. 21, 2013), where the FTC accused HTC America of making modifications to third-party software that created vulnerabilities in that software and then distributed that software to its customers.

[126] *Wi-fi* is an acronym for "wireless fidelity," which is defined as "a local area network that uses high frequency radio signals to transmit and receive data over distances of a few hundred feet, using Ethernet protocol. *See* http://www.thefreedictionary.com/wifi.

[127] Perkins Coie LLP, *Is it an Unfair Practice to Lack Adequate Security for Consumer Information?,* July 5, 2005, *available at* http://www.perkinscoie.com/news/pubs_detail.aspx?publication=735&op=updates (last visited Nov. 17, 2013).

[128] *See In the Matter of* BJ's Wholesale Club, Inc., Docket No. C-4148, Complaint, Sept. 20, 2005, *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf (last visited Nov. 17, 2013).

> 1. did not encrypt the information while in transit or when stored on the in-store computer networks;
> 2. stored the information in files that could be accessed anonymously -- that is, using a commonly known default user id and password;
> 3. did not use readily available security measures to limit access to its computer networks through wireless access points on the networks;
> 4. failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and
> 5. created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, and in violation of bank rules.[129]
>
> As a result, a hacker could have used the wireless access points on an in-store computer network to connect to the network and, without authorization, access personal information on the network.[130]

The question of whether any or all of the acts alleged in the complaint constituted "unfair acts or practices" was never adjudicated. BJ's immediately capitulated and agreed to a consent order. Under that order, which lasts for 20 years, BJ's must:

> • designate "an employee or employees to coordinate and be accountable for the information security program";
> • identify "material internal and external risks to security" including risks in "employee training and management, information systems . . ., and . . . response to . . . system failures";
> • design and implement "reasonable safeguards to control risks identified through risk assessment and regular testing"; and
> • adjust the information security system to the results of the assessments and changes in the company's operations.[131]

---

[129] *Id.* ¶ 7.

[130] *Id.*

[131] *In re* BJ's Wholesale Club, Docket No. C-4148, Decision and Order § I, *available at* http://www.ftc.gov/os/caselist/0423160/092305d00423160.pdf (last visited Nov. 17, 2013).

BJ's must also obtain a biennial assessment and report from a qualified, objective, independent, certified third-party professional concerning BJ's compliance with the Order.[132]

As one commentator noted, "[t]he agency will likely consider the terms of the BJ's settlement (which last for 20 years) as the standard that all companies that obtain and store consumer financial information must meet."[133]

3. DSW, Inc.

On December 1, 2005, the FTC announced[134] that it had entered into a settlement and consent judgment[135] with retail shoe discounter DSW, Inc. The agency claimed that DSW's "failure to take reasonable security measures to protect sensitive customer data was an unfair practice that violated federal law."[136]

According to the FTC's complaint,[137] DSW used computer networks to obtain authorization for credit card, debit card, and check purchases at its stores and to track inventory. For credit and debit card purchases, DSW collected information, such as name, card number, and expiration date, from the magnetic stripe on the back of the cards. The magnetic stripe information also contained a security code that could be used to create counterfeit cards that would appear to be genuine in the authorization process.[138] For check purchases, DSW collected information such as routing number, account number, check number, and the consumer's driver's license number and state.[139] According to the complaint, DSW's data security failures allowed hackers to gain access to information on more than 1.4 million customers.[140]

The FTC alleged that DSW:

---

[132] *Id.* § II.

[133] Perkins Coie LLP, *supra* note 127.

[134] Federal Trade Comm'n, *DSW Inc. Settles FTC Charges* (Dec. 1, 2005), *available at* http://www.ftc.gov/opa/2005/12/dsw.shtm (last visited Nov. 17, 2013).

[135] *See In re* DSW, Inc., Docket No. C-4157, Decision and Order, *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSCDecisionandOrder.pdf (last visited Nov. 17, 2013).

[136] *Id.*

[137] *In re* DSW, Inc., Docket No. C-4157, Complaint (Dec. 1, 2005), *available at* http://www.ftc.gov/os/caselist/0523096/051201comp0523096.pdf (last visited Nov. 17, 2013).

[138] *Id.* ¶ 5.

[139] *Id.*

[140] *Id.* ¶ 9.

> 1. Created unnecessary risks to sensitive information by storing it in multiple files when it no longer had a business need to keep the information;
> 2. Failed to use readily available security measures to limit access to its computer networks through wireless access points on the networks;
> 3. Stored the information in unencrypted files that could be easily accessed using a commonly known user ID and password;
> 4. Failed to limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and
> 5. Failed to employ sufficient measures to detect unauthorized access.[141]

As in the *BJ's Wholesale Club* case, the question of whether any of these acts constituted "unfair acts or practices" under Section 5 was never adjudicated, since DSW immediately settled. Under the Order, which lasts for 20 years, DSW must:

> • "Designate an employee or employees to coordinate and be accountable for the information security program";
> • "Identify material internal and external risks to security, confidentiality, and integrity of consumer information that could result in unauthorized disclosure, misuse, loss, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks";
> • "Design and implement reasonable safeguards to control risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems and procedures"; and
> • "Evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, and any other circumstances that DSW knows or has reason to know may have a material impact on the effectiveness of its information security program."[142]

DSW must also obtain a biennial assessment and report from a qualified, objective, independent, certified, third-party professional concerning DSW's compliance with the Order.[143]

---

[141] *Id.* ¶ 7.
[142] *In re* DSW, Inc., Decision and Order, *supra* note 135, at § I.
[143] *Id.* § II.

Interestingly, in commenting on the *DSW* decision, the Commission indicated that it might use its enforcement discretion under Section 5 of the FTC Act to go beyond the substantive requirements of the Safeguards Rule under the Gramm-Leach-Bliley Act, and protect personal consumer information even where the information is public.[144]

4. CardSystems Solutions, Inc.

Unlike BJ's Wholesale Club and DSW, CardSystems Solutions, Inc. (CSS) is not a retailer. According to the complaint,[145] CSS provides merchants with products and services used in "authorized processing" of credit and debit card purchases from the banks that issue the cards. CSS uses the Internet and web-based software applications to provide information to client merchants about authorizations it has performed for them.

CSS collects information from a customer's credit or debit card magnetic stripe, including, but not limited to, the customer name, card number and expiration date, a security code used to verify electronically that the card is genuine, and certain other information; formats and transmits the information to a computer network operated by or for a bank association (such as Visa or MasterCard) or another entity (such as American Express), which then transmits it to the issuing bank. The issuing bank receives the request, approves or declines the purchase, and transmits its response to the merchant over the same computer networks used to process the request. The response includes the personal information that was included in the authorization request the issuing bank received.

According to the complaint DSS "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information stored on its computer network,"[146] including:

> 1. Created unnecessary risks to the customers' information by storing it in a vulnerable format for up to 30 days;
> 2. Did not adequately assess the vulnerability of its web application and computer network to commonly known or

[144] Letter to Bank of America Corp., in *In re* DSW, Inc., (Mar. 7, 2005), *available at* http://www.ftc.gov/os/caselist/0523096/0523096DSWLettertoCommenterBankofAmerica.pdf (last visited Nov. 17, 2013).

[145] *In re* CardSystems Solutions, Inc., Docket No. C-4168, Complaint (Sept. 8, 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf (last visited Nov. 17, 2013).

[146] *Id.* ¶ 6.

> reasonably foreseeable attacks, including but not limited to "Structured Query Language" (or "SQL") injection attacks;
> 3. Did not implement simple, low-cost, and readily available defenses to such attacks;
> 4. Failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network;
> 5. Did not use readily available security measures to limit access between computers on its network and between such computers and the Internet; and
> 6. Failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.[147]

According to the complaint, a hacker exploited these "failures" and installed software on CSS's computer network that allowed him to collect and transmit magnetic stripe data stored on CSS's network to computers located outside the network.[148] This information was then used to manufacture counterfeit cards that were used to make fraudulent purchases.[149]

As in the two prior cases, the question of whether any of these acts constituted "unfair acts or practices" under Section 5 was never adjudicated, since CSS immediately agreed to settle. Under the Order, which lasts for 20 years, CSS must:

> • Designate "an employee or employees to coordinate and be accountable for the information security program";
> • Identify "material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information," and assess "the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures."

---

[147] *Id.*
[148] *Id.* ¶ 7.
[149] *Id.* ¶ 8.

> • "[D]esign and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures."
> • "[E]valuation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by [this order], any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program."[150]

As in the two previous cases, CSS must also obtain a biennial assessment and report from a qualified, objective, independent, certified, third-party professional concerning DSW's compliance with the Order.[151]

D. Applying the Unfairness Doctrine to Data Security Breaches

While the courts and Congress have given the Commission broad authority to take action against unfair practices, "[t]he Commission is hardly free to write its own law of consumer protection. . . ."[152] The Commission's exercise of its unfairness authority in any particular instance is subject to judicial review and may be affirmed or set aside by the court.[153]

In analyzing whether the Commission has properly applied the unfairness doctrine in any particular situation, it is important to look at the requirements set forth in the 1980 *Unfairness Statement:*

> 1. whether the practice injures consumers; and
> 2. whether it violates established public policy.[154]

The following analysis applies these requirements to the unfairness claims made by the FTC in the three data security breach cases discussed above.

---

[150] *In re* CardSystems Solutions, Inc., Docket No. C-4168, Decision and Order § I (Sept. 8, 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148CardSystemsdo.pdf (last visited Nov. 17, 2013).

[151] *Id.* § II.

[152] National Petroleum Refiners Ass'n v. Federal Trade Comm'n, 482 F.2d 672, 693 (D.C. Cir. 1973).

[153] *See Sperry & Hutchinson,* 405 U.S. at 249; Federal Trade Comm'n v. R.F. Keppel & Bro., 291 U.S. 304, 314 (1934).

[154] *See* notes 77-78 *supra* and accompanying text.

1. Injury to Consumers

Unjustified consumer injury from a party's conduct is the primary and most important factor in an unfairness analysis.[155] Indeed, if the injury to consumers is significant enough, it can be the *sole* basis for a finding of unfairness.[156]

However, not every consumer injury is actionable. To justify a finding of unfairness, a consumer injury must satisfy three requirements: (1) the injury must be substantial; (2) it must not be outweighed by any offsetting benefits to consumers or competition; and (3) the injury must be one that consumers could not reasonably have avoided.[157]

a. Substantial Injury

First, the injury must be "substantial."[158] "Substantial injury is an objective test."[159] As noted by the Commission:

> [T]he Commission believes that considerable attention should be devoted to the analysis of whether substantial net harm has occurred, not only because that is part of the unfairness test, but also because the focus on injury is the best way to ensure that the Commission acts responsibly and uses its resources wisely.[160]

The most common form of injury suffered by consumers is monetary harm.[161] A small degree of harm to a large number of consumers may be deemed "substantial," as may a significant amount of harm to each consumer.[162] Emotional harm, "other more subjective types of harm," and "trivial or merely speculative harms" generally would not be considered "substantial."[163]

Interestingly, in none of the FTC complaints filed to date has the Commission claimed that consumers suffered any

---

[155] "Unjustified consumer injury is the primary focus of the FTC Act." *Unfairness Statement,* 104 F.T.C. at 1073.

