THE FTC, THE UNFAIRNESS DOCTRINE, AND DATA SECURITY BREACH LITIGATION: HAS THE COMMISSION GONE TOO FAR?

MICHAEL D. SCOTT*

TABLE OF CONTENTS

* The author is a professor of law at Southwestern Law School in Los Angeles. He is author of seven legal treatises in the information technology law field, including SCOTT ON INFORMATION TECHNOLOGY LAW (3d 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 and Dean Bryant Garth and the Board of Trustees for their financial support for the research on this Article.

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]

INTRODUCTION

The Federal Trade Commission (FTC or the Commission) 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 become increasingly active in protecting consumer privacy rights online.[7]

---

1. FEDERAL TRADE COMMISSION, DISSENTING STATEMENT OF COMMISSIONER ORSON SWINDLE IN PRIVACY ONLINE: A REPORT TO CONGRESS FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 26 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/swindledissent.pdf [hereinafter Swindle Dissent].

2. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 3 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [hereinafter 2000 FTC REPORT] (statement of FTC Chairman Robert Pitofsky) ("Since 1995, the Commission has been at the forefront of the public debate on online privacy.").

3. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf [hereinafter 1998 FTC REPORT] ("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."); *see also* FEDERAL TRADE COMMISSION, A REPORT FROM THE FEDERAL TRADE COMMISSION STAFF: THE FTC'S FIRST FIVE YEARS PROTECTING CONSUMERS ONLINE (Dec. 1999), *available at* http://www.ftc.gov/os/1999/12/fiveyearreport.pdf.

4. *See* 1998 FTC REPORT, *supra* note 3, at i-ii ("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 id.* at 41; *see also* 2000 FTC REPORT, *supra* note 2, at ii-iii; FEDERAL TRADE COMMISSION, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 12 (July 1999), *available at* http://www.ftc.gov/os/1999/9907/privacy99.pdf [hereinafter 1999 FTC REPORT].

6. *See* 1998 FTC REPORT, *supra* note 3, at 3-4 ("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 protections are not implemented, the online

Section 5 of the Federal Trade Commission Act[8] (FTCA or FTC Act or the Act) 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] More recently, the agency made a "dramatic shift"[11] by filing complaints against organizations that have experienced data security breaches. Some of these companies made representations concerning the security of their computer systems, which the agency attacked as deceptive trade practices.[12] But the Commission sued other companies that made no such representations under § 5 of the Act for "unfair" trade practices.[13]

This Article will look at this new line of attack by the FTC. It will also analyze whether the Commission has exceeded its authority by 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. This Article will conclude with a proposal for

---

marketplace will fail to reach its full potential."); *see also* Letter from Mozelle W. Thompson, Fed. Trade Comm'n, to Sen. John McCain, Chairman, Comm. on Commerce, Science, and Transportation (Apr. 24, 2002), *available at* http:// www.ftc.gov/os/2002/04/sb2201thompson.htm (stating that "73% of online consumers who refused to purchase online did so because of privacy concerns"). It was estimated that $1.9 billion in e-commerce sales were lost in 2006 because of consumer concerns about Internet security. *See* Press Release, Gartner Consulting, Gartner Says Nearly $2 Billion Lost in E-Commerce Sales in 2006 Due to Security Concerns of U.S. Adults (Nov. 27, 2006), http://www.gartner.com/it/page.jsp?id=498974.

7. *See infra* Parts III-IV. 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. §§ 41-58 (2000).

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.*, Agreement Containing Consent Order, Geocities, No. 9823015 (F.T.C. Aug. 13, 1998), *available at* http://www.ftc.gov/os/1998/08/geo-ord.htm; *In re* Doubleclick, Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re* Intuit, Inc. Privacy Litigation, 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?* 1 (Dec. 6, 2005), *available at* www.goodwinprocter.com/getfile.aspx?filepath=/Files/publications/CA_DataSecurityBreaches_12_6_05.pdf.

12. *See infra* Part II.

13. *See infra* Part III.C.

legislation that would give the Commission specific authority to take action against companies that have experienced data security breaches, but only under well-defined guidelines.[14]

I. 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 the growth of both.[16] Commentators believed that market forces would punish those companies that did not adequately protect consumer privacy, while rewarding companies that protected privacy with increased sales.[17] The main element of self-regulation included FTC enforcement of those privacy policies that companies collecting personal information posted on their websites.[18]

By 2000, however, the Commission recognized 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 § 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]

---

14. *See infra* Part IV.B.

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. *See* 1998 FTC REPORT, *supra* note 3, at i-ii (explaining that "the Commission's goal has been to encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online").

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, at 4 (statement of Commissioner Thomas B. Leary, concurring in part and dissenting in part) [hereinafter Leary Statement] ("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.").

18. *See* Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web," Before the Subcomm. on Telecomms., Trade and Consumer Prot. of the House Comm. on Commerce (July 21, 1998), *available at* http://www.ftc.gov/os/1998/07/privac98.

19. *See* 2000 FTC REPORT, *supra* note 2, at ii ("The 2000 Survey, however, demonstrates that industry efforts alone have not been sufficient.").

20. 1998 FTC REPORT, *supra* note 3, at 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.").

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, the agency changed its position after the election of President George W. Bush and a change in leadership at the Commission. The new FTC Chairman, Timothy Muris, announced that the agency would expand enforcement of existing laws rather than pursue new legislation.[24] Muris indicated that the Commission was "primarily a law enforcement agency" that "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 particular issue of broad based, Internet only legislation is still premature at this moment."[26]

II. 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 focused on two activities that the agency identified as deceptive trade practices.[29]

First, the complaint alleged that GeoCities 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

---

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 . . . .").

23. *Id.* at 36-38.

24. Devin Gensch, *Putting Enforcement First*, THE RECORDER, Nov. 7, 2001, at 5; *see also* Timothy J. Muris, Chairman, FTC, Remarks at the Privacy 2001 Conference (Oct. 4, 2001), http://www.ftc.gov/speeches/muris/privisp1002.shtm (last visited Aug. 14, 2007).

25. *Challenges Facing the Federal Trade Commission: Hearing on H.R. 68 Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 107th Cong. 12 (2001) (statement of Timothy J. Muris, FTC Chairman), *available at* http://energycommerce.house.gov/reparchives/107/hearings/11072001Hearing403/print.htm.

26. *Id.*

27. Federal Trade Commission Act, 15 U.S.C. § 45(a) (2000). "Deceptive practices" under the FTCA are material representations or omissions likely to mislead a reasonable consumer. FTC v. Tashman, 318 F.3d 1273, 1277 (11th Cir. 2003). *See* 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/1998/08/geocitie.shtm.

29. *See* Complaint, GeoCities No. C-3850 (F.T.C. Feb. 5, 1999), *available at* http://www.ftc.gov/os/1999/02/9823015cmp.htm.

[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, the complaint alleged that GeoCities made "[m]isrepresentations involving sponsorship" when the site 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] The FTC claimed that GeoCities' conduct constituted "unfair or deceptive acts or practices" in violation of § 5 of the Act. The case quickly settled with the *GeoCities* Consent Order (Consent Order).[33]

The Consent Order required GeoCities to clearly post a privacy notice telling consumers "what information is being collected . . . its intended use[s] . . . , the third parties to whom it will be disclosed," and how consumers can access and remove the information.[34] 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.[35]

Since *Geocities*, the Commission has brought a number of cases against companies for violating their own published privacy policies.[36] 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 were able to gain unauthorized access to consumers' personal information[37] or the company intentionally disclosed

---

30. *See id.* paras. 12-16 (setting forth all of the misrepresentations involving information collected by Geocities alleged by the FTC).

31. *Id.* paras. 17-20.

32. *Id.* para. 19.

33. Decision and Order, Geocities, No. C-3850 (Feb. 5, 1999), *available at* http://www.ftc.gov/os/1999/02/9823015.do.htm.

34. *Id.* at 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* 1998 FTC REPORT, *supra* note 3, at 7-11. For a further discussion of these Principles, see *infra* Part III.B.

35. In addition, the provisions of the Geocities Consent Order (Consent Order) relating to the collection and use of information from children formed the basis for the Children's Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105-277, 112 Stat. 2681-2728 (1998), codified at 15 U.S.C. §§ 6501-6506 (2000), and its implementing regulations. 16 C.F.R. pt. 312 (2000).

36. Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promisesenf.html (last visited Feb. 1, 2008).

37. *See* Agreement Containing Consent Order, Guidance Software, Inc., No. 0623057, (F.T.C. Nov. 16, 2006), *available at* http://www.ftc.gov/os/caselist/0623057/0623057%20-Guidance%20consent%20agreement.pdf; Decision and Order, Nations Title Agency Inc., No. C-4161 (F.T.C. June 20, 2006), *available at* http://www.ftc.gov/os/caselist/0523117/0523117NationsTitleDecisionandOrder.pdf; Decision and Order, Petco Animal Supplies, Inc., No. C-4133 (F.T.C. Mar. 4, 2005), *available at* http://www.ftc.gov/os/caselist/0323221/050308do0323221.pdf; Decision and Order, MTS Inc., No. C-4110 (F.T.C. May 28, 2004), *available at* http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf;

the information to others[38]), making their privacy representations either deceptive or unfair.[39] The consent orders settling these cases required the companies to comply with their own privacy policies, as well as to implement "reasonable security measures" to safeguard customer data from unauthorized disclosure.[40]

The Commission has also used its § 5 powers to pursue deception claims against online companies for a variety of Internet-related claims unrelated to a violation of published privacy policies. These include claims against:

1. Spyware[41] and adware[42] distributors who surreptitiously downloaded software onto unsuspecting users' computers;[43]

Decision and Order, Guess?, Inc., No. C-4091 (F.T.C. July 30, 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf; Decision and Order, Microsoft Corp., No. C-4069 (F.T.C. Dec. 20, 2002), *available at* http://www.ftc.gov/os/caselist/0123240/microsoftdecision.pdf; Decision and Order, Eli Lilly & Co., No. C-4047 (F.T.C. May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elilillydo.htm.

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, it will not discuss these cases.

38. *See, e.g.*, Agreement Containing Consent Order, Vision I Props. LLC, No. 0423068 (F.T.C. Mar. 10, 2005), *available at* http://www.ftc.gov/os/caselist/0423068/050310agree0423068.pdf; Decision and Order, Gateway Learning Corp., No. C-4120 (F.T.C. Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.

39. In most of these cases, the complaint contained a "catch-all" allegation that the respondent's failure to comply with the FTC's own website privacy policy was either a deceptive or unfair act or practice, but the acts upon which the FTC grounded the complaint were the respondent's failure to comply with its own privacy policy. *See, e.g.*, Complaint, Petco Animal Supplies, Inc., No. C-4133 (F.T.C. Mar. 4, 2005), *available at* http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf (alleging 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 was therefore inaccessible to anyone but the customer providing the information"). *Id.* para. 11. The concluding paragraph of the complaint alleged generally that: "The acts and practices of 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.* para. 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 unfair act or practice.

40. The 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 the Commission's own privacy policies.

41. 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, track 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.'" FTC v. MaxTheater, Inc., No. 05-CV-0069-LRS, WL 3724918, at *2 (E.D. Wash. Dec. 6, 2005).