[156] *Id.*

[157] *Id. See also* 15 U.S.C. § 45(n).

[158] *Id.*

[159] Beales, *supra* note 54.

[160] *Id.*

[161] Unfairness Statement, 104 F.T.C. at 1073. However, in some situations (not presented to date in the case of data security breaches), the consumer injury may be unnecessary health or safety risks. *Id.*

[162] *Id.* n.12.

[163] *Id.*

monetary losses *at all.* In the *BJ's Wholesale Club* complaint, for example, the only allegation relating to injury was the following:

> Beginning in late 2003 and early 2004, banks began discovering fraudulent purchases that were made using counterfeit copies of credit and debit cards the banks had issued to customers. The customers had used their cards at respondent's stores before the fraudulent purchases were made, and personal information respondent obtained from their cards was stored on respondent's computer networks. This same information was contained on counterfeit copies of cards that were used to make several million dollars in fraudulent purchases. In response, banks and their customers cancelled and re-issued thousands of credit and debit cards that had been used at respondent's stores, and customers holding these cards were unable to use their cards to access credit and their own bank accounts.[164]

Similarly, in *In re DSW, Inc.,* the only allegation of consumer injury in the complaint stated:

> To date, there have been fraudulent charges on some of these accounts. Further, some customers whose checking account information was compromised were advised to close their accounts, thereby losing access to those accounts, and having incurred out-of-pocket expenses such as the cost of ordering new checks. Some of these checking account customers have contacted DSW requesting reimbursement of their out-of-pocket expenses, and DSW has provided some amount of reimbursement to these customers.[165]

---

[164] *See BJ's Wholesale Complaint* ¶ 8, *supra* note 125. In paragraph 9, the Commission alleged conclusorily that:

> As described in Paragraphs 7 and 8 above, respondent's failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice.

Id. ¶9.

[165] *In re* DSW, Inc., Complaint ¶ 9, *supra* note 137. As in the *BJ's Wholesale Club* complaint (*see* note 63 *supra*), there was only a conclusory allegation of consumer injury in the *DSW* complaint:

> [R]espondent's failure to provide reasonable and appropriate security measures to protect personal information and files caused or is likely to

And in *In re* CardSystems Solutions, Inc., the sole allegation of consumer injury stated:

> In early 2005, issuing banks began discovering several million dollars in fraudulent credit and debit card purchases that had been made with counterfeit cards. The counterfeit cards contained complete and accurate magnetic stripe data, including the security code used to verify that a card is genuine, and thus appeared genuine in the authorization process. The magnetic stripe data matched the information respondent had stored on its computer network. In response, issuing banks cancelled and re-issued thousands of credit and debit cards. Consumers holding these cards were unable to use them to access their credit and bank accounts until they received replacement cards.[166]

Federal law limits consumers' liability for unauthorized credit card charges to $50 per card as long as the credit card company is notified within 60 days of the unauthorized charge.[167] Many credit card companies do not require consumers to pay the $50 and will not hold consumers liable for the unauthorized charges, no matter how much time has elapsed since the discovery of the loss.[168] As such, it is probable that the consumers affected by these security breaches suffered no monetary loss at all.[169]

> cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was and is an unfair act or practice.

Id. ¶10.

[166] *In re* CardSystems Solutions, Inc., Complaint ¶ 8, *supra* note 142. As in the prior two complaints, the CSS complaint contained only a single, general allegation of consumer injury:

> As set forth in Paragraphs 6, 7, and 8, respondent's failure to employ reasonable and appropriate security measures to protect personal information it stored caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

Id. ¶9.

[167] *See* 12 C.F.R. § 226.12(b).

[168] *See* Prepared Statement of the Federal Trade Comm'n before the Subcomm. on Terrorism, Technology, and Homeland Security, Senate Comm. on the Judiciary, Identity Theft: Innovative Solutions for an Evolving Problem, at 3 n.3 (Mar. 21, 2007) (presented by Lydia Parnes, Dir. of the FTC Bureau of Consumer Protection), *available at* http://judiciary.senate.gov/pdf/3-21-

There has been only one reported decision[170] in a case brought by a consumer against any of the three entities discussed above in which consumer injury was discussed. In *Key v. DSW, Inc.*,[171] the plaintiff filed a class action suit against DSW for negligence, breach of contract, conversion and breach of fiduciary duty. She claimed that as a result of DSW's failure to secure the personal financial information of its customers (including the plaintiff), "unauthorized persons obtained access to and acquired the information of approximately 96,000 customers."[172] She alleged that as a consequence of DSW's actions she and the class members were subjected to "a substantially increased risk of identity theft, and have incurred the cost and inconvenience of, among other things, canceling credit cards, closing checking accounts, ordering new checks, obtaining credit reports and purchasing identity and/or credit monitoring."[173] The court dismissed the complaint on the ground that the plaintiff lacked standing to sue since she had identified *no actual injury* suffered as a result of DSW's conduct.

07Parnestestimony.pdf (last visited Nov. 17, 2013) [hereinafter "Parnes Testimony"]. *See also* ACOAS, *supra* note 93, Statement of Stewart Baker ("The Committee did not hear any evidence that consumers had actually suffered significant losses from exposure of their personal data on the Internet (it appears that losses from the well-publicized hacker thefts of credit card information fell mainly or exclusively on merchants and banks)"), *available at* http://www.ftc.gov/acoas/papers/individual_statements.pdf (last visited Nov. 17, 2013).

[169] Parnes Testimony, *supra* note 167, at 3 ("Of course, not all data breaches lead to identity theft; in fact, many prove harmless or are caught and addressed before any harm occurs"). *See also* Fred H. Cate, *Information Security Breaches and the Threat to Consumers,* 60 Consumer Fin. L.Q. Rep. 344, 346 (2006) ("Information security breaches are among the least common ways that personal information falls into the wrong hands").

[170] A second case, *Parke v. CardSystems Solutions, Inc.,* 2006 WL 2917604 (N.D. Cal. Oct. 11, 2006), contains allegations similar to the *Key* case against CSS and others, but did not address the issue of consumer injury. In *Richardson v. DSW, Inc.,* 2005 WL 2978755 (N.D. Ill. Nov. 3, 2005), the court dismissed the plaintiff's claim based on the Illinois Consumer Fraud Act because the state law requires that the conduct be intentional. The decision did not address the consumer injury issue, but held that there might be an implied contract upon which recovery could be founded obviating a motion to dismiss); and in the subsequent decision in *Richardson v. DSW, Inc.,* 2006 WL 163167 (Jan. 18, 2006), the court allowed the plaintiff to amend her complaint to allege a violation of the Illinois Consumer Fraud and Deceptive Practices Act based on an alleged breach of contract between DSW and the credit card issuers. Consumer injury was not discussed in that opinion either.

[171] 454 F. Supp. 2d 684 (S.D. Ohio 2006).

[172] *Id.* at 686.

[173] *Id.*

> In the identity theft context, courts have embraced the general rule that an alleged increase in risk of future injury is not an "actual or imminent injury." Consequently, courts have held that plaintiffs do not have standing, or have granted summary judgment for failure to establish damages in cases involving identity theft or claims of negligence and breach of confidentiality brought in response to a third party theft or unlawful access to financial information from a financial institution.
>
> * * *
>
> In sum, Plaintiff's claims are based on nothing more than a speculation that she will be a victim of wrongdoing at some unidentified point in the indefinite future. Because plaintiff has failed to allege that she suffered injury-in-fact that was either "actual or imminent," this Court is precluded from finding that she has standing under Article III.[174]

Other cases brought by consumers for data security breaches also have been dismissed for a failure to show any actual injury to the plaintiff-consumer.[175]

This is consistent with the findings of a report from the Government Accounting Office.[176] In that report, the GAO examined two-dozen highly publicized incidents involving breaches of sensitive personal information and the extent to which such breaches resulted in actual damages to consumers. The report concluded that:

> The extent to which data breaches have resulted in identity theft is not well known, largely because of the difficulty of determining the source of the data used to commit identity theft. However, available data and interviews with researchers, law enforcement officials, and industry representatives indicated that *most breaches have not resulted in detected incidents of identity theft,* particularly

---

[174] *Id.* at 689, 690.

[175] *Accord* Pisciotta v. Old National Bancorp., 2007 WL 2389770 (7th Cir. Aug. 23, 2007); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 7-8 (D.D.C. 2007); Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705, 712-13 (S.D. Ohio 2007); Bell v. Acxiom Corp., 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) (unpublished); Giordano v. Wachovia Securities LLC, 2006 WL 2177036, at *4 (D.N.J. July 31, 2006); Walters v. DHL Express, 2006 WL 1314132 at *5 (C.D. Ill. May 12, 2006); Forbes v. Wells Fargo Bank N.A., 420 F.Supp.2d 1018, 1021 (D. Minn. 2006); Guin v. Brazos Higher Educ. Serv. Corp., 2006 WL 288483, at *5-*6 (D. Minn. Feb. 7, 2006); Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906, at *3 (D. Ariz. Sept. 6, 2005).

[176] *See* GAO Report, *supra* note 110.

> the unauthorized creation of new accounts. For example, in reviewing the 24 largest breaches reported in the media from January 2000 through June 2005, GAO found that 3 included evidence of resulting fraud on existing accounts and 1 included evidence of unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, there was not sufficient information to make a determination.[177]

The President's Identity Theft Task Force reached the same conclusion.[178]

In a speech in early 2007, FTC Chairman Majoras responded to criticism that the cases discussed above did not establish any consumer injury:

> What is the substantial injury to American consumers? First, millions of dollars of fraudulent purchases were made using personal information obtained from the companies' computer networks. Some customers may end up liable for some of these fraudulent purchases, particularly if they failed to spot fraudulent purchases on their statements in a timely manner. In addition, some customers experienced substantial injury in the form of inconvenience and time spent dealing with the blocking and re-issuance of their credit and debit cards.[179]

---

[177] *Id.* (emphasis added.) While the security breach cases evaluated by the GAO predated the three cases discussed in the article, the conclusion reached by the report, namely, that few data security breach cases actually result in measurable injury to consumers, is still relevant to this discussion. *See also* Statement of Fred H. Cate, Director of the Center for Applied Cybersecurity Research, Indiana University in Bloomington: "The threat of identity theft from data losses is being greatly exaggerated, and that's because a lot of people have fallen into the trap of equating data loss with identity theft." *Quoted in* Steve Lohr, *Surging Losses, but Few Victims in Data Breaches,* N.Y. Times, Sept. 27, 2006, *available at* http://www.nytimes.com/2006/09/27/technology/circuits/27lost.html?ex=1317009600&en=32a16386036e9009&ei=5088&partner=rssnyt&emc=rss (last visited Nov. 17, 2013).