42. Adware is "[a] type of 'spyware' that uses collected information to display targeted advertisements . . . ." FTC v. Seismic Entm't Prod, Inc., No. 04-377-JD, 2004 WL 2403124, at *1 (D.N.H. Oct. 21, 2004).

2. Companies or individuals who made materially deceptive representations in marketing a spyware removal product;[44]

3. Those who made fraudulent claims in selling prescription drugs online;[45]

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;[46]

5. A reverse auction site that used improper promotional activities to solicit users of a competitive auction site;[47] and

6. Unauthorized charges in connection with "phishing."[48]

Most of these complaints included general allegations that the conduct was a deceptive or unfair act or practice,[49] but the focus was always on the deceptiveness of the targeted practices.

III. FTC'S CHANGE OF TACTICS: APPLYING THE "UNFAIRNESS" PRINCIPLE TO DATA SECURITY BREACHES

Recently the FTC filed complaints against three companies that experienced data security breaches without any violation of published privacy policies. The Commission 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 § 5 of the FTC Act.

---

43. *See, e.g.*, Complaint, Zango, Inc., No. C-4186 (F.T.C. Mar. 7, 2007), *available at* http://www.ftc.gov/os/caselist/0523130/0523130c4186complaint.pdf; *MaxTheater, Inc.*, 2005 WL 3724918 at *2; *Seismic Entm't Prod. Inc.*, 2004 WL 2403124 at *1.

44. FTC v. Trustsoft, Inc., No. H05-1905, 2005 WL 1523915, at *1 (S.D. Tex. June 14, 2005).

45. Complaint, FTC v. Rennert (F.T.C. July 6, 2000), *available at* http://www.ftc.gov/os/2000/07/iogcomp.htm.

46. United States v. ChoicePoint, Inc., No. 106-CV-0198 (N.D. Ga. Jan. 26, 2005), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf.

47. Complaint, FTC v. ReverseAuction.com (D.D.C. Jan. 6, 2000), *available at* http://www.ftc.gov/os/2000/01/reversecmp.htm.

48. Complaint, FTC v. Hill, No. H 03-5537 (S.D. Tex. Dec. 3, 2003), *available at* http://www.ftc.gov/os/caselist/0323102/040322cmp0323102.pdf; FTC v. C.J., No. 03-CV-5275-GHK (RZX) (C.D. Cal. July 24, 2003), *available at* http://www.ftc.gov/os/2003/07/phishingcomp.pdf. "Phishing" is a high-tech scam that uses 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* Office Of Consumer & Bus. Educ., Federal Trade Comm'n, FTC Consumer Alert, How Not to Get Hooked by a "Phishing" Scam 1 (2006), *available at* http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.pdf.

49. *See, e.g.*, Complaint, Zango, Inc., No. C-4186, paras 16-18 (F.T.C. Mar. 7, 2007) (claiming deceptive failure to adequately disclose adware, unfair installation of adware and unfair uninstall practices).

While the concept of "unfairness" has developed within the FTC and the courts over the last three decades, it has a checkered history.[50] Generally, the doctrine has been limited to the advertising, marketing, and sale of products or services.[51]

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

A. Evolution of the Unfairness Doctrine

Congress established the Federal Trade Commission in 1915.[52] Its purpose "was to prevent unfair methods of competition in commerce as part of the battle to 'bust the trusts.'"[53] Congress expanded FTC's authority over the ensuing decades. In 1938, Congress passed the Wheeler-Lea Amendment,[54] 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."[55]

Congress granted the FTC jurisdiction over "unfair" acts or practices in § 5 of the FTC Act in 1938.[56] The FTC did not use the "unfairness" prong of § 5 extensively until 1972. In that year, a U.S. Supreme Court decision encouraged the Commission to apply the unfairness doctrine to protect

---

50. *See* J. Howard Beales, III, Director, Bureau of Consumer Prot., Fed. Trade Comm'n, *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 Aug. 14, 2007) (noting that "the Commission's unfairness powers have been both used and avoided inappropriately").

51. *See, e.g.*, Bureau of Consumer Prot., Federal Trade Comm'n, Dot Com Disclosures, http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom (last visited Feb. 1, 2008).

52. The Commission was created by the Federal Trade Commission Act (Act of Sept. 26, 1914, ch. 311, § 5, 38 Stat. 717 (codified as amended at 15 U.S.C. §§ 41-58 (2000)). The Commission consists of a five-member board with broad authority to regulate unfair and deceptive business practices. No more than three FTC board members can be from the same political party, and they are appointed for overlapping seven-year terms. *Id.*§ 41.

53. FTC, About the Federal Trade Commission, http://ftc.gov/ftc/about.shtm (last visited Feb. 1, 2008). Yet, even at this early date, Congress recognized how vague the concept of "unfairness" was. *See* H.R. REP. NO. 1142, at 19 (1914) (Conf. Rep.) ("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* S. REP. NO. 597, at 13 (1914) (relaying the committee's decision to leave it up to the Commission to determine what practices are unfair).

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

55. Beales, *supra* note 50.

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

consumers in the area of advertising.[57] In *FTC v. Sperry & Hutchinson Co.*,[58] the Court noted that the consumer, as well as the competitor, needed protection from unfair trade practices, stating:

> [L]egislative 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.[59]

In a footnote,[60] the Court approvingly cited the criteria for unfairness that the Commission set forth in an earlier proposed rule relating to cigarette advertising and labeling (Cigarette Rule).[61] The factors set forth in the Cigarette Rule were:

> 1. [W]hether 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. [W]hether it is immoral, unethical, oppressive, or unscrupulous;
>
> 3. [W]hether it causes substantial injury to consumers (or competitors or other businessmen).[62]

This decision, and the 1975 Magnuson-Moss Warranty-Federal Trade Commission Improvement Act,[63] which provided the FTC with rulemaking authority,[64] resulted in an "ensuing decade of 'over-exuberance' as the agency tested the outer limits of its powers."[65] The FTC's actions were widely criticized,[66] and the matter came to a head in 1980.

---

57. *See* Dorothy Cohen, *Unfairness in Advertising Revisited,* 46 J. MARKETING 73, 73 (1982) ("A 1972 Supreme Court decision (*FTC v. Sperry & Hutchinson Co.*), encouraging the FTC to apply unfairness in protecting consumers, added a new dimension to advertising regulation and control.").

58. 405 U.S. 233 (1972).

59. *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).

60. *Sperry & Hutchinson*, 405 U.S. at 244 n.5.

61. Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8,355 (July 2, 1964) (to be codified at 16 C.F.R. pt. 408) [hereinafter Cigarette Rule].

62. *Id.*

63. Pub. L. No. 93-637, 88 Stat. 2183 (1974) (codified as amended at 15 U.S.C. §§ 2301-2312 (2000)).

64. Cohen, *supra* note 57, at 74 ("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.").

65. Skitol, *supra* note 59, 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

1. 1980 Unfairness Statement

In 1980 Congress enacted the Federal Trade Commission Improvement Act,[67] 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."[68]

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 (Unfairness Statement)[69] to the ranking members of the Committee in which it "narrow[ed] the unfairness doctrine."[70] 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.[71]

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

---

series of unsound decisions, persistent and unwise use of FTC resources, and imposition of costly and unnecessary requirements on retailers and advertisers.").

66. *See, e.g.*, Teresa M. Schwartz, *Regulating Unfair Practices Under the FTC Act: The Need for a Legal Standard of Unfairness*, 11 AKRON L. REV. 1 (1977) (observing that the unfairness theory was undefined, which allowed the FTC to shape it according to the conditions the agency was attempting to regulate); William C. Erxleben, *The FTC's Kaleidoscopic Unfairness Statute: Section 5*, 10 GONZ. L. REV. 333, 351 (1975) (analogizing the unfairness directives to the articles of the United States Constitution in that both were intentionally flexible and allow for interpretation and thus acknowledging that the result "may be alarming to some").

67. Pub. L. No. 96-252, 94 Stat. 374 (1980) (codified as amended in scattered sections of 15 U.S.C.).

68. Gellhorn, *supra* note 65, at 942.

69. *See* FTC Policy Statement on Unfairness, Letter from Michael Pertschuk, Chairman, Fed. Trade Comm'n to Wendell H. Ford, Chairman, and John C. Danforth, Ranking Minority Member, S. Comm. on Commerce, Science, and Transp., Consumer Subcomm. (Dec. 17, 1980), *reprinted in* Int'l Harvester Co., 104 F.T.C. 949, 1070-76 (1984) [hereinafter Unfairness Statement]. *See generally* TIMOTHY J. MURIS & J. HOWARD BEALES, III, THE LIMITS OF UNFAIRNESS UNDER THE FEDERAL TRADE COMMISSION ACT 23-25 (1991) (discussing the developments that led to the preparation of the Unfairness Statement, especially the Commission's use of unfairness subsequent to 1980); 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) (tracing the development of the law from early unfairness issue and deception theory cases to the unfairness statement and its effects on consumer sovereignty).

70. Gellhorn, *supra* note 65, at 956.

71. Unfairness Statement, *supra* note 69, at 1071.

> expectation that the underlying criteria would evolve and develop over time.[72]

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

1. "[W]hether the practice injures consumers;"
2. "[W]hether it violates established public policy;" and
3. "[W]hether it is unethical or unscrupulous."[73]

The Unfairness Statement stated that the Commission now agreed to abandon the third element, and "pledged to proceed only if either the unjustified consumer injury test or the violation of public policy test was satisfied."[74]

In 1984, the Commission formally adopted its 1980 Unfairness Statement as the standard that it would apply in proceedings challenging specific acts or practices as unfair.[75]

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.[76]

---

72. *Id*. at 1072.

73. *Id.* These factors were adapted from the factors set forth in the Cigarette Rule, *supra* note 61. 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." Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 971 (D.C. Cir. 1985) (citing FTC v. Sperry & Hutchinson, 405 U.S. 233, 244-45 n.5 (1972)). However, "the FTC's use of its unfairness doctrine has substantially evolved since *Sperry*." Letter from Timothy J. Muris, Chairman, FTC to the U.S. Dep't of Transp. (June 6, 2003), *available at* http://www.ftc.gov/os/2003/06/dotcomment.htm.

74. Gellhorn, *supra* note 65, at 942.

75. Unfairness Statement, *supra* note 69.

76. Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, 108 Stat. 1691 (1994) (codified at 15 U.S.C. § 45(n)).

B. The FTC's 2000 Report and Data Security

The issue of data security[77] predates the Internet. Data security is one of the lynchpins of what are generally referred to as the Fair Information Practice Principles.[78] A report by the Department of Health, Education and Welfare first articulated the Fair Information Practice Principles in 1973.[79] Since then, "a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies."[80]

One of the Fair Information Practice Principles, referred to as the Security Principle and 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.[81]

---

77. 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 (2006), *available at* http://www.cnss.gov/Assets/pdf/cns si_4009.pdf.

78. 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.").

79. *See* SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, DEP'T OF HEALTH, EDUC. AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS xxiii (1973).

80. 1998 FTC REPORT, *supra* note 3, at 48 n.27. Numerous reports, European legislation, and foreign standards set forth the core fair information practice principles. *See, e.g.*, CANADIAN STANDARDS ASS'N, MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION, Council Directive 95/46, 1995 O.J. (L281) 30, 31 (EC); DEP'T OF COMMERCE, PRIVACY AND THE NII: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (1995); ORG. FOR ECON. CO-OPERATION AND DEV., GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 7-8 (1981); PRIVACY WORKING GROUP, INFO. INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION 4-5 (1995); THE REPORT OF THE PRIVACY PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 1 (1977).

81. 1998 FTC REPORT, *supra* note 3, at 10.

"Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers."[82] The Commission promoted the Fair Information Practice Principles[83] as appropriate benchmarks for companies in self-regulating their promulgation and use of online privacy policies.[84] They also served as the basis for the Consent Order in the *Geocities* case,[85] and were implemented in the Children's Online Privacy Protection Act of 1998.[86]

In December 1999, the Commission established the Advisory Committee on Online Access and Security.[87] The Advisory Committee was asked to "consider the parameters of 'reasonable access' to personal information collected from and about consumers online and 'adequate security' for such information."[88] The Advisory Committee submitted its Final Report on May 15, 2000.[89]

In its Final Report, the Advisory Committee indicated that:

1. Security is a process, and no single standard can assure adequate security because technology and security threats are constantly evolving;[90]
2. Each 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;"[91]
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.[92]

---

82. *Id.* at 11.

83. *See* 2000 FTC REPORT, *supra* note 2, at 34 (presenting the Commission's statement that "[a]s a general matter, however, the Commission lacks authority to require firms to adopt information practice policies").

84. *Consumer Privacy on the World Wide Web: Hearing Before the Subcomm. on Telecomms., Trade and Consumer Prot. of the H. Comm. on Commerce*, 105th Cong. (1998) (statement of Robert Pitofsky, Chairman, FTC), *available at* http://www.ftc.gov/os/1998/9807/privac98.htm.

85. *See generally* Geocities, No. C-3850 at IV (Feb. 5, 1999), *available at* http://www.ftc.gov/os/1999/02/9823015.do.htm (requiring GeoCities to provide clear and prominent notice to consumers regarding the collection and use of personal information).

86. Pub. L. No. 105-277, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. §§ 6501-6506 (2000), and its implementing regulations codified at 16 C.F.R. pt. 312 (2000)).

87. *See* FTC Advisory Committee on Online Access and Security, http://www.ftc.gov/acoas/ (last visited Feb. 1, 2008).

88. 2000 FTC REPORT, *supra* note 2, at 28.

89. *See generally* FED. TRADE COMM'N ADVISORY COMM., FINAL REPORT ON ONLINE ACCESS AND SECURITY (2000), http://www.ftc.gov/acoas/papers/acoasfinal1.pdf [hereinafter ACOAS].

90. *Id.* at 19.

91. *Id.* at 25.

92. *Id.*

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 websites to the extent not already provided by the COPPA"; (ii) apply the Fair Information Practice Principles to online data privacy generally;[93] and (iii) give the Commission specific authority to "promulgate more detailed standards pursuant to the Administrative Procedure Act."[94] 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 . . . .[95]

Orson Swindle strongly dissented to the 2000 Report by objecting to the Commission's seeming abandonment of self-regulation in favor of "extensive government regulation."[96]

> 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 breathtakingly broad laws whose details will be filled in later during the rulemaking process.

---

93. 2000 FTC REPORT, *supra* note 2, at 36.

94. *See id.* at ii-iii, 36 (referencing the Administrative Procedure Act, 5 U.S.C. § 553 (2000), and noting that self-regulatory efforts by industries were insufficient to protect certain data, and calling for the FTC to implement its own regulations). 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) to define the proposed legislation requirements. . . .").

95. 2000 FTC REPORT, *supra* note 2, at 37-38.

96. Swindle Dissent, *supra* note 1, at 1.

> 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.[97]

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.[98]

Commissioner Thomas B. Leary also dissented from portions of the Report, including the provisions relating to data security.[99] 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."[100]

Leary also disagreed with the Commission's claim that the fair information practices are "widely-accepted" in the online and offline worlds.[101] Leary indicated that the Report failed to explain the meaning of "'reasonable' standards" 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."[102] 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. This is a legislative judgment. Congress can, and already does pass industry-specific legislation to deal with these situations."[103]

---

97. *Id.* at 1-2.
98. *Id.* at 27.
99. *See* Leary Statement, *supra* note 17, at 4.
100. *Id.* at 1.
101. *See id.* at 5-6 (citing a survey implying that the "fair information practices" are far from widely-accepted in the business community and in "the offline world").
102. *Id.* at 6 (observing that the Commission never really defined what "reasonable standards" actually meant).
103. *Id.* at 7 (citing Fair Credit Reporting Act, 15 U.S.C. § 1681 (2000); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 15 U.S.C.); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000); Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified in scattered sections of 47 U.S.C.); and Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified in scattered sections of 47 U.S.C.)).

Over seven years have passed since the Commission pushed for specific legislation to provide broad consumer privacy protection, but Congress thus far has declined to act. Recently, 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 § 5 of the FTC Act.

C. A Data Security Breach as an "Unfair Act or Practice"

The FTC recently began to apply the unfairness doctrine to situations in which a company has suffered a data security breach. The Commission has not held hearings, solicited public comments, engaged in rulemaking, or issued any policy statements or guidelines on when, if ever, the unfairness doctrine can or should be applied to data security breaches.[104] 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 in the last few years. As recently as 2003, J. Howard Beales III, 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 modern unfairness authority continues to be to protect consumer sovereignty by attacking practices that impede consumers' ability to make informed choices.*[105]

Some commentators question 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.[106]

Since all of the actions brought to date have quickly settled, no judicial opinions exist on the efficacy or legality of the Commission's actions

---

104. Prior statements from FTC officials seemed to indicate that the Commission 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, May 31, 2001, http://www.wired.com/politics/security/news/2001/05/44173 ("'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.'").

105. Beales, *supra* note 50, at Part III (emphasis added).

106. *See, e.g.*, Holly K. Towle, *Let's Play "Name that Security Violation!"*, 3 CYBERSPACE LAW., Apr. 2006, at 11 (questioning the link between a data security breach and an actual "unfair act or practice" under the existing law), *available at* http://www.klgates.com/newsstand/Detail.aspx?publication=3220.

brought under the unfairness doctrine. As discussed below, it is unclear whether the Commission should apply the unfairness doctrine 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.[107]

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 commentator Holly K. Towle stated: "[T]he FTC seems to have found a heretofore unknown, federal, general obligation to maintain security for personally identifiable data."[108]

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 numbers (SSN) or financial information such as credit card numbers."[109] Data security breaches can take many forms and do not necessarily lead to any consumer injury.[110]

A variety of activities may give rise to data security breaches. Breaches can result from intentional actions, including hacking,[111] employee theft,[112]

---

107. *See* Thomas B. Leary, Commissioner, FTC, Remarks at the Conference on Unfairness and the Internet, http://www.ftc.gov/speeches/leary/unfairness.shtm (last visited Aug. 14, 2007) [hereinafter Leary Speech] (stating "'unfair' is a particularly imprecise and flexible term, so its meaning has evolved over time").

108. Towle, *supra* note 106.

109. GEN. ACCOUNTING OFFICE, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN, GAO-07-737 2, *available at* (2007), http://www.gao.gov/new.items/d07737.pdf?source=ra [hereinafter GAO Report]; *see id.* at 2 n.2 (defining personally identifiable information as "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").

110. The GAO reported that in a study of the twenty-four largest data security breaches reported in the media from January 2000 through June 2005, that only four included evidence of subsequent fraudulent activities. *Id.* at 5-6. The vast majority (eighteen) showed no clear evidence of any identity theft, and the remaining two lacked sufficient information to make any determination. *Id.*

111. 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, http://scmagazine.com/us/news/article/647277/457-million-victim-tjx-companies-breach-lead-federal-notification-law; *see also* Orders, Bell v. Acxiom Corp., No. 4:06CV00485-WRW (E.D. Ark. Oct. 3, 2006) (unpublished decision) (stating that in 2003 Acxiom's computer databanks were compromised and client files revealed to the hackers).

112. *See, e.g.*, Towle, *supra* note 106 (listing and describing the many forms of data security breaches).

theft of equipment (such as laptop computers[113] and hard drives[114]), and deception or misrepresentation to obtain unauthorized data.[115] They can also arise from negligent conduct by the organization that suffered the security breach, including the loss of laptop computers or hard disks,[116] loss of data tapes,[117] unintentional exposure of data on the Internet,[118] and improper disposal of data.[119] Security breaches can also arise from an organization's implementation of software that the organization reasonably believes to be secure, but which contains vulnerabilities that render it insecure.[120]

To date, the Commission has filed complaints against three companies—BJ's Wholesale Club, DSW, Inc. and CardSystems Solutions, Inc.[121]—that

---

113. *See, e.g.*, Robert Ellis Smith, *Laptop Hall Of Shame*, FORBES, Sept. 7, 2006, http://www.forbes.com/columnists/2006/09/06/laptops-hall-of-shame-cx_res_0907laptops.html (detailing security risks and breaches that have plagued the on going and widespread use of laptop computers).

114. *See, e.g.*, Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705 (S.D. Ohio 2007) (involving the theft of a hard drive from Litton's Atlanta office); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006) (including an example of a stolen hard drive containing unencrypted customer information as a security breach).

115. *See, e.g.*, Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.shtm (recalling that the FTC charged ChoicePoint with a violation of the Fair Credit Reporting Act by providing customer data to individuals who did not have a permissible purpose to obtain that data).

116. *See, e.g.*, Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 2-3 (D.D.C. 2007) (entailing facts where the plaintiffs alleged that an ING employee's negligent conduct led to the loss of a computer and thus a security breach).

117. Paul Shread, *Bank's Tape Loss Puts Spotlight on Backup Practices*, ENTERPRISE STORAGE FORUM, Feb. 28, 2005, http://www.enterprisestorageforum.com/continuity/news/article.php/3486036 (describing Bank of America's loss of computer data tapes containing customer and account information for 1.2 million federal employees).

118. *See, e.g.*, Press Release, Texas Woman's University, Data Exposure Response (Jan. 25, 2007), http://www.twu.edu/response/index.asp (disclosing a personal data compromise via the internet at Texas Woman's University).

119. *See, e.g.*, Debra Black, *Rogers Pins Data Dump on Sales Firm*, THESTAR.COM, Apr. 9, 2007, http://www.thestar.com/article/200900 (covering a case where a third party sales company improperly disposed of sensitive data leading to the compromise of that data).

120. *See* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 62 MD. L. REV. (forthcoming 2008). An earlier draft of the article is available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1010069 (last visited Feb. 1, 2008) (noting that even systems and networks that are seemingly secure may still be vulnerable to hackers).