[178] *See* President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan 2, 3 (Apr. 2007) ("The loss of theft of personal information by itself, however, does not immediately lead to identity theft. . . . [D]uring the past year, the personal records of 73 million people have been lost or stolen, but there is no evidence of a surge in identity theft or financial fraud as a result"), *available at* http://www.identitytheft.gov/reports/StrategicPlan.pdf (last visited Nov. 17, 2013) [hereinafter "Task Force Report"].

[179] Marjoras Remarks, *infra* note 231, at 8.

Yet, none of these "injuries" constitute "substantial consumer injury" as required by the unfairness doctrine. As noted above,[180] it is likely that consumers bore none of the cost of the asserted fraudulent transactions. Further, the fact that some consumers "may" have been liable "if" they failed to report the fraudulent purchases is pure speculation, which is also not actionable under the unfairness doctrine.[181] Finally, the "inconvenience or time" customers may have spent in obtaining replacement credit/debit cards are not monetary damages either.[182] Even after the FTC has had ample opportunity to thoroughly investigate these data breaches in detail, the Commission cannot point to *any* consumer injury cognizable under the unfairness doctrine.

The difficulty of establishing substantial consumer injury when applying the unfairness doctrine to online privacy violations was highlighted in an earlier FTC enforcement action that did not involve a data security breach. In *Federal Trade Commission v. ReverseAuction.com, Inc.,*[183] the complaint alleged that the respondent, an online auction provider, became a member of eBay and was thereby granted access to the e-mail addresses, eBay user IDs, and feedback ratings of other eBay members. When registering as a member, respondent agreed to abide by eBay's privacy agreement, which prohibited members from using the personal identifying information of any eBay member obtained through eBay's web site to send unsolicited commercial e-mail.

The Commission alleged that respondent violated Section 5 by using other eBay members' user IDs, feedback ratings, and e-mail addresses for the purpose of sending those members unsolicited commercial e-mail, in contravention of its agreement with eBay. The complaint pled in the alternative that ReverseAuction engaged in deception by falsely representing to eBay that it would abide by the privacy agreement,[184] or that ReverseAuction's use of the eBay member information for the purposes of sending unsolicited commercial e-mail was an unfair practice.[185]

All of the commissioners voted to support the deception claim, but two of the commissioners voted against the unfairness

[180] *See* notes 164-66 *supra* and accompanying text..

[181] *See* note 160 *supra*.

[182] *See* notes 170-71 *supra* and accompanying text.

[183] Complaint (D.D.C. Jan. 6, 2000), *available at* http://www.ftc.gov/os/2000/01/reversecmp.htm (last visited Nov. 17, 2013).

[184] *Id.* ¶ 16.

[185] *Id.* ¶ 17.

claim.[186] Commissioners Swindle and Leary dissented from the Commission's decision on the ground that there was no proof of substantial consumer injury as a result of the respondents' activities.

> The Commission has no authority to declare an act or practice unfair unless it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (emphasis added). The statutory requirement of substantial injury is actually derived from the Commission's own Statement of Policy, issued in 1980. The Commission explained at that time that, "[t]he Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm . . . Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair." Letter from the Commission to the Consumer Subcommittee of the Senate Committee on Commerce, Science, and Transportation, *Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction,* 4 Trade Reg. Rep. (CCH) ¶ 13,203 (Dec. 17, 1980), *reprinted in* International Harvester, Inc., 104 F.T.C. 949, 1070-76 (1984).
>
> We do not say that privacy concerns can never support an unfairness claim. In this case, however, ReverseAuction's use of eBay members' information to send them e-mail did not cause substantial enough injury to meet the statutory standard.[187]

The dissenting Commissioners further explained their position on the unfairness claim:

> The injury in this case was caused by deception: that is, by ReverseAuction's failure to honor its express commitments. It is not necessary or appropriate to plead a less precise theory.

---

[186] *See* Statement of Commissioners Orson Swindle and Thomas B. Leary Concurring in Part and Dissenting in Part, in *ReverseAuction.com, Inc.,* File No. 0023046, *available at* http://www.ftc.gov/os/2000/01/reversesl.htm (last visited Nov. 17, 2013).

[187] *Id.*

> Industry self-regulation and consumer preferences, as expressed in the marketplace, are the best and most efficient ways to formulate privacy arrangements on the Internet and in commerce generally. Because proliferation of the kind of deceptive conduct in which ReverseAuction allegedly engaged could undermine consumer confidence in such privacy arrangements, we believe that it is appropriate to pursue this matter under a deception theory. The unfairness theory, however, posits substantial injury stemming from ReverseAuction's use of information readily available to millions of eBay members to send commercial e-mail. *This standard for substantial injury overstates the appropriate level of government-enforced privacy protection on the Internet, and provides no rationale for when unsolicited commercial e-mail is unfair and when it is not. We are troubled by the possibility of an expansive and unwarranted use of the unfairness doctrine.*[188]

The same concern applies to unfairness claims based upon data security breaches. Without any rules or guidelines, applying the unfairness doctrine to data security breaches offers the possibility of "an expansive and unwarranted use of the unfairness doctrine."

b. Cost-Benefit Analysis

The second requirement for an unfairness finding is that the injury must "not be outweighed by any offsetting consumer or competitive benefits. . . ."[189] The Commission will consider the cost-benefit trade-offs of the practice, and will not find a practice unfair "unless it is injurious in its net effects."[190] The agency will also take into account the cost to remedy the alleged injury to the parties involved, as well as "the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters."[191]

There is no question that there is a potential cost, and in some cases a substantial cost, in a company not properly

---

[188] *Id.* (emphasis added).

[189] Unfairness Statement, 104 F.T.C. at 1073. *See also* 15 U.S.C. § 45(n).

[190] Unfairness Statement, 104 F.T.C. at 1073. "When making this determination the Commission may refer to existing public policies for help in ascertaining the existence of consumer injury and the relative weights that should be assigned to various costs and benefits." *Id.* n.17.

[191] *Id.* at 1073-74.

protecting consumers' personal information from unauthorized access or disclosure. However, there is also a cost, and in many cases an enormous cost, in providing a high level of protection for that information.[192] To properly assess the "cost-benefit trade-offs" in this area, some attempt must be made to quantify the cost of increasing the protection of consumers' data above a certain threshold level.

It is clearly unreasonable for an entity to gather sensitive consumer information and invest no money in implementing security techniques to safeguard that information. It is also clear that there is no such thing as absolute security – no matter how much money is spent. Computer systems simply cannot be made 100% secure.[193] That is a fact of life, and is something the Commission itself has recognized:

> For example, perfect security, if it existed, would come at such a high cost that the failure to have perfect security would not violate the Commission's unfairness standard. . . .[194]

So, given the two extremes – no security being unacceptable and absolute security being unattainable, how is an entity to conduct the cost-benefit analysis of how much security is "enough" to avoid being deemed "unfair" by the Commission, and at what cost? A cost-benefit analysis depends invariably "on subjective valuations which may vary from person to person, as well as across sociological or income groups."[195] Without formal hearings and rulemaking, it is impossible for the FTC, or a court, to make that determination.

---

[192] *See* ACOAS, *supra* note 93, at 23 ("Security – and the resulting protection for personal data – can be set at almost any level depending on the costs one is willing to incur, not only in dollars but in inconvenience for users and administrators of the system.").

[193] *See* Statement of the Federal Trade Commission Before the House Subcomm. on Technology, Information Policy, Intergovernmental Relations, and the Census, Comm. on Government Reform (Apr. 21, 2004) at 4 ("The Commission recognized that there is no such thing as 'perfect' security and that breaches can occur even when a company has taken all reasonable precaution."), *available at* http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf (last visited Nov. 17, 2013) [hereinafter "FTC Statement"]. *See also* Deborah Platt Majoras, *The Federal Trade Commission: Learning from History as We Confront Today's Consumer Challenges,* 75 UMKC L. Rev. 115, 128 (2006) ("The laws and rules we enforce do not require that information security be perfect. Such a standard would be costly and unobtainable.").

[194] Majoras Remarks, *infra* note 236, at 9.

[195] Richard Craswell, *The Identification of Unfair Acts and Practices by the Federal Trade Commission,* 1981 Wisc. L. Rev. 107, 138.

As noted by FTC Commissioner Swindle, in dissenting from the 2000 FTC Privacy Report:

> [T]he Privacy Report fails to pose and to answer basic questions that all regulators and lawmakers should consider before embarking on extensive regulation that could severely stifle the New Economy. *Shockingly, there is absolutely no consideration of the costs and benefits of regulation; nor the effects on competition and consumer choice;* nor the experience to date with government regulation of privacy; nor constitutional implications and concerns; nor how this vague and vast mandate will be enforced.[196]

To date the Commission has conducted no cost-benefit analysis of the economic impact of its application of the unfairness doctrine to data security breaches, or if it has, it has not disclosed the result of that analysis to the public.

c. Consumers' Ability to Avoid Injury

The third element of the test is whether the consumer could have reasonably avoided the injury.[197] "If consumers could have made a different choice, but did not, the Commission should respect that choice."[198] However, where the harm is not one that the consumer could have avoided by choosing not to engage in trade with the vendor, the agency may take action to halt behavior "that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[199]

While it is possible that a consumer could live a reasonably full and productive life without using a credit or debit card or personal check (i.e., would conduct all of her transactions with cash only), and would, therefore, have a significantly lower chance of suffering injury as a result of a data security breach, it is likely that the FTC would consider such an alternative "unreasonable." Further, while the three cases discussed above all involved credit/debit cards and checks, other instances of data security breaches have involved other forms of financial transactions, such

---

[196] Swindle Dissent, *supra* note 1, at 16.

[197] Unfairness Statement, 104 F.T.C. at 1074. *See also* 15 U.S.C. § 45(n).

[198] Beales, *supra* note 54.

[199] Unfairness Statement, 104 F.T.C. at 1074. However, the examples given by the Commission—coercion, unduly influencing susceptible consumers, and not making available important price or performance information—are not in any way analogous to conduct by a company that results in a data security breach.

as student loans,[200] bank accounts,[201] and other types of financial,[202] as well as health insurance[203] transactions.

Further, in the *BJ's Wholesale Club* and *DSW* cases, "customers could not know that their personal information was vulnerable on respondents' computer networks, and thus had no reason to avoid using their credit and debit cards at these stores. Further, after providing their information to BJ's or DSW, customers could not prevent the breach from occurring. . . . And in the case of payment processor CardSystems, consumers did not even know that CardSystems processed their transactions, let alone that it stored their personal information on its computer network, or left their information vulnerable."[204]

It is likely that the Commission or a court hearing a case involving an allegation of unfairness under the circumstances presented in these cases would find that the consumer did not have the ability to avoid injury, and hence that this prong of the consumer injury analysis had been met.