121. Some might argue that the FTC has actually filed four unfair trade practice actions for data security breaches. However, in *United States v. ChoicePoint, Inc.*, the allegations were qualitatively different than those contained in the other three cases. Complaint at 7-9, United States v. ChoicePoint, Inc., No. 1 06-CV-0198 (N.D. Ga. Jan. 30, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf. In the *BJ's Wholesale Club, DSW*, and *CardSystems* cases discussed *infra*, the respondents were accused of failing to implement proper security measures, thereby allowing hackers to gain access to consumers' personal information. The *Choicepoint* complaint, in contrast, alleged that the respondent failed to properly verify or authenticate the identity and qualifications of prospective subscribers before granting them access to its databases of consumer data, and failed to properly monitor the activities of these unauthorized subscribers. *Id.* para. 25. The case did not relate to data security breaches at all. *See* Press Release, FTC, ChoicePoint

suffered data security breaches, and are alleged to have engaged in unfair trade practices. Each of these cases is discussed in detail below.

2. BJ's Wholesale Club

In 2005, thieves used a Wi-Fi[122] system at a BJ's Wholesale Club store in Miami 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 losses from fraudulent transactions using counterfeit credit cards garnered from the stolen data allegedly totaled around $13 million.[123]

The FTC filed a complaint[124] against BJ's for an unfair act or practice due to BJ's failure to provide "reasonable security" for its computer network, alleging that BJ's:

> 1. [D]id not encrypt the information while in transit or when stored on the in-store computer networks;
>
> 2. [S]tored the information in files that could be accessed anonymously—that is, using a commonly known default user id and password;
>
> 3. [D]id not use readily available security measures to limit access to its computer networks through wireless access points on the networks;
>
> 4. [F]ailed to employ sufficient measures to detect unauthorized access or conduct security investigations; and
>
> 5. Created unnecessary risks to the information by storing the data for up to thirty days when it no longer had a business need to keep the information, and in violation of bank rules.[125]

"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."[126]

Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.html.

122. "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, and uses ethernet protocol." *See* The Free Dictionary, http://www.thefreedictionary.com/wifi.

123. Perkins Coie LLP, *Is It an Unfair Practice to Lack Adequate Security for Consumer Information?*, July 5, 2005, http://www.perkinscoie.com/news/pubs_detail.aspx?publication=735&op=updates (estimating the financial damage of the BJ's security breach at around $13 million).

124. *See* Complaint, BJ's Wholesale Club, Inc. No. C-4148 (F.T.C. Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf.

125. *Id.* para. 7.

126. *Id.*

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 twenty 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.[127]

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.[128]

As one commentator noted, "[t]he agency will likely consider the terms of the BJ's settlement (which will last for twenty years) as the standard that all companies that obtain and store consumer financial information must meet."[129]

3. DSW, Inc.

On December 1, 2005, the FTC announced[130] that it had entered into a settlement and consent judgment[131] 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."[132]

According to the FTC's complaint,[133] DSW used computer networks to obtain authorization for credit card, debit card, and check purchases at its stores as well as to track inventory. For credit and debit card purchases,

---

127. Decision and Order, at 2-3, BJ's Wholesale Club, No. C-4148 (F.T.C. Sept. 20, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf.

128. *See id.* at 3 (ordering BJ's to improve security by obtaining an assessment of its data safeguards).

129. Perkins Coie LLP, *supra* note 123.

130. *See* Press Release, FTC, DSW Inc. Settles FTC Charges (Dec. 1, 2005), http://www.ftc.gov/opa/2005/12/dsw.shtm (announcing the settlement between the FTC and DSW Inc.).

131. *See* Decision and Order, DSW, Inc., No. C-4157 (F.T.C.), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSCDecisionandOrder.pdf (forming an agreement between DSW and the FTC).

132. *See* Press Release, FTC, DSW Inc. Settles FTC Charges (Dec. 1, 2005), http://www.ftc.gov/opa/2005/12/dsw.shtm (announcing the settlement between the FTC and DSW Inc.).

133. *See* Complaint, DSW, Inc., No. C-4157 (F.T.C. Dec. 1, 2005), *available at* http://www.ftc.gov/os/caselist/0523096/051201comp0523096.pdf (alleging that DSW stored sensitive consumer data that became vulnerable to computer hackers and identity thieves).

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 thieves could use to create counterfeit cards that would appear to be genuine in the authorization process.[134] DSW collected information, including the routing number, account number, check number, and the consumer's driver's license number and state, when they accepted personal checks for payment.[135] According to the complaint, DSW's data security failures allowed hackers to gain access to information on more than 1.4 million customers.[136]

The FTC alleged that DSW:

> 1. [C]reated 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 [those] networks;
>
> 3. [S]tored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password;
>
> 4. [Failed to] limit sufficiently the ability of computers on other in-store and corporate networks; and
>
> 5. [Failed to] employ sufficient measures to detect unauthorized access.[137]

As in *BJ's Wholesale Club*, no adjudication addressed the question of whether any of these acts constituted "unfair acts or practices" under § 5 because DSW immediately settled. Under the Order, which also lasts for twenty years, DSW must:

> • "[D]esignat[e] . . . an employee or employees to coordinate and be accountable for the information security program";
>
> • "[I]dentif[y] . . . material internal and external risks to the security, confidentiality, and integrity of consumer 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";
>
> • "[D]esign and implement[] . . . reasonable safeguards to control the risks identified through risk assessment, and regular[ly] test[] or monitor[] . . . the effectiveness of the safeguards' key controls, systems and procedures"; and

---

134. *See id.* para. 5 (detailing how the personal data stored by DSW could be hacked, stolen, and used to create quite authentic-looking credit cards).

135. *See id.* (explaining that when taking checks from customers, DSW recorded sensitive financial data and stored it in such a fashion that made it vulnerable to hackers and identity thieves).

136. *Id.* para. 9.

137. *Id.* para. 7.

> • "[E]valuat[e] and adjust[] . . . [its] information security program in light of the results of the testing and monitoring . . . , any material changes to [its] operations or business arrangements, or any other circumstances that [DSW] knows or has reason to know may have a material impact on the effectiveness of its information security program."[138]

DSW must also obtain a biennial assessment and report "from a qualified, objective, independent, third-party professional" concerning DSW's compliance with the Order.[139]

Interestingly, in commenting on the *DSW* decision, the Commission indicated that it might use its enforcement discretion under § 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.[140]

4. CardSystems Solutions, Inc.

Unlike BJ's Wholesale Club and DSW, CardSystems Solutions, Inc. (CSS) is not a retailer. According to the complaint,[141] CSS provides merchants with products and services used in "authorized processing" of credit and debit card purchases from the banks that issue the cards, and CSS uses the Internet and web-based software applications to provide information to client merchants about authorizations it performed for them.

Specifically, 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 the information 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 included in the authorization request that the issuing bank received.

---

138. Decision and Order, at 2-3, DSW, Inc., No. C-4157 (F.T.C. Dec. 1, 2005), *available at* http://www.ftc.gov/os/caselist/0523096/051201comp0523096.pdf.

139. *Id.* at 3.

140. *See* Letter from Donald Clark, FTC, Secretary, to Kathryn D. Kohler, Asst. General Counsel, Bank of America Corp., Re: DSW, Inc., Matter No. 0523096 (Mar. 7, 2005), *available at* http://www.ftc.gov/os/caselist/0523096/0523096DSWLettertoCommenterBankofAmerica.pdf.

141. Complaint, CardSystems Solutions, Inc., No. C-4168 (F.T.C. Sept. 8, 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf.

According to the complaint, CSS "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information stored on its computer network."[142] In particular, the complaint alleges that CSS:

> 1. [C]reated unnecessary risks to the [customers'] information by storing it in a vulnerable format for up to 30 days;
>
> 2. [D]id not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks, including but not limited to "Structured Query Language" (or "SQL") injection attacks;
>
> 3. [D]id not implement simple, low-cost, and readily available defenses to such attacks;
>
> 4. [F]ailed 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. [D]id not use readily available security measures to limit access between computers on its network and between such computers and the Internet; and
>
> 6. [F]ailed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.[143]

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.[144] The hacker then used this information to manufacture counterfeit cards that were subsequently used to make fraudulent purchases.[145]

As in the two prior cases, no adjudication addressed the question of whether any of these acts constituted "unfair acts or practices" under § 5, since CSS immediately agreed to settle. Under the Order in this case, which again lasts for twenty years, CSS must:

> • [D]esignat[e] an employee or employees to coordinate and be accountable for the information security program;
>
> • [I]dentif[y] . . . 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

142. *Id.* para. 6.
143. *Id.*
144. *Id.* para. 7.
145. *Id.* para. 8.

> 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.
>
> • [D]esign and implement[] . . . 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]valuat[e] and adjust[] . . . respondent's information security program in light of the results of the testing and monitoring required by [the 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.[146]

As in the two previous cases, CSS must also obtain a biennial assessment and report from a qualified, objective, independent, third-party professional concerning DSW's compliance with the Order.[147]

D. Applying the Unfairness Doctrine to Data Security Breaches

While the courts and Congress give the Commission broad authority to take action against unfair practices, "[t]he Commission is hardly free to write its own law of consumer protection."[148] The Commission's exercise of its unfairness authority in any particular instance remains subject to judicial review and may be affirmed or set aside for abuse of agency discretion.[149]

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

1. "[W]hether the practice injures consumers;" and
2. "[W]hether it violates established public policy."[150]

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

---

146. Decision and Order at 3, CardSystems Solutions, Inc. No. C-4168) (F.T.C. Sept. 8, 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148CardSystemsdo.pdf.

147. *Id.*

148. Nat'l Petroleum Refiners Ass'n v. FTC, 482 F.2d 672, 693 (D.C. Cir. 1973).

149. *See* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 249 (1972) (clarifying that a court can vacate an agency's unfairness determination for failure to adequately set forth the grounds for its determination); FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 314 (1934) (holding that courts can review agency unfairness determinations).

150. *See* Unfairness Statement, *supra* note 69, at 1072; *supra* notes 74-75 and accompanying text.

1. Injury to Consumers

Unjustified consumer injury from a party's conduct constitutes the primary and most important factor in an unfairness analysis.[151] Indeed, if the injury to consumers is significant enough, it can be the *sole* basis for a finding of unfairness.[152] 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.[153]

a. Substantial Injury

First, the injury must be "substantial."[154] "Substantial injury is an objective test."[155] 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.[156]

The most common form of injury suffered by consumers is monetary harm.[157] A small degree of harm to a large number of consumers may be deemed "substantial," as may a significant risk of harm to each consumer.[158] Emotional harm, "other more subjective types of harm," and "trivial or merely speculative harm[s]" generally would not be considered "substantial."[159]

---

151. *See* Unfairness Statement, *supra* note 69, at 1073 ("Unjustified consumer injury is the primary focus of the FTC Act.").
152. *Id.*
153. *Id.*; *see also* 15 U.S.C. § 45(n) (2000) (setting forth the standard for unfairness determinations).
154. Unfairness Statement, *supra* note 69, at 1073.
155. *See* Beales, *supra* note 50, at Part III (discussing the elements of the unfairness doctrine and the role the FTC's unfairness authority should play in fashioning consumer protection policy).
156. Unfairness Statement, *supra* note 69, at 1073.
157. *See id.* (discussing examples of monetary harm that amount to "substantial injury" under the unfairness doctrine, such as "when sellers coerce consumers into purchasing unwanted goods or services[,] or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defense arising from the transaction"). 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.*
158. *Id.* at n.12.
159. *Id.*

Interestingly, the Commission has not claimed that consumers suffered any monetary losses in any of the FTC complaints filed to date. In the *BJ's Wholesale Club* complaint, for example, the FTC made only the following allegation relating to injury:

> 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.[160]

Instead of alleging any specific consumer injury caused by BJ's Wholesale Club's actions, the Commission only conclusorily alleged that BJ'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," which constituted an "unfair act or practice."[161] 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 for their out-of-pocket expenses, and DSW has provided some amount of reimbursement to these customers.[162]

---

160. *See* Complaint, BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005) *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf. 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. para. 9.

161. *Id.* at 3.

162. Complaint para. 9, DSW, Inc., No. C-4157 (F.T.C. Dec. 1, 2005) *available at* http://www.ftc.gov/os/caselist/0523096/051201comp0523096.pdf. As in the *BJ's Wholesale Club* complaint (see *supra* note 124), there was only a conclusorily allegation of consumer injury in the *DSW* complaint.

And in *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.[163]

Federal law limits consumers' liability for unauthorized credit card charges to fifty dollars per card as long as the credit card company is notified within sixty days of the unauthorized charge.[164] In fact, many credit card companies do not require consumers to pay the fifty dollars and will not hold consumers liable for the unauthorized charges, no matter how much time elapsed since the discovery of the loss.[165] As such, consumers affected by these security breaches may suffer no monetary loss at all.[166]

---

163. Complaint para. 8, CardSystems Solutions, Inc., No. C-4168 (F.T.C. Sept. 8, 2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf. 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. para. 9.

164. *See* 12 C.F.R. § 226.12(b) (2007) ("The liability of the cardholder for unauthorized use of a credit card shall not exceed the lesser of $50 or the amount of money, property, labor or services obtained by the unauthorized use before notification to the card issuer.").

165. *See Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the Subcomm. on Terrorism, Tech., and Homeland Sec.*, 110th Cong. 3 n.3 (Mar. 21, 2007) (statement of Lydia Parnes, Dir., FTC Bureau of Consumer Protection), *available at* http://judiciary.senate.gov/pdf/3-21-07Parnestestimony.pdf [hereinafter Parnes Testimony] (discussing limitations on consumer liability for unauthorized credit charges); *see also* ACOAS, *supra* note 89 (Statement of Stewart Baker), *available at* http://www.ftc.gov/acoas/papers/individual_statements.pdf ("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).").

166. Parnes Testimony, *supra* note 165, at 4 ("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.").

Out of all the cases brought by consumers against the three entities discussed above, only one reported decision discussed consumer injury.[167] In *Key v. DSW, Inc.*,[168] the plaintiff filed a class action suit against DSW for negligence, breach of contract, conversion, and breach of fiduciary duty. The plaintiff 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."[169] The complaint alleged that as a consequence of DSW's actions, the plaintiff and the class members were subjected to "'a substantially increased risk of identity theft, and . . . 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.'"[170] However, the court dismissed the complaint on the ground that the plaintiff lacked standing to sue because she had identified *no actual injury* suffered as a result of DSW's conduct. As the court explained:

> 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.[171]

---

167. *See* Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006) (dismissing for lack of standing where the plaintiffs merely alleged that their information was subjected to a substantially higher risk of identity theft). 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 CardSystems Solutions 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 that law requires that the conduct be intentional and the plaintiff had not alleged intentionality. 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. 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 Act based on an alleged breach of contract between DSW and the credit card issuers. However, consumer injury was not discussed in that opinion either.

168. *Key*, 454 F. Supp. 2d at 686.

169. *Id.*

170. *Id.*

171. *Id.* at 689, 690 (citations omitted).

Other cases brought by consumers for data security breaches have been dismissed for a failure to show any actual injury to the plaintiff-consumer.[172]

This result remains consistent with the findings of a recently released report from the Government Accountability Office (GAO).[173] 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 the unauthorized creation of new accounts. For example, in reviewing the twenty-four largest breaches reported in the media from January 2000 through June 2005, GAO found that three included evidence of resulting fraud on existing accounts and one included evidence of unauthorized creation of new accounts. For eighteen of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining two, there was not sufficient information to make a determination.[174]

---

172. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp., 499 F.3d 629, 639 (7th Cir. 2007) (finding that "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs ha[d] not suffered a harm that the law is prepared to remedy"); Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705, 712-13 (S.D. Ohio 2007) (granting defendant's motion for summary judgment in a suit against a mortgage loan service provider for negligence in protecting the personal information of its customers); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 7-8 (D.D.C. 2007) (holding that an increased risk of identity theft did not constitute injury-in-fact sufficient to confer standing); Forbes v. Wells Fargo Bank N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006) (granting bank's motion for summary judgment in a suit for breach of contract, breach of fiduciary duty, and negligence after computers containing bank customer's personal information were stolen from the bank); Order, Bell v. Acxiom Corp., 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) (granting defendant's motion for summary judgment because the injuries plaintiff complained of were merely speculative and failed to satisfy the injury-in-fact test); Giordano v. Wachovia Sec. LLC, 2006 WL 2177036, at *4 (D.N.J. July 31, 2006) (remanding to state court for plaintiff's failure to establish a concrete and personalized injury); Guin v. Brazos Higher Educ. Serv. Corp., 2006 WL 288483, at *4-*5 (D. Minn. Feb. 7, 2006) (dismissing a suit by plaintiffs alleging that the defendant had negligently allowed an employee to keep unencrypted customer data on a laptop computer stolen from the employee's home); Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906, at *3 (D. Ariz. Sept. 6, 2005) (granting defendant's motion for summary judgment in a suit for negligence after a theft of computer hard drives containing personal information of the plaintiffs).

173. *See* GAO Report, *supra* note 109.

174. *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* Steve Lohr, *Surging Losses, but Few Victims in Data Breaches*, N.Y. TIMES, Sept. 27, 2006, at G1, *available at* http://www.nytimes.

The President's Identity Theft Task Force recently reached the same conclusion.[175]

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.[176]

However, none of these "injuries" constitute "substantial consumer injury" as required by the unfairness doctrine. As noted above,[177] it remains unlikely that consumers bore any of the cost of the asserted fraudulent transactions. Furthermore, 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.[178] Finally, the "inconvenience or time" customers may spend in obtaining replacement credit/debit cards fails to qualify as monetary damages.[179] Thus, even at this late date, after the FTC has had ample opportunity to thoroughly investigate these three data breaches in detail, the Commission cannot point to *any* consumer injury cognizable under the unfairness doctrine.

An earlier FTC enforcement action that did not involve a data security breach highlighted the difficulty of establishing substantial consumer injury when applying the unfairness doctrine to online privacy violations. In *Federal Trade Commission v. ReverseAuction.com, Inc.*, the FTC alleged

---

com/2006/09/27/technology/circuits/27lost.html (quoting Fred H. Cate, Director of the Center for Applied Cybersecurity Research, Indiana University in Bloomington, who stated "[t]he threat of identity theft from data losses is being greatly exaggerated, . . . because a lot of people have fallen into the trap of equating data loss with identity theft").

175. *See* PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 2-3 (2007), *available at* http://www.identitytheft.gov/reports/StrategicPlan.pdf [hereinafter Task Force Report] ("The loss or 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.").

176. Deborah Platt Majoras, Chairman, Remarks at the Internet Security Summit, Protecting Consumer Information in the 21st Century: The FTC's Principled Approach, The process and Freedom Foundation, Securing the Internet Project 8 (May, 10, 2006), *available at* http://ftc.gov/speeches/majoras/060510ProgressFreedomFoundationRev051006.pdf [hereinafter Marjoras Reparks].

177. *See supra* notes 166-68 and accompanying text.

178. *See supra* note 169.

179. *See supra* notes 172-73 and accompanying text.

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.[180] 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 website to send unsolicited commercial e-mail.

The Commission alleged that ReverseAuction violated § 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,[181] or that ReverseAuction's use of eBay member information for the purposes of sending unsolicited commercial e-mail constituted an unfair practice.[182]

All of the commissioners voted to support the deception claim, but two of the commissioners voted against the unfairness claim.[183] 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." 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."
>
> 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.[184]

---

180. Complaint para. 8, FTC v. ReverseAuction.com, Inc. (D.D.C. Jan. 6, 2000), *available at* http://www.ftc.gov/os/2000/01/reversecmp.htm.

181. *Id.* para. 16.

182. *Id.* para. 17.

183. *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.

184. *Id.* (internal citations and emphasis omitted).

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.
>
> 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.*[185]

The same concern applies to unfairness claims based on 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 "not be outweighed by any offsetting consumer or competitive benefits . . . ."[186] 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."[187] 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."[188]

There is no question that there is a potential cost, and in some cases a substantial cost, in a company not properly protecting consumers' personal information from unauthorized access or disclosure. However, there is also

---

185. *Id.* (emphasis added).
186. Int'l Harvester Co., 104 F.T.C. 949, 1073 (1984); *see also* 15 U.S.C. § 45(n) (2000).
187. *Int'l Harvester*, 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.* at n.17.
188. *Id.* at 1073-74.

a cost, and in many cases an enormous cost, in providing a high level of protection for that information.[189] 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.[190] That remains a fact of life, and the Commission itself recognizes this shortfall: "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 . . . ."[191]

So, given the two extremes—no security as unacceptable and absolute security as 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."[192] Without formal hearings and rulemaking, it remains impossible for the FTC, or a court, to make that determination.

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*

---

189. *See* ACOAS, *supra* note 89, at 23 (asserting that security 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).

190. *See* Prepared 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, *available at* http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf [hereinafter FTC Statement] ("[T]he Commission recognized that there is no such thing as 'perfect' security and that breaches can occur even when a company has taken all reasonable precautions."); *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) (explaining, in terms of a cost benefit analysis, the balance between the possible injury to consumers and the cost that a company must pay to safeguard information while stressing the agency's focus on reasonableness and indicating that a consumer's data was the currency of the information economy).

191. Majoras Remarks, *supra* note 176, at 9.

192. Richard Craswell, *The Identification of Unfair Acts and Practices by the Federal Trade Commission*, 1981 WIS. L. REV. 107, 134.

> *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.[193]

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:[194] "[I]f consumers could have made a different choice, but did not, the Commission should respect that choice."[195] 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."[196]

While it remains possible for a consumer to live a reasonably full and productive life without using a credit or debit card or personal check (i.e., conducting all of her transactions with cash only), and would, therefore, result in 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 as student loans,[197] bank accounts,[198] and other types of financial,[199] as well as health insurance,[200] transactions.

---

193. Swindle Dissent, *supra* note 1, at 16 (emphasis added).

194. Int'l Harvester Co., 104 F.T.C. 949, 1074 (1984) (spelling out the three-part test used to determine if a consumer's injury was legally unfair); *see also* 15 U.S.C. § 45(n) (2000).

195. Beales, *supra* note 50.

196. Unfairness Statement, *supra* note 69, 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.

197. *See* Guin v. Brazos Higher Educ. Serv. Corp., 2006 WL 288483 (D. Minn. Feb. 7, 2006) (addressing a student loan company's information security breach after confidential unencrypted information on an employee laptop was stolen).

198. *See* Forbes v. Wells Fargo Bank N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006) (discussing a bank's information security breach when granting summary judgment in finding that the plaintiffs suffered no injury in fact from increased likelihood of information breach).