2. Violation of an Established Public Policy

The second factor in an unfairness analysis is whether the practice violates a public policy "as it has been established by statute, common law, industry practice, or otherwise."[205] In its *Unfairness Statement,* the Commission observed that, "[a]lthough public policy" has been listed "as a separate consideration, it is used most frequently by the Commission as a means of providing additional evidence on the degree of consumer injury caused by specific practices."[206]

However, it may be an independent basis for a finding of unfairness when "the policy is so clear that it will entirely determine the question of consumer injury, so there is little need for a separate analysis by the Commission."[207]

The agency will use public policy to support a finding of unfairness when the policy has been formally acknowledged in laws and judicial decisions and widely recognized by legislatures and courts. If a public policy is not well-established, the agency

---

[200] Guin v. Brazos Higher Educ. Serv. Corp., 2006 WL 288483 (D. Minn. Feb. 7, 2006)

[201] Forbes v. Wells Fargo Bank N.A., 420 F.Supp.2d 1018 (D. Minn. 2006)

[202] *See, e.g.,* Giordano v. Wachovia Securities LLC, 2006 WL 2177036 (D.N.J. July 31, 2006) (personal information relating to a retirement account).

[203] Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005).

[204] Marjoras Remarks, *infra* note 231, at 10.

[205] Unfairness Statement, 104 F.T.C. at 1074.

[206] *Id.* at 1075.

[207] *Id.*

will "act only on the basis of convincing independent evidence that the practice was distorting the operation of the market and thereby causing unjustified consumer injury."[208]

In 1982, the Commission further limited the role of public policy, stating that it was not an independent basis for unfairness,[209] but rather it "may provide additional evidence" of unfairness.[210]

Congress subsequently codified this reduced role in 1994.[211]

> Under the statutory standard, the Commission may consider public policies, but it cannot use public policy as an independent basis for finding unfairness. The Commission's long and dangerous flirtation with ill-defined public policy as a basis for independent action was over.[212]

The question here is whether the Commission is applying a *clearly established* public policy in the data security breach cases. For a policy to be clearly established, "it must be widely-followed, and embodied in statutes, judicial decisions or the Constitution."[213]

Since 2000, Congress has authorized the Commission to hold hearings and to promulgate rules under several statutes,

---

[208] *Id.* at 1076.

[209] 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 568-70.

[210] *Id.* The reduced role of public policy was reflected in the Commission's Credit Practices Rule adopted by the Commission in 1984.

> Earlier articulations of the consumer unfairness doctrine have also focused on whether "public policy" condemned the practice in question. In its December 1980 statement, the Commission stated that it relies on public policy to help it assess whether a particular form of conduct does in fact tend to harm consumers. We have thus considered established public policy "as a means of providing additional evidence on the degree of consumer injury caused by specific practices."

Credit Practices Rule, Statement of Basis and Purpose and Regulatory Analysis, 49 Fed. Reg. 7740, 7743 (Mar. 1, 1984).

[211] Federal Trade Commission Act Amendments of 1994 (H.R. 2243), *codified at* 15 U.S.C. §45(n). *See* quote accompanying note 77 *supra*.

[212] Beales, *supra* note 54.

[213] Chris Jay Hoofnagle, *Privacy Practices Below the Lowest Common Denominator: The Federal Trade Commission's Initial Application of Unfair and Deceptive Trade Practices Authority to Protect Consumer Privacy (1997-2000)*, at 2-3, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=507582 (last visited Nov. 17, 2013).

including Title V of the Gramm-Leach-Bliley Financial Services Modernization Act,[214] the Fair Credit Reporting Act,[215] and the Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act of 2002.[216]

Some commentators have suggested[217] that the unfairness complaints filed by the Commission for data security breaches are actually being brought pursuant to the Safeguards Rule[218] the Commission promulgated under the authority granted to it in the GLB.[219] The Safeguards Rule requires financial institutions to have reasonable policies and procedures to ensure the security, confidentiality and integrity of customer information.[220] The *financial institutions* covered by the Rule include not only lenders and other traditional financial institutions, but also companies providing other types of financial products and services to consumers.[221] These institutions include, for example, payday lenders, check-cashing businesses, professional tax preparers, auto dealers engaged in financing or leasing, electronic funds transfer networks, mortgage brokers, credit counselors, real estate settlement companies, and retailers that issue credit cards to consumers.[222]

The Rule is intended to be flexible to accommodate the wide range of entities covered by GLB, as well as the wide range of circumstances companies face in securing customer information. Accordingly, the Rule requires financial institutions to implement a written information security program that is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.[223] Each financial institution must also: (1) assign one or more employees to oversee the program; (2) conduct a risk

---

[214] 15 U.S.C. §§ 6801 *et seq*. [hereinafter "GLB"].

[215] *Id.* §§ 1681 *et seq*.

[216] Pub. L. 107-204, 116 Stat. 745 (2002).

[217] *See* FTC Statement, *supra* note 189, at 5. *See also* note 264 *infra* and accompanying text.

[218] Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314 (May 23, 2002). *See also* Commission's Privacy of Consumer Financial Information Rule ("Privacy Rule"), 16 C.F.R. Part 313 (May 24, 2000).

[219] The Safeguards Rule, implementing Section 501(b) of the GLB (15 U.S.C. § 6801(b)), was promulgated by the Commission on May 23, 2002, and became effective on May 23, 2003.

[220] 16 C.F.R. Part 314.1(a).

[221] 15 U.S.C. § 6809(3)(A). *Financial institutions* are defined as businesses that are engaged in certain "financial activities" described in Section 4(d) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843(k)) and its accompanying regulations. 12 C.F.R. §§ 225.28, 225.86.

[222] 15 U.S.C. § 6809.

[223] 16 C.F.R. § 314.3.

assessment; (3) put safeguards in place to control the risks identified in the assessment and regularly test and monitor them; (4) require service providers, by written contract, to protect customers' personal information; and (5) periodically update its security program.[224]

However, the GLB is limited to financial institutions, and does not, by its very language, apply to retailers like BJ's Wholesale Club and DSW, or to credit card processing services like CardSystems. As such, the GLB and the Safeguards Rule should not be deemed to be the "clearly established public policy" on which the FTC can base its unfairness actions against entities that do not come within the carefully delineated definition of "financial institutions." If the GLB or other industry-specific laws are to be extended to cover entities not currently within their limited purview, it is up to Congress to make that determination, not the FTC.[225]

There simply was no established public policy in existence at the time of the filing of these first three complaints that the Commission could have relied upon to justify its actions. As noted by one commentator:

> To suddenly create and enforce a list in hindsight, as the FTC apparently did, is to govern more by the concept of "shock and awe" than by publicly considered and published public policy.[226]

E. The FTC Has Provided No Meaningful Guidance on What It Considers Unfair in the Data Security Breach Context

Before the Commission filed its first unfairness action against BJ's Wholesale Club, it had issued no policy statements, conducted no rulemaking,[227] and made no pronouncements that it

---

[224] *Id.* § 314.4.

[225] "Although we believe that Section 5 already requires companies holding sensitive data to have in place procedures to secure it if the failure to do so is likely to cause substantial consumer injury, we believe Congress should consider whether new legislation incorporating the flexible standard of the Commission's Safeguards Rule is appropriate." FTC Statement Before the Senate Comm. on Commerce, Science & Transportation on Data Breaches on Identity Theft 9-10 (June 15, 2005), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf (last visited Nov. 17, 2013).

[226] Towle, *supra* note 110.

[227] "Under 15 U.S.C. § 57a, the Commission is authorized to prescribe 'rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce' within the meaning of Section 5(a)(1) of the FTC Act. The statute requires that Commission rulemaking proceedings provide

was even considering the application of the unfairness doctrine to those who suffered data security breaches without a concomitant violation of a published privacy policy.

And even now, with dozens of complaints and a similar number of Consent Orders[228] on record,[229] it is far from clear if the Commission will file an action in any specific set of circumstances, or what companies can do proactively to avoid an FTC enforcement action if they later suffer a data security breach.[230]

---

an opportunity for informal hearings at which interested parties are accorded limited rights of cross examination." Federal Trade Comm'n, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority 3 (Sept. 2002), *available at* http://www.ftc.gov/ogc/brfovrvw.shtm (last visited Nov. 17, 2013).

[228] "The uncertainties associated with lawmaking by consent decree is, of course, one of the unintended consequences of an otherwise efficient and increasingly popular process." Leary Speech, *supra* note 108.

[229] The unfairness cases include: *In re* TRENDnet, Inc., FTC File No. 122 3090 (Sept. 4, 2013) (consent order approved for public comment); *In re* Compete, Inc., FTC Docket No. C-4384, FTC File No. 102-3155 (Feb. 20, 2013) (consent order); *In re* EPN, Inc., FTC Docket No. C-4370, FTC File No. 112-3143 (Oct. 3, 2012) (consent order); *In re* Upromise, Inc., FTC Docket No. C-4351, FTC File No. 102-3116 (Mar. 27, 2012) (consent order); *In re* Lookout Servs., Inc., FTC Docket No. C-4326, FTC File No. 102-3076 (June 15, 2011) (consent order); *In re* Ceridian Corp., FTC Docket No. C-4325, FTC File No. 102-3160 (June 8, 2011) (consent order); *In re* Rite Aid Corp., FTC Docket No. C-4308, FTC File No. 072-3121 (Nov. 12, 2010 (consent order); *In re* Dave & Buster's, Inc., FTC Docket No. C-4291, FTC File No. 082-3153 (May 20, 2010) (consent order); United States v. Rental Research Servs., No. 0:09-CV-00524 (D. Minn. Mar. 6, 2009) (stipulated order); *In re* CVS Caremark Corp. , FTC Docket No. C-4259, FTC File No. 072-3119 (Jun. 18, 2009) (consent order); *In re* The TJX Cos., FTC Docket No. C-4227, FTC File No. 072-3055 (July 29, 2008) (consent order); *In re* Reed Elsevier Inc., FTC File No. 052-3094 (July 29, 2008) (consent order); *In re* CardSystems Solutions, Inc., FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (consent order); *In re* DSW, Inc., FTC Docket No. C-4157, FTC File No. 052-3096 (Mar. 7, 2006) (consent order); *In re* BJ's Wholesale Club, Inc., FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (consent order).

[230] *See, e.g.,* Christopher Wolf, *Dazed and Confused: Data Law Disarray,* Bus. Wk. Online, Apr. 2, 2006 ("As for the underlying security of the systems storing personal data, the FTC takes a 'we know it when we see it approach,' suing companies whose weak data security it believes amounts to an unfair consumer practice."), *available at* http://www.businessweek.com/technology/content/apr2006/tc20060403_290411.htm?campaign_id=search (last visited Nov. 17, 2013). *See also* Goodwin Proctor LLP, *supra* note 11, at 2-3 ("The FTC did not provide any general guidance or standards for what would be reasonable for other companies to avoid similar liability."). The FTC recently issued a publication titled *Protecting Personal Information: A Guide to Business* (Apr. 2007), which provides general advice on what a business can do to protect the personal information it collects and stores. However, the publication does not indicate whether a company following the suggested actions will be deemed in compliance with the Commission's "reasonable security measures" standard in the event of a data security breach, or whether a failure to do so will be deemed an "unfair" business practice.