199. *See, e.g.*, Giordano v. Wachovia Securities, LLC, No. 06-476 (JBS), 2006 WL 2177036 (D.N.J. July 31, 2006) (dealing with a financial institution's loss of personal information relating to retirement accounts).

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.[201]

The Commission or a court hearing a case involving an allegation of unfairness under the circumstances presented in these cases would likely 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."[202] 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."[203]

However, public policy 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."[204]

The agency will use public policy to support a finding of unfairness when laws and judicial decisions have formally acknowledged the policy, and legislatures and courts have widely recognized it. If a public policy is not well-established, the agency 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."[205]

---

200. *See* Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-015PHXSRB, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005) (addressing a health care manager's loss of personal information that led to identity theft).
201. Majoras Remarks, *supra* note 176, at 10.
202. Unfairness Statement, *supra* note 69, at 1074.
203. *Id.* at 1075.
204. *Id.*
205. *Id.* at 1076.

In 1982, the Commission further limited the role of public policy, stating that it was not an independent basis for unfairness,[206] but rather it "may provide additional evidence" of unfairness.[207] Congress subsequently codified this reduced role in 1994:[208] "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."[209]

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."[210]

Since 2000, Congress has authorized the Commission to hold hearings and to promulgate rules under several statutes, including Title V of the Gramm-Leach-Bliley Financial Services Modernization Act (GLB),[211] the Fair Credit Reporting Act,[212] and the Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act of 2002.[213]

Some commentators suggest[214] that the unfairness complaints filed by the Commission for data security breaches are actually being brought pursuant to the Safeguards Rule[215] that the Commission promulgated under

---

206. Letter from James C. Miller, Chairman, FTC to Bob Packwood, Chairman, Comm. on Commerce, Sci., and Trasnp., and Bob Kasten, Chairman, SubComm. On Consumer Comm. on Commerce, Sci., and Transp. (Mar. 5, 1982), *reprinted in* Antitrust & Trade Reg. Rep. (BNA) No. 1055, at 568-70 (Mar. 11, 1982).

207. *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.

Trade Regulation Rule; Credit Practices, 49 Fed. Reg. 7,740, 7,743 (Mar. 1, 1984).

208. Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, 108 Stat. 1691 (1994), codified at 15 U.S.C. § 45(n) (2000).

209. Beales, *supra* note 50.

210. 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 (Jan. 7, 2007), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=507582.

211. Gramm-Leach-Bliley Financial Services Modernization Act (GLB), 15 U.S.C. §§ 6801-6809, 6821-6827 (2000).

212. *Id.* § 1681.

213. Pub. L. No. 107-204, 116 Stat. 745 (2002).

214. *See* FTC Statement, *supra* note 190, at 5; *see also infra* note 267 and accompanying text.

215. Standards for Safeguarding Customer Information (Safeguards Rule), 16 C.F.R. pt. 314 (2002); *see also* Privacy of Consumer Financial Information Rule (Privacy Rule), 16 C.F.R. pt. 313 (2000).

the authority granted to it in the GLB.[216] The Safeguards Rule requires financial institutions to maintain reasonable policies and procedures to ensure the security, confidentiality, and integrity of customer information.[217] 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.[218] 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.[219]

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.[220] Each financial institution must also: (1) assign one or more employees to oversee the program; (2) conduct a risk 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.[221]

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

---

216. The Safeguards Rule, implementing Section 501(b) of the GLB (15 U.S.C. § 6801(b) (2000)), was promulgated by the Commission on May 23, 2002 and became effective on May 23, 2003.

217. 16 C.F.R. § 314.1(a) (2007).

218. 15 U.S.C. § 6809(3)(A) (2000). "Financial institutions" are defined as businesses that are engaged in certain "financial activities" described in § 4(d) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843(k) (2000)) and its accompanying regulations. 12 C.F.R. §§ 225.28, 225.86 (2007).

219. 15 U.S.C. § 6809.

220. 16 C.F.R. § 314.3.

221. *Id.* § 314.4.

"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.[222]

No established public policy existed at the time of the filing of these three complaints that the Commission could have relied upon to justify its actions. One commentator noted that "[t]o 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."[223]

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 issued no policy statements, conducted no rulemaking,[224] and made no pronouncements that it 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 three complaints and three consent orders[225] on record, it remains far from clear whether the Commission will file an action in a specific set of circumstances, or what actions companies can proactively take to avoid an FTC enforcement action if they later suffer a data security breach.[226]

---

222. FTC Statement Before the Senate Comm. on Commerce, Sci. & Transp. on Data Breaches and Identity Theft 9-10 (June 15, 2005), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

> 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.

Id.

223. Towle, *supra* note 106.

224. FTC, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority (Sept. 2002), *available at* http://www.ftc.gov/ogc/brfovrvw.shtm.

> Under . . . 15 U.S.C. Sec. 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 an opportunity for informal hearings at which interested parties are accorded limited rights of cross examination.

Id.

225. *See* Leary Speech, *supra* note 107 (stating that "[t]he uncertainties associated with lawmaking by consent decree is, of course, one of the unintended consequences of an otherwise efficient and increasingly popular process").

226. *See, e.g.*, Christopher Wolf, *Dazed and Confused: Data Law Disarray,* BUS. WK., Apr. 2, 2006, *available at* http://www.businessweek.com/technology/content/apr2006/tc20060403_290411.htm?campaign_id=search (indicating that regarding "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");

A review of the allegations in the three complaints filed to date does not provide much in the way of meaningful guidance.[227] As shown in Table 1, the allegations against the three respondents were virtually identical. The variations between the allegations in BJ's and DSW on one hand, and CardSystems on the other, resulted 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.

TABLE 1

Respondent / *Allegations*	*BJ's Wholesale Club*	*DSW, Inc.*	*CardSystems Solutions, Inc.*
No data encryption	Failed to encrypt information in transit or when stored on in-store computer networks	Failed to encrypt information in files	Stored information in a "vulnerable format"
Failed to limit access	Stored information in files that could be accessed using default user ID and password	Stored information in files that could be accessed using default user ID and password ——— Failed to limit the ability of computers on one in-store network to connect to computers on other in-store and corporate networks	Failed to use strong passwords to prevent hacker from gaining control of computers on its network and accessing personal information stored on the network ——— Failed to use readily available security measures to limit access between computers on its network and between such computers and the Internet

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, that 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. FTC, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (Apr. 2007), *available at* http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf.

227. *Panel Probes Revival of Unfairness Doctrine in FTC and States' Consumer Protection Cases*, Antitrust & Trade Reg. Rep. (BNA) No. 2150, at 352 (Apr. 9, 2004) (quoting Prof. Steven Calkin, Wayne St. Univ. School of Law) [hereinafter Panel Probes Revival] (noting that "while codified, the unfairness test 'was not explained satisfactorily'" because there was no legislative or judicial guidance, "leaving practitioners with a 'variety of consent orders and anecdotal' evidence for guidance").

Readily available security measures not used	Failed to use readily available security measures to limit access to its computer networks through wireless access points	Failed to use readily available security measures to limit access to its computer networks through wireless access points	Failed to implement simple, low-cost, and readily available defenses
Security measures to detect unauthorized access not used	Failed to employ sufficient measures to detect unauthorized access or conduct security investigations	Failed to employ sufficient measures to detect unauthorized access	Failed to employ sufficient measures to detect unauthorized access to personal information or conduct security investigations
Stored information too long	Created unnecessary risks to information by storing it for up to thirty days when no longer needed and in violation of bank rules	Created unnecessary risks to sensitive information by storing when it no longer had a business need to keep information	Created unnecessary risks to customers' information by storing it for up to thirty days
Failed to properly assess security risks			Did not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks, including but not limited to, Structured Query Language (or SQL) injection attacks

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 later *BJ's Wholesale Club, DSW*, and *CardSystems* complaints.[228]

228. For example, in *Guess?*, the Commission alleged that:
> Since at least October 2000, Respondents' application and website have been vulnerable to commonly 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.

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 occurred in the statements made by respondents in their privacy policies. The security breaches merely constituted evidence of the deceptiveness of their privacy policies.[229] 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 § 5.

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 future respondents) 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's Wholesale Club* complaint[230] and Consent Order.[231] 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 in Table 1) that the Commission deemed unfair in those particular circumstances. It remains unclear whether all of these failures must occur before the FTC will bring an unfairness action,[232] or whether only one or a subset of the failures would be sufficient for an unfairness action,[233] or whether there are other security shortcomings that either alone or in combination with 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.

Complaint at 3, para. 8, *Guess?*, No. C-4091 (F.T.C. June 18, 2003), *available at* http://www.ftc.gov/os/2003/08/guesscomp.pdf. This allegation is virtually identical to one of the allegations made in the *CardSystems* complaint. *See CardSystems* Complaint, *supra* note 141, at 2, para. 6 (alleging a failure of the Respondent "to provide reasonable and appropriate security for personal information stored on its computer network").

229. FTC Statement, *supra* note 190, at 4. As noted by the Commission, "[t]he companies that have been subject to 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." *Id.*

230. *See BJ's Wholesale Club* Complaint, *supra* note 124, at 3, para. 10 (alleging the acts and practices of BJ's Wholesale Club to constitute "unfair acts or practices" in violation of § 5(a)).

231. *See BJ's Wholesale Club* Decision and Order, *supra* note 128 (ordering BJ's Wholesale Club to establish a comprehensive information security program).

232. *See Panel Probes Revival*, *supra* note 227, at 352 (describing the uncertainties of the unfairness doctrine as practitioners have no formal guidance as to its application); *see also* Marjoras Remarks, *supra* note 176 ("[T]he respondents engaged in a number of practices, *taken together*, that failed to supply reasonable security for sensitive consumer information.").

233. Majoras Remarks, *supra* note 176, at 8 ("While any one of the failures may have been a problem, combined, they created an open invitation for a cyberheist.").

> 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.[234]

Further, while the three FTC complaints discussed above all claim that the respondents' shortcomings included 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.[235] In fact, in a comment relating to the *DSW* proposed order, the Commission stated that a failure to encrypt personal consumer information would not, in and of itself, establish a lack of reasonable security measures.[236]

Earlier statements from the Commission create further uncertainty as to the precedential value of these complaints. As noted 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. . . .

---

234. Towle, *supra* note 106.

235. *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.").

236. Letter from Donald S. Clark, Secretary, FTC, to Russell W. Schrader, Senior Vice President and Assistant General Counsel, VISA U.S.A. Inc., in DSW, Inc. (Mar. 7, 2005), *available at* http://www.ftc.gov/os/caselist/0523096/0523096DSWLettertoCommenterVisa.pdf ("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.").

> 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 . . . 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.[237]

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

> 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 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.[238]

The primary objection to the FTC's position on unfairness in the data breach context is its unconstrained nature. No guidelines exist under which the Commission will act or refrain from acting if a data security breach occurs. Companies cannot know in advance whether the steps they have taken and the costs they have incurred to implement data security measures will be deemed adequate. Adequacy becomes what three commissioners say it is.[239] And because data security is a moving target, what the Commission might consider adequate today could be considered inadequate next week; "[s]tated differently, mechanical mitigation of the specific vulnerabilities or poor practices cited in prior FTC actions is inadequate."[240] As noted by the Commission:

---

237. FTC Statement, *supra* note 190, at 4-5; *see also* Deborah Platt Majoras, Chairman, FTC, Remarks at the IAPP Privacy Summit, Building a Culture of Privacy and Security—Together 4-5 (Mar. 7, 2007), *available at* http://www.ftc.gov/speeches/majoras/070307iapp.pdf ("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.").