A review of the allegations in the first three complaints filed does not provide much in the way of meaningful guidance.[231] The allegations are virtually identical. The variations between the allegations in BJ's and DSW on one hand and CardSystems on the other arose primarily from the different roles that the entities play in the credit/debit card processing system – BJ's and DSW are retailers, while CardSystems is a credit card processor used by retailers.

The allegations in these first three cases (as well as virtually all of the subsequent cases) fall into five categories (with some variations):

1. Failure to use data encryption
2. Failure to limit access to data
3. Failure to use readily available security measures
4. Failure to use security measures to detect unauthorized access
5. Information stored for too long

The *CardSystems Solutions* case also involved a sixth category:

6. Failure to properly assess security risks

Those that support the agency's unfairness actions could argue that even though the Commission gave no advanced notice of its intent to pursue data security breaches as unfair acts or practices, the respondents were still "on notice" because the FTC's prior deceptiveness complaints contained allegations that the respondents' failure to implement reasonable security measures made the statements in their privacy policies deceptive. Indeed, in many of the previous deceptiveness cases, the complaints identified security failures that were similar, and in some cases identical, to those set forth in the three later complaints.[232]

---

[231] As noted by one commentator about the unfairness doctrine in general:

> "[W]hile codified, the unfairness test 'was not explained satisfactorily.' There was no rulemaking or formal litigation, leaving practitioners with a 'variety of consent orders and anecdotal' evidence for guidance."

Panel Probes Revival of Unfairness Doctrine in FTC and States' Consumer Protection Cases, 86 Antitrust & Trade Reg. Rpt. (BNA), Apr. 9, 2004, at 354 (*quoting* Prof. Steven Calkin, Wayne St. Univ. School of Law).

[232] For example, in *In re* Guess?, Complaint, at 3, ¶8, Docket No. C-4091 (June 18, 2003), *available at* http://www.ftc.gov/os/2003/08/guesscomp.pdf (last visited Nov. 17, 2013), the Commission alleged that: "Since at least October 2000, Respondents' application and website have been vulnerable to commonly

The simple response is that in the earlier deceptiveness cases, the alleged *security failures* were not the basis for the claim of deception; the deception was in *the statements* made by respondents in their privacy policies. The security breaches were merely evidence of the deceptiveness of their privacy policies.[233] In reading the deceptiveness complaints, one could *only* conclude that as long as an entity made no privacy representations, a security breach alone would not give rise to an action under Section 5 at all.

Those that support the agency's unfairness actions could also argue that even if BJ's Wholesale Club could claim lack of notice, subsequent respondents like DSW and CardSystems (as well as all of the companies targeted by the FTC for data security breaches since those cases[234]) were now on notice of the Commission's intent to bring unfairness claims for data security breaches as a result of the allegations set forth in the *BJ Wholesale Club* complaint[235] and Consent Order.[236] The problem with that argument is that the allegations in the *BJ's Wholesale Club* complaint, and the complaints in *DSW* and *CardSystems,* only identify six general types of acts and omissions (as identified above) that the Commission deemed unfair *in those particular circumstances*. It is unclear whether all of these failures must occur before an unfairness action will be brought,[237] whether only one or a subset of such failures would be sufficient,[238] or whether

known or reasonably foreseeable attacks from third parties attempting to obtain access to customer information stored in Respondents' databases. These attacks include, but are not limited to, web-based application attacks such as 'Structured Query Language' ('SQL') injection attacks." This allegation is virtually identical to one of the allegations made in the CardSystems complaint. *See* CardSystems Complaint, *supra* note 142, at 2, ¶6.

[233] As noted by the Commission, "[t]he companies that have been subject of enforcement actions have made explicit or implicit promises that they would take appropriate steps to protect sensitive information obtained from consumers. Their security measures, however, proved to be inadequate; their promises, therefore, deceptive." FTC Statement, *supra* note 189, at 4.

[234] *See* cases set forth in note 229 *supra*.

[235] *See* note 125 *supra*.

[236] *See* note 128 *supra*.

[237] *See* note 225 *supra*. *See also* Remarks of Chairman Deborah Platt Majoras, Protection Consumer Information in the 21st Century: The FTC's Principled Approach, The Progress and Freedom Foundation, Securing the Internet Project, Internet Security Summit 7 (May 10, 2006) ("[T]he respondents engaged in a number of practices, *taken together*, that failed to supply reasonable security for sensitive consumer information) (emphasis in original), *available at* http://www.ftc.gov/speeches/majoras/060510ProgressFreedomFoundationRev051006.pdf (last visited Nov. 17, 2013) [hereinafter "Majoras Remarks"].

[238] Majoras Remarks, *supra* note 236, at 8 ("While any one of the failures may have been a problem, combined, they created an open invitation for a cyberheist.").

there are other security shortcomings that either alone or in combination with some or all of those enumerated in the complaints would constitute unfair acts or practices in the eyes of the Commission.

Indeed, one commentator has argued that at least one of the acts alleged to have been unfair is actually a proper and legal business practice.

> Parts of the FTC's list are simply wrong. Look at the allegation that BJ's "created unnecessary risks to the information by storing it for up to 30 days when it no longer had a business need to keep the information, and in violation of bank rules." There was a business need to keep at least part of the Info. For one thing, the federal Truth in Lending Act (12 CFR § 226.13) gives a credit card holder 60 days to dispute a transaction and gives the card issuer another 90 days to investigate it and make a reasonable determination regarding the validity of the transaction. This investigation is done by contacting the retailer and making it supply, essentially, proof that the transaction occurred with the cardholder. The issuer conducting the investigation might determine to side with the cardholder and that will initially relieve the cardholder of the repayment obligation. But that is not necessarily the end of it. If the retailer does not agree with that determination, the retailer can take it all up in court. How long does a court action take? Several years in most states.
>
> In short, there is a business need to keep Info for more than 30 days.[239]

Further, while the three FTC's complaints discussed above all claim that one of the respondents' shortcomings was their failure to encrypt data stored on their computer systems, neither the GLB, nor the Safeguards Rule promulgated by the Commission under the GLB require that stored data be encrypted.[240] In fact, in responding to a comment relating to the DSW proposed order, the Commission stated that a failure to encrypt personal, consumer

---

[239] Towle, *supra* note 110.

[240] *See, e.g.*, Guin v. Brazos Higher Educ. Serv. Corp., 2006 WL 288483, at *4 & n.2 (D. Minn. Feb. 7, 2006) ("While it appears that the FTC routinely cautions businesses to '[p]rovide for secure data transmission' when collecting customer information by encrypting such information 'in transit,' there is nothing in the GLB Act about this standard, and the FTC does not provide regulations regarding whether data should be encrypted when stored on the hard drive of a computer.").

information would not in and of itself establish a lack of reasonable security measures.[241]

Earlier statements from the Commission itself create further uncertainty as to the precedential value of these complaints. As note in a 2004 congressional statement:

> First, a company's security procedures must be appropriate for the kind of information it collects and maintains. Different levels of sensitivity may dictate different types of security measures. . . .
>
> The second principle . . . is that not all breaches of information security are violations of FTC law – the Commission is not simply saying "gotcha" for security breaches. Although a breach may indicate a problem with a company's security, breaches can happen, as noted above, even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces. Instead, the Commission recognizes that security is an ongoing process of using reasonable and appropriate measures in light of the circumstances.[242]

The ad hoc nature of the inquiry into the "adequacy" of security measures is highlighted by the FTC Statement itself:

> When breaches occur, our staff reviews available information to determine whether the incident warrants further examination. If it does, the staff gathers information to enable us to assess the reasonableness of the company's procedures in light of the circumstances

[241] Letter to VISA U.S.A., Inc., in *In re* DSW, Inc., (Mar. 7, 2005) ("The Commission agrees that the failure to encrypt does not *ipso facto* establish that a company lacked reasonable procedures to safeguard the information. Accordingly, the complaint in this matter alleges that DSW's *overall* security procedures were not reasonable, and cites several deficiencies (including the failure to encrypt) which, taken together, support this conclusion."), *available at* http://www.ftc.gov/os/caselist/0523096/0523096DSWLettertoCommenterVisa.pdf (last visited Nov. 17, 2013).

[242] FTC Statement, *supra* note 179, at 4, 5. *See also* Statement of Chairman Majoras, at the IAPP Privacy Summit, *Building a Culture of Privacy and Security—Together,* at 4, 5 (Mar. 7, 2007) ("In bringing each case, our message has been the same: companies must maintain reasonable and appropriate measures to protect sensitive consumer information. This requirement is process-oriented, rather than technology-oriented. . . . Our standard is not perfection; it is reasonableness. But I want to underscore that the FTC will enforce aggressively this standard to protect data security."), *available at* http://www.ftc.gov/speeches/majoras/070307iapp.pdf (last visited Nov. 17, 2013).

> surrounding the breach. This allows the Commission to determine whether the breach resulted from the failure to have procedures in place that are reasonable in light of the sensitivity of the information. In many instances, we have concluded that FTC action is not warranted. When we find a failure to implement reasonable procedures, however, we act.[243]

The primary objection to the FTC's position on unfairness in the data breach context is its unconstrained nature. There are no guidelines under which the Commission will act or refrain from acting if a data security breach occurs. Companies cannot know in advance whether the steps taken and the costs incurred to implement data security measures will be deemed adequate. Adequacy becomes whatever three commissioners say it is.[244]

And because data security is a moving target, what the Commission might consider adequate today could be considered inadequate next week or next month. "Stated differently, mechanical mitigation of the specific vulnerabilities or poor practices cited in prior FTC actions is inadequate."[245] As noted by the Commission:

> The risks companies and consumers confront change over time. Hackers and thieves will adapt to whatever measures are in place, and new technologies likely will have new vulnerabilities waiting to be discovered. As a result, companies need to assess the risks they face on an ongoing basis and make adjustments to reduce these risks.[246]

The results of the vagueness of this "adequacy" standard are twofold. First, some companies will avoid engaging in commercial activities that have a significant risk of consumer injury in case of a data security breach, which will lessen innovation and competition in those activities.[247]

---

[243] FTC Statement, *supra* note 189, at 5-6.

[244] "The moral of this story is that unfairness can be misused, particularly when there is no principled basis for applying it." Beales, *supra* note 51.

[245] Ronald D. Lee & Amy Ralph Mudge, *Reasonable Security: The FTC's Focus on Personal Privacy Initiatives Highlights the Importance of Integrated Information Security Programs,* 1 Privacy & Data Security L.J. 643, 651 (2006).

[246] Beales, *supra* note 51, at 7.

[247] See, e.g., Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange,* 2000 Stanford Tech. L. Rev. at 2, ¶ 93 ("Legislators should consider the reality of regulatory costs and the resulting contraction of services and opportunities before, not after, they act. As shown by the FTC's Advisory Committee on Access and Security, the issues created by even seemingly simple

Second, rational companies may over invest in new technologies to ensure that their security measures will be deemed adequate, resulting in increased costs that will be passed on to consumers in the form of higher prices, without proof that such additional costs will, in fact, provide enhanced protect for consumer data. Alternatively, if companies are unable to pass on those increased costs to consumers, they will need to absorb those cost, possibly by cutting back on spending on innovation. If the security costs become too high, companies simply will go out of business.[248]

Thus far the FTC has made no effort to determine whether the increased cost or reduced competition that may result from enforcement of its vague "adequacy" standard is worth the potential benefit of making it more difficult, but certainly not impossible, for determined cybercriminals to obtain the personal data anyway.

F. Claims for Failure to Adequately Police Security Practices of their Customers

In 2011 the FTC began filing complaints against data resellers who allegedly failure to adequately police the security practices of its customers to whom it provided consumers' personal information.[249] In the *SettlementOne*[250] and *ACRAnet*[251] complaints, the FTC alleged that hackers had gained access to their end user client's computers. In *Fajilan*, the complaint alleged that the hackers had gained access to both Fajilan's network and the networks of Fajilan's "end user clients."[252] The complaints

rules quickly grow complicated when set against the extraordinarily wide variety of information exchange practices that run throughout modern society.").

[248] *See* ACOAS, *supra* note 93, Statement of Daniel E. Geer ("Stern rules create stern costs; this is only natural. If, however, these stern costs tax day-to-day operations, rather than exception handling, then the sterner those rules are the fewer will be the entities that can bear the overhead."), *available at* http://www.ftc.gov/acoas/papers/individual_statements.pdf (last visited Nov. 17, 2013).

[249] *See* In re SettlementOne Credit Corp., File No. 082-3208 (Feb. 3, 2011), Complaint, *available at* http://www.ftc.gov/os/caselist/0823208/110203settlementonecmpt.pdf (hereinafter "SettlementOne Complaint") (last visited Nov. 29, 2013); In re ACRAnet, Inc., File No. 092-3088 (Feb. 3, 2011), Complaint, *available at* http://www.ftc.gov/os/caselist/0923088/110203acranetcmpt.pdf (hereinafter "ACRAnet Complaint") (last visited Nov. 29, 2013); In re Fajilan and Assocs., File No. 092-3089 (Feb. 3, 2011), Complaint, *available at* http://www.ftc.gov/os/caselist/0923089/110203statewidecmpt.pdf ((hereinafter "Fajilan Complaint") (last visited Nov. 29, 2013).

[250] SettlementOne Complaint, *supra* note 248, ¶ 10.

[251] ACRAnet Complaint, *supra* note 248, ¶ 9.

[252] Fajilan Complaint, *supra* note 248, ¶ 10.

alleged that the hackers had accessed 784 consumer reports from the networks of SettlementOne's clients,[253] 694 consumer reports form the networks of ACRAnet's clients,[254] and 323 consumer reports from Fajilan's clients.[255]

The complaints alleged that the data resellers should have taken steps to prevent the breaches by "evaluating the security of end user's computer networks," "requiring [the end users to implement] appropriate information security measures," and "training end user clients" concerning data security practices.[256]

The complaints further asserted that the data resellers should have required that "new and existing end user clients submit . . . documentation demonstrating that the clients' computer systems were virus free and otherwise properly protected."[257]

The Commission claimed that the data resellers failure to adequately police its customers for good data security practices violated the Gramm-Leach-Bliley Act,[258] the Fair Credit Reporting Act[259] and constituted an "unfair practice" under Section 5 of the FTC Act.[260]

It can be argued that the Commission viewed these cases as a shot across the bow of all companies that provide personal data to third parties. The press release accompanying the announcement of the settlement of the three data resellers, for example, at least implied that the duty to police imposed on the data resellers in these cases would be applied more broadly in the future. That press release contained a statement from the Director of the Commission's Bureau of Consumer Protection, David Vladeck, which stated:

---

[253] SettlementOne Complaint, *supra* note 248, ¶ 10.

[254] ACRAnet Complaint, *supra* note 248, ¶ 9.

[255] Fajilan Complaint, *supra* note 248, ¶ 10.

[256] SettlementOne Complaint, *supra* note 248 ¶ 8(c); ACRAnet Complaint, *supra* note 248, ¶ 7(c); and Fajilan Complaint, *supra* note 248, ¶ 8(c).

[257] SettlementOne Complaint, *supra* note 248, ¶ 8(c); ACRAnet Complaint, *supra* note 248, ¶ 7(c); Fajilan Complaint, *supra* note 248, ¶8(c).

[258] Title V of the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. §§ 6801, 6809, 6821, and 6827) (full-text); 16 C.F.R. part 313 (implementing privacy rules pursuant to GLB Act).

[259] Pub. L. No. 91-508, tit. 6, §601, 84 Stat. 1128, *codified as amended*, 15 U.S.C. §1681-1681x (Oct. 26, 1970).

[260] For a detailed analysis of the application of Gramm-Leach-Bliley Act and the Fair Credit Reporting Act to these cases, *see* David Alan Zetoony, *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for Its Breaches?*, 2011 STANFORD TECH. L. REV. 12, ¶¶ 20-37, *available at* http://stlr.stanford.edu/pdf/zetoony-ten-year-anniversary.pdf (last visited Nov. 30, 2013).

> These cases should send a strong message that *companies giving their clients online access to sensitive consumer information* must have reasonable procedures to secure it . . . . Had these three companies taken adequate steps to ensure the use of basic computer security measures, they might have foiled the hackers who wound up gaining access to extensive personal information in the consumer reporting system.[261]

Further, a statement issued by four of the Commissioners -- Brill, Leibowitz, Rosch, and Ramirez — made clear their belief that these cases would have far reaching implications for "all of those in the chain of handling consumer data," not just data resellers.

> [W]e are also cognizant of the fact that these are the first cases in which the Commission has held resellers responsible for downstream data protection failures. Looking forward, the actions we announce today should put resellers – *indeed, all of those in the chain of handling consumer data* – on notice of the seriousness with which we view their legal obligations to proactively protect consumers' data. The Commission should use all of the tools at its disposal to protect consumers from the enormous risks posed by security breaches that may lead to identity theft.[262]

Criticizing the Commissioners' statement, the Consumer Data Industry Association stated:

> The Commissioners' statements describe some potentially very significant new obligations for firms that provide consumer data to end-users or others. The Commissioners would impose these obligations without any public dialogue or administrative process. Before considering such a major policy shift, the Commission should engage

[261] Press Release, Federal Trade Commission, Credit Report Resellers Settle FTC Charges; Security Failures Allowed Hackers to Access Consumers' Personal Information (Feb. 3, 2011) (emphasis added), *available at* http://www.ftc.gov/opa/2011/02/settlement.shtm (last visited Nov. 30, 2013).

[262] Revised Statement of Commissioner Brill, In Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join, In the Matter of Settlement One Credit Corporation, ACRAnet, Inc. and Fajilan and Associates, FTC File Nos. 082-3208, 098-3088, 092- 3089 (Aug. 15, 2011) (emphasis added), *available at* http://www.ftc.gov/os/2011/08/110819settlementonestatement.pdf (last visited Nov. 29, 2013).

> knowledgeable industry participants in a discussion of the import of these obligations.[263]

It is also doubtful that a failure to police the data security activities of customers constitutes unfairness, as defined in the 1980 Unfairness Statement[264]:

> The three-part test established in the Unfairness Statement, later codified by Congress, permits the use of unfairness authority only where there is (1) "substantial" consumer injury, (2) the injury is not "outweighed by countervailing benefits to consumers or to competition," and (3) the injury is "not reasonably avoidable by consumers themselves." It is highly doubtful that the practice about which the Commission complains — a failure to police a company's customers by monitoring their data security practices — meets any of these criteria.[265]

G. HTC America – A Further Expansion of FTC Authority

On February 22, 2013, the FTC issued a complaint against mobile device manufacturer vendor HTC America, Inc.[266] The complaint alleged that HTC America modified third-party software used on its devices before distributing those devices to its customers, and in doing so "failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices."[267]

> Among other things, respondent: (a) failed to implement an adequate program to assess the security of products it shipped to consumers; (b) failed to implement adequate

---

[263] Letter from Stuart K. Pratt, President & CEO, Consumer Data Industry Association, to Federal Trade Commission 2 (Mar. 7, 2011) (public comment to Agreement Containing Consent Order, ACRAnet, Inc., File No. 092-3088, *available at* http://www.ftc.gov/os/comments/acranet/00018-58217.pdf (last visited Nov. 30, 2013).

[264] See § IV.A.1 *supra*.

[265] David A. Zetoony, *supra* note 259, ¶ 39.

[266] In the Matter of HTC America, Inc., Draft Complaint, FTC File No. 1223049 (Feb. 22, 2013) ("HTC Complaint"), *available at* http://www.ftc.gov/os/caselist/1223049/130222htccmpt.pdf (last visited November 20, 2013), *superseded by* Complaint, Docket No. C-4406 (July 2, 2013), *available at* http://www.ftc.gov/os/caselist/1223049/130702htccmpt.pdf (last visited November 20, 2013) [hereinafter "HTC Complaint"].

[267] HTC Complaint, *supra* note 265, at 2 ¶7.

> privacy and security guidance or training for its engineering staff; (c) failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices; (d) failed to follow well-known and commonly-accepted secure programming practices, including secure practices that were expressly described in the operating system's guides for manufacturers and developers, which would have ensured that applications only had access to users' information with their consent; and (e) failed to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents.[268]

Unlike the data security-related complaints previously filed by the FTC, this complaint does not allege *any* security breach or damages purportedly incurred by users as a result of the modifications to HTC America devices. Instead it merely alleges that:

> As a result of its failures described in Paragraph 7, HTC introduced numerous security vulnerabilities in the process of customizing its mobile devices. Once in place, HTC failed to detect and mitigate these vulnerabilities, which, if exploited, provide third-party applications with unauthorized access to sensitive information and sensitive device functionality.[269]

As for harm to consumers, the complaint concedes that there is no evidence that any users of HTC America devices have been harmed by these actions, despite the fact that the accused software has been distributed since 2009 and today is on approximately 18.3 million HTC devices.[270]

> Because of the potential exposure of sensitive information and sensitive device functionality through the security vulnerabilities in HTC mobile devices, consumers are at risk of financial and physical injury and other harm.[271]

---

[268] *Id. See also id.* ¶¶9-15.
[269] *Id.* ¶8.
[270] *Id.* ¶11.
[271] *Id.* ¶16.

Despite the total lack of actual harm to anyone, the FTC filed its complaint, based on the unfairness prong of Section 5, stating:

> As set forth in Paragraph 7-18, HTC failed to employ reasonable and appropriate security practices in the design and customization of the software on its mobile devices. HTC's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.[272]

This was an unprecedented expansion of the unfairness doctrine to attack conduct that has resulted in no harm to anyone. The FTC is attempting to expand its jurisdiction under Section 5 into "unfair security practices."

There is nothing in the Consent Order[273] entered into by HTC America that provides software developers or distributors of embedded software any meaningful guidance as to what conduct the FTC would consider "unfair security practices."