238. FTC Statement, *supra* note 190, at 5-6.

239. Beales, *supra* note 50 (indicating that "the moral" of the history of the FTC's use of unfairness authority "is that unfairness can be misused, particularly when there is no principled basis for applying it").

240. 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).

> 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.[241]

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 competition in those activities.[242] 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 protection for consumer data. If the security costs become too high, companies simply will go out of business.[243]

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.

IV. A LEGISLATIVE PROPOSAL

If Congress enacted legislation providing for specific FTC oversight of corporate data security under carefully constrained rules and regulations, the legislation could alleviate much of the uncertainty and negative effects of the FTC's seemingly ad hoc enforcement actions under the unfairness doctrine against companies that have suffered data security breaches.

---

241. Prepared Statement of the Federal Trade Commission on Cybersecurity and Consumer Data: What's at Risk for the Consumer? Before the Subcomm. on Commerce, Trade & Consumer Prot. of the House Comm. on Energy and Commerce (Nov. 19, 2003), *available at* http://www.ftc.gov/os/2003/11/031119swindletest.shtm.

242. *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 STAN. TECH. L. REV. 2, 24, *available at* http://stlr.stanford.edu/pdf/walker-information-exchange.pdf. (indicating that "[l]egislators should consider the reality of regulatory costs and the resulting contraction of services and opportunities before . . . they act. As shown by the FTC's Advisory Committee on Access and Security, the issues created by even seemingly simple rules quickly grow complicated when set against the extraordinarily wide variety of information exchange practices that run throughout modern society.").

243. *See* ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY, FED. TRADE COMM'N, FINAL REPORT, Statement of Daniel E. Geer, Jr., *available at* http://www.ftc.gov/acoas/papers/individual_statements.pdf (pointing out that, although it is natural that "[s]tern rules create stern costs," if "these stern costs tax day-to-day operation rather than taxing exception handling, then the sterner those rules are the fewer will be the entities that can bear the overhead").

Several laws and regulations already exist under which the FTC has authority to conduct rulemaking and file enforcement actions for data security breaches. These laws and regulations include the Commission's Safeguards Rule[244] under Title V of the Gramm-Leach-Bliley Act,[245] which contains data security requirements for financial institutions,[246] and the Fair Credit Reporting Act (FCRA),[247] which "includes certain diligence requirements for consumer reporting agencies and safe disposal obligations for companies that maintain consumer report information."[248]

While each of these laws applies to specific, narrowly defined industries, this existing legislation can provide guidance for the type of legislation that Congress might enact to give the FTC authority to proceed against entities not currently covered by the GLB or FCRA for data security breaches.

A recent report from the President's Identity Theft Task Force[249] recommends that Congress establish "a national standard imposing safeguards requirements on all private entities that maintain sensitive consumer information."[250] It further recommends that "[c]oordinated rulemaking authority under the Administrative Procedure Act should be given to the FTC [and other federal agencies] to implement the national standards," and that the agencies be given enforcement authority of the standards "against entities under their respective jurisdictions."[251]

Currently, four bills remain pending in Congress that relate to data security breach notification.[252] These include: (1) H.R. 836, the Cyber-Security Enhancement and Consumer Data Protection Act of 2007;[253] (2) H.R. 958, the Data Accountability and Trust Act;[254] (3) S. 239, the Notification of Risk of Personal Data Act;[255] and (4) S. 495, the Personal Data Privacy and Security Act of 2007.[256] Each of these bills would establish a national law governing data security breach notification obligations and would preempt state notification laws.

---

244. Standards for Safeguarding Consumer Information, 16 C.F.R. pt. 314 (2007).
245. The entities covered by the GLB are defined and identified in 15 U.S.C. § 6809, including financial institutions. 15 U.S.C. § 6809 (3) (2000).
246. *See* 15 U.S.C. § 6801(a), (b)(1-3) (2000) (listing obligatory safeguards for financial institutions to implement to protect their customers' nonpublic personal information).
247. 15 U.S.C. §§ 1681-1681x.
248. Parnes Testimony, *supra* note 165, at 4-5 (internal citations omitted).
249. Task Force Report, *supra* note 178.
250. *See id.* at 35 (recommending standards to provide "clarity and predictability for businesses and consumers").
251. *Id.* at 37.
252. New bills will undoubtedly be introduced, and existing bills amended or abandoned. However, these bills are useful exemplars of the types of federal security breach notification legislation currently being proposed.
253. Cyber-Security Enhancement and Consumer Data Protection Act of 2007, H.R. 386, 110th Cong. (2007).
254. Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007).
255. Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007).
256. Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007).

Three of the four bills (S. 239, S. 495, and H.R. 958), as currently written, would give the FTC responsibility to establish guidelines for data security breach notification. However, none of these bills currently address the FTC's jurisdiction to take action against entities that experience data security breaches, or the rules the Commission should apply in determining when to take such action.

If Congress intends the FTC to become the primary agent for data security breach notification regulations, it is only natural that it also provide specific guidance for when the Commission can take enforcement actions against companies for such breaches.

A. The Gramm-Leach-Bliley Act as a Model for Data Security Breach Legislation

The primary purpose of the Gramm-Leach-Bliley Act[257] was to remove restrictions that prevented the merger of certain types of financial institutions.[258] The Act contained a number of provisions requiring financial institutions to implement measures to secure customer personal information against unauthorized access, use, or disclosure.[259] The Act requires financial institutions to provide privacy notices that explain their information-sharing practices.[260] Financial institutions must also inform their customers of the right to "opt-out" if they do not want their information shared with certain nonaffiliated third parties.[261] Finally, the Act requires financial institutions to safeguard the security and confidentiality of customer information.[262] It is these latter provisions that are relevant to this discussion.

The Act provides that information security standards established by the FTC must include various safeguards to protect against both "unauthorized access to" and the "use of" customer information in a manner that could result in "substantial harm or inconvenience to any customer."[263] The FTC has authority to enforce the privacy provisions.[264]

---

257. 15 U.S.C. § 6801(a)-(b)(1)-(3) (2000).
258. *See id.* § 6809 (identifying the entities covered by the GLB).
259. Lydia Parnes, Acting Dir., FTC Bureau of Consumer Protection, Remarks before the IAPP, The FTC and Consumer Privacy: Onward and Upward 8 (Oct. 28, 2004), *available at* www.ftc.gov/speeches/parnes/041028conprivparnes.pdf [hereinafter Parnes Remarks].
260. 15 U.S.C. § 6802(a).
261. *Id.* § 6802(b)(1)(A)-(C).
262. *Id.*
263. *Id.* § 6801(b)(3).
264. *Id.* §§ 6805(a)-(d), 6822(a).

The Safeguards Rule[265] requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including:

> A. Designat[ing] one or more employees to coordinate [the] information security program;
>
> B. Identifyi[ng] reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information . . . and assessing the sufficiency of any safeguards in place to control these risks;
>
> C. Design[ing] and implement[ing] information safeguards to control the risks [identified] through risk assessment, and regularly test[ing] or otherwise monitor[ing] the effectiveness of the safeguards' key controls, systems, and procedures;
>
> D. Overseei[ng] service providers . . . and requiring [them] by contract to [protect the security and confidentiality of customer information]; and
>
> E. Evaluat[ing] and adjust[ing] [the] information security program in light of the results of testing and monitoring . . . changes to [the business operation, and other relevant circumstances].[266]

It appears that the Commission, in the absence of more specific legislation, is looking to the Safeguards Rule for guidance in filing complaints against non-financial institutions for data security breaches. As noted by Lydia Parnes, an FTC director:

> Although the Safeguards Rule only applies to financial institutions, it serves as a useful guide for good information security practices in all industries. Indeed, the final orders in our four information security cases draw on the requirements of the Rule and, conversely, if the businesses followed the requirements of the Rule, they would not have faced the FTC law enforcement actions.[267]

More recently, FTC Chairman Majoras stated, "The consent orders settling these cases have required the companies to implement appropriate information security programs that generally conform to the standards that

---

265. 16 C.F.R. § 314.3 (2007).

266. *Id.*

267. Parnes Remarks, *supra* note 259; *see also* Parnes Testimony, *supra* note 165, at 7-8 ("The FTC Safeguards Rule promulgated under the GLB Act serves as a good model of this approach . . . . It also is a flexible and adaptable standard that accounts for the fact that risks, technologies, and business models change over time, and that a static technology-based standard would quickly become obsolete and might stifle innovation in security practices. The Commission will continue to apply the "reasonable procedures" principles in enforcing existing data security laws.").

the Commission set forth in the GLBA Safeguards Rule."[268] Chairman Majoras specifically requested that Congress extend the existing Safeguards Rule to non-financial institutions.[269]

While it remains undoubtedly tempting for the Commission to unilaterally adopt the Safeguards Rule in connection with its enforcement actions against non-financial institutions, thereby avoiding the time and effort required to conduct new rulemaking, it is inappropriate to do so. Financial institutions are already heavily regulated by the federal government,[270] unlike retailers and other organizations that might come under this new legislation. The Safeguards Rule was adopted after lengthy rulemaking[271] and the review of myriad submissions from interested parties.[272] The Safeguards Rule was specifically tailored to the financial industry and its concerns. Entities outside the financial industry were not involved in that rulemaking process and had no input into that process.

While the Safeguards Rule may provide important insights into the issues that new rules aimed at non-financial institutions should address, it would be a mistake to simply reenact the Safeguards Rule without going through a formal rulemaking process, which will allow a complete analysis of where non-financial institutions may differ from financial institutions in terms of security procedures and how the rules need to be tailored to

---

268. Prepared Statement of the FTC Before the Senate Comm. on Commerce, Sci. and Transp., Data Breaches and Identity Theft 5 (June 16, 2005), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf. *But see supra* note 140 and accompanying text (indicating that this statement is at odds with an earlier statement by the Commission indicating that it might go beyond the substantive requirements of the Safeguards Rule under certain circumstances).

269. Prepared Statement, *supra* note 268, at 7 ("The Commission recommends that Congress consider whether companies that hold sensitive consumer data, for whatever purpose, should be required to take reasonable measures to ensure its safety. Such a requirement could extend the FTC's existing GLBA Safeguards Rule to companies that are not financial institutions."); *see also id.* at 9-10 ("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."). *Accord* GAO, PERSONAL INFORMATION: KEY FEDERAL PRIVACY LAWS DO NOT REQUIRE INFORMATION RESELLERS TO SAFEGUARD ALL SENSITIVE DATA, HIGHLIGHTS FROM GAO-06-674, A REPORT TO THE COMM. ON BANKING, HOUSING AND URBAN AFFAIRS, U.S. SENATE 56, *available at* http://www.gao/gov/new.items/d06674.pdf.

270. Financial institutions are regulated by myriad federal agencies, including the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Securities Exchange Commission, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Office of Thrift Supervision, as well as comparable state agencies.