Read narrowly, *HTC America* would only apply to an organization that took existing software and modified it to make it less secure. However, read more broadly, the FTC could pursue a Section 5 unfairness action against any entity that distributed software the agency considers less secure than another version of the software without proof of any harm having come to the public as a result.

At least with the security breach cases, the FTC had some factual evidence that the security undertaken was less than adequate – namely the breach itself. Under *HTC America*, the FTC is acting without any evidence that the software actually distributed was likely to result in a security breach. As a practical matter, no software is 100% secure.[274] So the mere fact that HTC America's version of the software was *less secure* than the version received from Google does not prove that it was inadequately secure for its intended use.

V. Looking Forward

[272] *Id.* ¶21. The FTC also made claims that specific conduct of HTC America also constituted deception under the Act. Those claims are not discussed in this article.

[273] In the Matter of HTC America, Inc., Docket No. C-4406, Decision and Order (July 2, 2013), *available at* http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf (last visited Nov. 20, 2013).

[274]

While the FTC continues to expand its use of "unfairness" prong of Section 5 of the FTC Act in data security cases, the courts, and perhaps Congress, soon may weigh in on the efficacy and propriety of the FTC's current course.

A. Respondents Fight Back

Before 2011, the Commission had filed over 35 complaints for allegedly failed to protect consumers' personal information appropriately.[275] All of those complaints were resolved by a Consent Order; none were litigated. However, there are now two cases in which the respondents are challenging the FTC's authority under the "unfairness" doctrine.

1. FTC v. LabMD

In December 21, 2011, the FTC issued a Civil Investigative Demand ("CID") to LabMD, Inc. for, *inter alia,* the production of all documents related to any "security risk, vulnerability, and incidents through which [Petitioner's] documents and information [] either were or could have been disclosed to unrelated third parties."[276] LabMD filed a petition to limit or quash the CID. LabMD's petition was unsuccessful. When LabMD continued its refusal to produce the requested documents, the FTC filed a request for a court order to require production of the documents.[277]

In September 2012, the court ordered LabMD to attend a hearing and file a pleading asserting its "legal and factual support for failing to comply with the FTC's CIDs" and explain why the court should not order compliance with the CIDs.[278] After the hearing, the court generally agreed with LabMD that the

---

[275] *See* Hearing on Data Security Before the House Subcomm. on Commerce, Mfg., and Trade of the House Comm. on Energy and Commerce, 112th Cong., 3 n.6 (2011) (statement of David C. Vladeck, Dir. of the Bureau of Consumer Protection at the Federal Trade Comm'n), *available at* http://www.ftc.gov/opa/2011/05/pdf/110504datasecurityhouse.pdf (last visited Nov. 2, 2013).

[276] In re LabMD, Inc., LabMD's Petition to Limit or Quash the Civil Investigative Demand 1 (FTC Jan. 10, 2012), *available at* http://www.ftc.gov/os/quash/120110labmdpetition.pdf (last visited Nov. 30, 2013).

[277] Federal Trade Comm'n v. LabMD, Inc., No. 1:12-cv-3005-WSD, slip op. at 4 (N.D. Ga. Nov. 26, 2012).

[278] *Id.* at 4-5.

"unfairness" doctrine is "not unlimited."[279] In response to LabMD's argument that the FTC's use of the unfairness doctrine is improper because the FTC had not shown any injury to consumers,[280] the court held that one could persuasively argue that the "unfairness" doctrine does not grant the FTC authority to investigate data security breaches.[281]

However, the court found that "in light of the threat of substantial consumer harm that occurs when consumers are victims of identity theft," it agreed with the FTC that protecting the privacy of consumer data online comes within the FTC's investigative authority.[282] The court concluded that:

> [I]t is a plausible argument to assert that poor data security and consumer privacy practices facilitate and contribute to predictable and substantial harm to consumers in violation of Section 5 because it is disturbingly commonplace for people to wrongfully exploit poor data security and consumer privacy practices to wrongfully acquire and exploit personal consumer information.[283]

The court did not adjudicate whether the FTC has the authority to apply the "unfairness doctrine" to data security breaches, since to enforce the CID, the court only had to find that the FTC had a "plausible argument" for investigative jurisdiction.[284]

Thereafter, August 29, 2013, the FTC filed an Administrative Complaint against LabMD alleging that it violated the unfairness doctrine of Section 5 by "fail[ing] to provide reasonable and appropriate security for personal information on its computer networks."[285] On November 12, 2013, LabMD filed a motion to dismiss[286] based, in part, on LabMD's position that the

---

[279] *Id.* at 10 ("Although it is given broad discretion to determine what constitutes an unfair practice, the FTC's authority to investigate unfair practices using its subpoena enforcement power is not unlimited.")

[280] *Id.* at 11.

[281] *Id.* at 6-7 ("there is significant merit to . . . (LabMD's) argument that Section 5 does not justify an investigation into data security practices and consumer privacy issues").

[282] *Id.* at 13.

[283] *Id.* at 14-15.

[284] *Id.* at 15 (LabMD's argument "is not a sufficient reason to deny the FTC's request for enforcement").

[285] In re LabMD, Inc., Complaint, ¶¶ 22-23, FTC File No. 102 3099, Docket No. 9357 (Oct. 29, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmd part3.pdf.

[286] In the Matter of LabMD, Inc., Respondent LabMD's, Inc.'s Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings (Nov.

FTC lacks Section 5 "unfairness" authority to regulate patient-information data-security practices.[287] On November 22, 2013, the FTC filed its response.[288]

On January 16, 2014, the Commission issued its Order Denying LabMD's Motion To Dismiss.[289] In denying LabMD's motion, the Commission held that LabMD's position ("that the Commission has no authority to address private companies' data security practices as "unfair . . . acts or practices" under Section 5(a)(1) of the Federal Trade Commission Act")

> if accepted, would greatly restrict the Commission's ability to protect consumers from unwanted privacy intrusions, fraudulent misuse of their personal information, or even identity theft that may result from businesses' failure to establish and maintain reasonable and appropriate data security measures. The Commission would be unable to hold a business accountable for its conduct, even if its data security program is so inadequate that it "causes or is likely to cause substantial injury to consumers [that] is not reasonably avoidable by consumers themselves and [such injury is] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).[290]

The Commission concluded that "the FTC Act's prohibition of "unfair . . . acts or practices" applies to a company's failure to implement reasonable and appropriate data security measures."[291]

The case has continued to move forward since that ruling. On May 1, 2014, an administrative law judge granted LabMD's motion to compel testimony of an FTC official about "what data security standard, if any, have been published by the FTC or the Bureau, upon which Complaint Counsel intends to rely at trial to

---

12, 2013), *available at* http://www.ftc.gov/os/adjpro/d9357/131112respondLabMDmodiscomplaintdatyadminproceed.pdf (last visited Nov. 30, 2013).

[287] *Id.* at 9.

[288] In the Matter of LabMD, Inc., Complaint Counsel's Response in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice to Stay Administrative Proceedings (Nov. 22, 2013), *available at* http://www.ftc.gov/os/adjpro/d9357/131122ccoppositiontormotiontodismiss.pdf (last visited Nov. 30, 2013).

[289] In the Matter of LabMD, Inc., Commission Order Denying LabMD's Motion To Dismiss (Jan. 16, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf.

[290] *Id.* at 1-2.

[291] *Id.* at 2.

demonstrate that Respondent's data security practices were not reasonable and appropriate."[292]

Meanwhile, on March 20, 2014, LabMD filed a separate legal action against the FTC alleging that the agency abused its power and regulatory authority by filing an administrative complaint against LabMD over information security issues.[293] LabMD asserts that the administrative complaint filed by the FTC against the firm "is arbitrary, capricious, an abuse of discretion and power, in excess of statutory authority and short of statutory right, and contrary to law and constitutional right."[294]

2. FTC v. Wyndham Hotels

On June 26, 2012, the Commission filed a complaint against Wyndham Hotels for alleged data security failures that led to three data security breaches at Wyndham hotels in less than two years.[295] The FTC alleged that these "security failures led to fraudulent charges on consumers' accounts, more than $10.6 million in fraud loss, and the export of hundreds of thousands of consumers' payment card account information to a domain registered in Russia."[296]

The FTC accused Wyndham of engaging in both deceptive[297] and unfair[298] acts or practices in violation of Section 5 of the FTC Act.

On April 26, 2013, Wyndham filed a Motion to Dismiss[299] claiming, *inter alia,* that

---

[292] In the Matter of LabMD, Inc., Administrative Law Judge's Order Granting Respondent's Motion to Compel Testimony (May 1, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140501labmdordercompel.pdf.

[293] LabMD, Inc. v. Federal Trade Comm'n, Complaint (N.D. Ga. Mar. 20, 2014), *available at* http://docs.ismgcorp.com/files/external/20140320_DKT001_Verified_Complaint_for_Declaratory_and_Injunctive_Relief.PDF.

[294] *Id.* ¶104.

[295] Federal Trade Comm'n v. Wyndham Worldwide Corporation, Complaint, FTC File No. 1023142 (June 26, 2012), *available at* http://www.ftc.gov/os/caselist/1023142/120626wyndamhotelscmpt.pdf (last visited Nov. 30, 2013). The FTC amended its complaint on August 9, 2012 (*available at* http://www.ftc.gov/os/caselist/1023142/120809wyndhamcmpt.pdf (last visited Nov. 30, 2013)) [hereinafter "Wyndham Complaint"].

[296] *Id.* ¶ 2.

[297] *Id.* ¶¶ 20-23.

[298] *Id.* ¶¶ 24-40, 43, 47-49.

[299] Federal Trade Comm'n v. Wyndham Worldwide Corporation, Motion to Dismiss (Aug. 27, 2012), *available at* http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1398&context=historical (last visited Nov. 30, 2013).

> Nothing in the text or history of Section 5 purports to give the FTC authority to decide whether data-security protections are "unfair," and Congress's repeated enactment of specific data-security statutes (and failed attempts to enact comprehensive data-security laws) confirm that the statute cannot be construed so broadly. Simply put, Section 5's prohibition on "unfair" trade practices does not give the FTC authority to prescribe data-security standards for all private businesses.[300]

Wyndham's motion asserts that "the FTC is attempting to circumvent the legislative process by acting as if 'it has the statutory authority to do that which Congress has refused: establish data-security standards for the private sector and enforce those standards in federal court.'"[301]

A hearing on Wyndham's motion took place on November 8, 2013. On April 7, 2014, the court issues its order denying Wyndham's motion to dismiss.[302] The court held only that the FTC's complaint "sufficiently pleads an unfairness claim under the FTC Act and satisfies Federal Rule of Civil Procedure 8(a)."[303] However, the judge went out of her way to say:

> To be sure, the Court does not render a decision on liability today. Instead, it resolves a motion to dismiss a complaint. A liability determination is for another day. And this decision does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked. Instead, the Court denies a motion to dismiss given the allegations in this complaint—which must be taken as true at this stage—in view of binding and persuasive precedent.[304]

B. Congress Chimes In

[300] *Id.* at 7.

[301] Casselle Smith, *Wyndham Case Challenges FTC's Authority Over Cybersecurity,* FTC Beat (June 12, 2013), *available at* http://ftcbeat.com/2013/06/12/wyndham-case-challenges-ftcs-authority-over-cybersecurity/ (last visited Nov. 30, 2013).

[302] Federal Trade Comm'n v. Wyndham Worldwide Corporation, 2014 WL 1349019 (Apr. 7, 2014)

[303] *Id.* at *16.

[304] *Id.* at *4.

In October 2013, high-ranking members of the House and Senate Judiciary Committees sent a letter[305] to FTC Chairwoman Edith Ramirez insisting that the FTC issue guidelines defining just how far its Section 5 authority goes beyond the antitrust laws.[306] Referring specifically to the earlier proposed policy statements on the "unfair methods of competition" prong of Section 5 of the FTC Act by Commissioners Josh Wright[307] and Maureen K. Ohlhausen,[308] the letter states:

> [W]e take issue with your views that it is difficult to articulate the outer bounds of Section 5 authority or that existing decisions provide sufficient guidance.[309] In fact,

---

[305] http://judiciary.house.gov/news/2013/Signed%20Letter%20to%20FTC.pdf (last visited Nov. 27, 2013) [hereinafter "Congressional Letter"]. This letter strikes a similar position and tone to an earlier letter to the FTC from 10 Republican Senators in November 2012 to then-FTC Chairman Jon Leibowitz regarding a rumored FTC action against Google (*available at* http://www.webpronews.com/gop-senators-to-ftc-ease-up-on-tech-companies-like-google-2012-11 (last visited Nov. 26, 2013)). In that letter the senators stated:

> We are concerned about the apparent eagerness of the Commission under your leadership to expand Section 5 actions without a clear indication of authority or a limiting principle. When a federal regulatory agency uses creative theories to expand its activities, entrepreneurs may be deterred from innovating and growing lest they be targeted by government action. . . . We hope the Commission considers the consequences of hampering legitimate business model innovations and market activities of companies under an aimless, expansive, and possibly unauthorized use of the Commission's powers. We support innovation and believe economic expansion will follow if the government acts with humility rather than experimentation.

[306] "Even though the letter focuses on competition cases, the same general principles apply in consumer protection law." Berin Szoka & Geoffrey Manne, "FTC Must Limit Competition Authority, Congressional Judiciary Leadership Urges" (Oct. 23, 2013), *available at* http://techfreedom.org/post/64928331421/ftc-must-limit-competition-authority-congressional (last visited Nov. 26, 2013).

[307] Statement of Commissioner Joshua D. Wright Proposed Policy Statement Regarding Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act (June 19, 2013), *available at* http://www.ftc.gov/speeches/wright/130619umcpolicystatement.pdf (last visited Nov. 26, 2013).

[308] Section 5: Principles of Navigation, Remarks of Maureen K. Ohlhausen, Commissioner, Federal Trade Commission, at the U.S. Chamber of Commerce (Washington, D.C., July 25, 2013, *available at* http://www.ftc.gov/speeches/ohlhausen /130725section5speech.pdf (last visited Nov. 26, 2013).

[309] This statement is a reference to FTC Chairwoman Edith Ramirez' congressional testimony where she stated:

> Senator, I do agree that it is beneficial for the agencies to provide clear enforcement criteria where they can. I do take a different view with

> two of your fellow Commissioners have issued separate, but largely consistent, policy statements on the parameters of Section 5. Further, obtaining clear principles from a body of decisions that are largely formed through private settlement agreements and tailored to case-specific facts would be difficult enough, but when coupled with a lack of judicial review by courts who have not upheld a standalone Section 5 case since the 1960s, it is virtually impossible.[310]

Noting that prior calls for the FTC to publish guidance on how Section 5 will be applied to unfairness actions have not produced "a clear standard to which the public and business community can refer,"[311] the letter goes on to say that:

> The absence of clear parameters for the FTC's Section 5 authority based on empirical and economic justifications engenders uncertainty in the business community. This uncertainty acts as a deterrent to innovation and creativity, which are critical drivers of the American economy and are vitally important in today's challenging economic environment. Accordingly, articulating a standard by which the FTC intends to utilize its Section 5 unfair methods of competition authority should be a high priority.[312]

As noted by two commentators:

> These Congressmen . . . are asking the FTC to . . . move from a *discretionary* model of asserting what the law is to an *evolutionary* model of developing law over time – if not through actually litigating cases, then, at a minimum, clearly explaining the principles that limit its authority.[313]

> regard to Section 5. I do believe that this is an area that is difficult to specify precisely what the outer bounds are. . . . However, I will say again that I do believe that there is guidance that's provided. If you look back at the recent cases in which the agency has taken action, using Section 5 on a standalone basis. . . .

Oversight of the Enforcement of the Antitrust Laws Hearing Before the Subcomm. On Antitrust, Competition Policy and Consumer Rights of the Subcomm. On the Judiciary, 113th Cong. (Apr. 16, 2013), *quoted in* Congressional Letter, *supra* note 296, at 2 n. 9.

[310] Congressional Letter, *supra* note 296, at 2-3.

[311] *Id.* at 1.

[312] *Id.*

[313] Berin Szoka & Geoffrey Manne, *supra* note 297 (emphasis in original).

This dispute is reminiscent of an earlier battle between Congress and the FTC over the Commission's aggressive use of Section 5 in consumer protection cases during the 1970s. "In the 1970's, the Commission began to use its unfairness authority to legislate against perceived violations of 'public policy.' This misuse of its unfairness jurisdiction caused consternation in Congress."[314] "Only under heavy pressure from Congress, including a brief shutdown of the agency (and significant public criticism for becoming the 'National Nanny'), did the agency finally produce a Policy Statement on Unfairness — which Congress eventually codified by statute."[315]

Whether this letter will evolve into a replay of the 1970s is currently unclear.

C. Hints of FTC's Future Plans for the "Unfairness" Doctrine

It is clear from statements made by the FTC over the last few years, that unless restrained by the courts or Congress, the Commission plans to continue to use its Section 5 "unfairness" powers to broaden its authority over data collection, storage, access and usage practices. In 2011, for example, the FTC's Director of the Bureau of Consumer Protection testified before Congress:

> As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector and has brought more than 30 law enforcement actions against businesses that allegedly failed to protect consumers' personal information appropriately. . . . Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Accordingly, the Commission has undertaken substantial efforts to promote data security in the private

[314] Beales , *supra* note 54.

[315] Geoffrey Manne & Berin Szoka, *Section 5 of the FTC Act and Monopolization Cases: A Brief Primer,* Truth on the Market (Nov. 26, 2012), *available at* http://truthonthemarket.com/2012/11/26/section-5-of-the-ftc-act-and-monopolization-cases-a-brief-primer (last visited Nov, 26, 2013). For a discussion of the FTC's *Policy Statement on Unfairness*, see § IV.A.1 *supra*.

> sector through law enforcement, education, and policy initiatives.[316]

In March 2012, the Commission issued a report titled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers."[317] That report set forth "best practices" to be used by companies

> as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. To the extent these best practices exceed existing legal requirements, they are not intended to serve as a template for law enforcement or regulations under laws currently enforced by the FTC.[318]

Commissioner J. Thomas Rosch dissented from the issuance of the Final Privacy Report on several grounds:[319]

> 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. . . .
>
> [T]he Commission represented in its 1980, and 1982, Statements to Congress that, absent deception, it will not generally enforce Section 5 against alleged intangible harm. . . .
>
> 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

---

[316] Hearing on Data Security Before the H. Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy and Commerce, 112th Cong., at 1 (2011) (statement of David C. Vladeck, Dir. of the FTC Bureau of Consumer Protection), *available at* http://www.ftc.gov/opa/2011/05/pdf/110504datasecurityhouse.pdf (last visited Nov. 29, 2013).

[317] Federal Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (last visited Nov. 29, 2013) [hereinafter *Privacy Report*].

[318] Edith Ramirez, The Privacy Challenges of Big Data: A View from the Lifeguard's Chair (Technology Policy Institute Aspen Forum) 3 (Aug. 19 2013), *available at* http://www.ftc.gov/speeches/ramirez/130819bigdataaspen.pdf (last visited Nov. 29, 2013) [hereinafter "Ramirez Speech"].

[319] *See Privacy Report, supra* note 308 App. C.

> 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. 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). 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.[320]

More recently, FTC Chairman Edith Ramirez indicated that the FTC should use its Section 5 authority to regulate the evolution of "big data"[321] in the interest of consumer privacy "to ensure that these advances [in data collection and use] are accomplished by sufficiently rigorous privacy safeguards."[322] Likened the FTC's role to that of lifeguard, she stated:

> Like a vigilant lifeguard, the FTC's job is not to spoil anyone's fun but to make sure that no one gets hurt. With big data, the FTC's job is to get out of the way of innovation while making sure that consumer privacy is respected.[323]

Noting the growth of "big data," Chairman Ramirez stated:

> [W]ith big data comes big responsibility. Firms that acquire and maintain large sets of consumer data must be responsible stewards of that information. The FTC can already bring actions under Section 5 of the FTC Act, and we will continue to be active in data security under my watch.[324]

---

[320] *Id.* at C-4 and C-5 (citations omitted).

[321] Chairman Ramirez defines "big data" as "datasets whose size is beyond the ability of typical database software tools to capture, store, manage and analyze." *Id.* at 3 (*citing* MCKINSEY & CO., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION AND PRODUCTIVITY 1 (June 2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation (last visited Nov. 29, 2013)).

[322] *Ramirez Speech, supra* note 309.

[323] *Id.* at 2.

[324] *Id.* at 6.

Her advice to companies that collect personal data are:

> The FTC's privacy agenda aims to persuade companies to minimize risks in ways that encourage, not undercut, their ability to reap the rewards of a data-driven economy. The FTC urges companies to follow the three core principles laid out in the FTC's 2012 Privacy Report: privacy-by-design, simplified choice, and greater transparency.[325]

VI. Conclusion

Protecting personal data is a huge problem. The question is: What is the best way to deal with data protection?

The Federal Trade Commission has taken the lead in the online privacy area. It initially promoted self-regulation, but eventually realized that self-regulation was not working. Thereafter it began taking legal action against entities that violated the terms of their own privacy policies as deceptive trade practices under Section 5 of the FTC Act. Over the past 8 years, the Commission has filing a steady stream of complaints under its "unfairness" doctrine against companies that have experienced data security breaches, have failed to adequately police their customers' use of supplied data, and more recently against a company that purportedly distributed software with weakened security.

These actions were filed without any guidelines and without any advance notice to the respondents that their actions might violate Section 5 of the FTC Act. The complaints and consent orders entered into in these cases have provided limited guidance as to what a company should do (or not do) to avoid being the target of an unfairness action by the Commission.

Data security is too important to be left to the whim of the Federal Trade Commission or any other government agency. Companies need to know what is expected of them, so that they can implement appropriate technologies and put in place proper procedures to provide the appropriate level of protection for sensitive personal data. So far that has not occurred.

---

[325] *Id.* at 8.