271. *See* Standards for Safeguarding Customer Information, 66 Fed. Reg. 41,162 (Aug. 7, 2001) (codified at 16 C.F.R. pt. 314); *see also* Privacy of Customer Financial Information—Security, 65 Fed. Reg. 54,186 (Sept. 7, 2000) (codified at 16 C.F.R. pt. 313).

272. *See* Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,484 (May 23, 2002) (codified at 16 C.F.R. pt. 314) (noting that the Commission received thirty comments in response to the Advanced Notice of Proposed Rulemaking and forty-four comments in response to its Notice of Proposed Rulemaking).

address those differences. Without that rulemaking process, it seems impossible for anyone to predict how similar or how different the final rules will be from the Safeguards Rule.

For example, numerous internationally recognized standards in the information technology industry exist that could be adopted, either in whole or in part, as part of the rulemaking process. These standards could provide the "reasonable" information security measures the FTC is looking for. These standards include:

> 1. International Standards Organization—ISO 17799. This standard consists of a comprehensive set of controls comprising best practices in information security and forms an internationally recognizable generic information security standard . . . .
>
> 2. International Standards Organization—ISO 27001. This standard focuses on data security and requires that a company strictly follow a set of stringent business practices and policies that have been developed to facilitate data security and systems uptime, limit vulnerabilities, mitigate risks and perform other steps to ensure data security.
>
> 3. National Institute of Standards and Technology—NIST Advanced Encryption Standard. This standard specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data.
>
> 4. NIST Electronic Authentication Guideline (Special Publication 800-63). This publication, along with OMB E-Authentication Guidance (OMB 04-04), provide technical guidance on how to implement e-authentication. The publication covers topics including: providing a model for e-authentication, registration and identity proofing, authentication protocols and technical requirements. This publication also adopts the OMB's four-level system which rates the consequences of authentication errors and misuse of credentials.
>
> 5. NIST Information Security Handbook (Special Publication 800-100). This publication provides wide-ranging information on various aspects of information security . . . . It also provides guidance for facilitating a more consistent approach to information security programs throughout the federal government. This publication states that it can be used by CIOs and CSOs in a variety of fields to construct security requirements for their company.
>
> 6. Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures,

> network architecture, software design and other critical protective measures. This comprehensive standard is intended to help companies to proactively protect customer account data . . . .
>
> 7. BITS—Financial Institution Shared Assessments Program—Standardized Information Gathering (SIG). This program was designed to create a standardized approach to obtaining consistent information about a service provider's information technology practices and controls. It consists of a questionnaire and a set of executable tests, both designed to document a service provider's ability to actively manage information security controls. It is supposed to be used by financial institutions to assess the information security policies of the companies to which they have outsourced functions, however it can be utilized more broadly as it provides useful questions and document requests companies can request from service providers.[273]

Adopting an internationally recognized standard, or at least basing its new rules on one or more of these standards, would provide companies with a much more specific set of guidelines for compliance than the vague "adequacy" standard currently being used by the Commission.

B. Proposed Statutory Language

Legislation to implement regulations on information security breaches and provide for FTC enforcement of those regulations can be proposed as a stand alone law or as part of another bill, such as one that requires entities to notify customers of an information security breach. As noted above,[274] a number of currently pending federal bills exist that would give the FTC authority to develop regulations regarding data security breach notifications and to enforce those regulations. It may make sense to amend one or more of those pending bills to address the FTC's authority to develop and enforce regulations concerning data security breaches as well.

---

273. John B. Kennedy & Anne E. Kennedy, *What Went Wrong? What Went Right? Corporate Responses to Privacy and Security Breaches*, 903 PLI/Pat 11, 29-31 (PLI June-July 2007); *see also* NAT'L INST. OF STANDARDS AND TECH., FED. INFORMATION PROCESSING STANDARD PUB. 199, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFO. SYSTEMS (Feb. 2004); NAT'L INST. OF STANDARDS AND TECH., FED. INFO. PROCESSING STANDARD PUB. 200, MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS (Mar. 2006); NAT'L INST. OF STANDARDS AND TECH. SPECIAL PUB. 800-53, RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS (Feb. 2005); NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUB. 800-37, GUIDE FOR THE SECURITY CERTIFICATION AND ACCREDITATION OF FEDERAL INFORMATION SYSTEMS (May 2004) (articulating other data security standards for federal computer systems that might be instructive).

274. *See supra* notes 253-56 and accompanying text.

PROPOSED LEGISLATION[275]

§ 1. Protection of Sensitive Personally Identifiable Information

(a) Privacy obligation policy – It is the policy of Congress that each business entity that collects sensitive, personally identifiable information has an affirmative and continuing obligation to respect the privacy of and protect the security and confidentiality of such information.

(b) Business Entity Safeguards – In furtherance of the policy in subsection (a) of this section, the Federal Trade Commission shall establish and enforce appropriate standards for those business entities subject to its jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

§ 2. Rulemaking.

(a)(1) Rulemaking – Not later than one (1) year after the date of enactment of this Act, the Federal Trade Commission shall promulgate regulations under section 553 of title 5, United States Code, to require each business entity subject to its jurisdiction that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information, or contracts to have any third party entity maintain such data for such person, to establish and implement policies and procedures regarding information security practices for the treatment and protection of sensitive personally identifiable information taking into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by such business entity;

(B) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and

(C) the cost of implementing such safeguards.

---

275. Portions of the following text were adapted from the GLB (15 U.S.C. § 6801(a)-(b)), the Fair Credit Reporting Act (*id.* §§ 1681a-1681s), the Telemarketing and Consumer Fraud and Abuse Prevention Act (*id.* § 6101(1)-(5)), and the proposed bills identified in *supra* notes 253-56.

In connection with subsection (B), the Commission shall take into consideration existing, generally accepted national and international information security standards, including but not limited to, ISO 17799, ISO 27001, NIST Advanced Encryption Standard, NIST Electronic Authentication Guideline (Special Publication 800-63), NIST Information Security Handbook (Special Publication 800-100), the Payment Card Industry Data Security Standard (PCI DSS), and BITS-Financial Institution Sharing Assessments Program-Standardized Information Gathering (SIG).

(2) Requirements – Such regulations shall require the policies and procedures to include the following:

(A) A security policy with respect to the collection, use, sale, other dissemination, and maintenance of such sensitive personally identifiable information;

(B) The identification of an officer or other individual as the point of contact with responsibility for the management of information security;

(C) A process for identifying and assessing any reasonably foreseeable vulnerabilities in the system maintained by such person that contains such sensitive personally identifiable information, which shall include regular monitoring for a breach of security of such system;

(D) A process for taking preventive and corrective action to mitigate against any vulnerabilities identified in the process required by subparagraph (C), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software;

(E) A process for disposing of obsolete data in electronic form containing sensitive personally identifiable information by shredding, permanently erasing, or otherwise modifying the sensitive personally identifiable information contained in such data to make such sensitive personally identifiable information permanently unreadable or undecipherable.

(3) Treatment of Entities Governed by Other Law – In promulgating the regulations under this subsection, the Commission may determine to be in compliance with this subsection any business entity that is required under any other Federal law to maintain standards and safeguards for information security and protection of sensitive personally identifiable information that provide equal or greater protection than those required under this subsection.

§ 3. Enforcement.

(a)(1) Enforcement by Federal Trade Commission – Compliance with the regulations promulgated under § 2 of this title shall be enforced under the Federal Trade Commission Act [15 U.S.C. §§ 41 et seq.] by the Federal Trade Commission with respect to any business entity under its jurisdiction that collects, stores, uses, or discloses sensitive personally identifiable information and all other persons subject thereto, except to the extent that enforcement of the requirements imposed under this title is specifically committed to some other government agencies.

(2) For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed under this title shall constitute an unfair or deceptive act or practice in commerce in violation of § 5(a) of the Federal Trade Commission Act [15 U.S.C. § 45(a)] and shall be subject to enforcement by the Federal Trade Commission under § 5(b) thereof [15 U.S.C. § 45(b)] with respect to any entity or person subject to enforcement by the Federal Trade Commission pursuant to this subsection.

(3) The Federal Trade Commission shall have such procedural, investigative, and enforcement powers, including the power to issue procedural rules in enforcing compliance with the requirements imposed under this title and to require the filing of reports, the production of documents, and the appearance of witnesses as though the applicable terms and conditions of the Federal Trade Commission Act were part of this title.

(4) Any person violating any of the provisions of this title shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though the applicable terms and provisions thereof were incorporated into and made a part of this title.

(5)

(A) In the event of a knowing violation, which constitutes a pattern or practice of violations of this title, the Commission may commence a civil action to recover a civil penalty in a district court of the United States against any person that violates this title. In such action, such person shall be liable for a civil penalty of not more than $2,500 per violation.

(B) In determining the amount of a civil penalty under subparagraph (A), the court shall take into account the degree of culpability, any history of prior such conduct,

ability to pay, effect on ability to continue to do business, and such other matters as justice may require.

(6) Notwithstanding paragraph (2), a court may not impose any civil penalty on a person for a violation of this title unless the person has been enjoined from committing the violation, or ordered not to commit the violation, in an action or proceeding brought by or on behalf of the Federal Trade Commission, and has violated the injunction or order, and the court may not impose any civil penalty for any violation occurring before the date of the violation of the injunction or order.

(7) State Law – This Act shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this Act, and then only to the extent of the inconsistency. For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter, as determined by the Federal Trade Commission.

(8) No Private Right of Action. This statute shall not be construed to provide a private right of action on any individual or entity other than the Federal Trade Commission.

§ 4. Definitions.

In this Act, the following definitions shall apply:

(a) AFFILIATE – The term "affiliate" means persons related by common ownership or by corporate control.

(b) BUSINESS ENTITY –The term "business entity" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, venture established to make a profit, or nonprofit, and any contractor, subcontractor, affiliate, or licensee thereof engaged in interstate commerce.

(c) SECURITY BREACH—

(1) IN GENERAL – The term "security breach" means compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, acquisition of or access to sensitive personally identifiable information that is unauthorized or in excess of authorization.

(2) EXCLUSION – The term "security breach" does not include—
  (i) a good faith acquisition of sensitive personally identifiable information by a business entity, or an employee or agent of a business entity, if the sensitive personally identifiable information is not subject to further unauthorized disclosure; or
  (ii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements.

(d) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION – The term "sensitive personally identifiable information" means any non-public information or compilation of information, in electronic or digital form that includes—

(1) an individual's first and last name or first initial and last name in combination with any 1 of the following data elements:
  (i) A non-truncated social security number, driver's license number, passport number, or alien registration number.
  (ii) Any 2 of the following:
    (I) Home address or telephone number.
    (II) Mother's maiden name, if identified as such.
    (III) Month, day, and year of birth.
  (iii) Unique biometric data such as a fingerprint, voiceprint, retina or iris image, or any other unique physical representation.
  (iv) A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value; or

(2) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value.

CONCLUSION

Identity theft remains a significant problem.[276] Data security breaches which reveal consumers' personal information are one source of the problem.[277] The question is what is the best way to deal with data security breaches.

The FTC has taken the lead in the area of online privacy. 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 § 5 of the FTC Act. More recently, the Commission began filing cases against companies that have experienced data security breaches under its unfairness doctrine.

These latest actions were seemingly filed at random,[278] without any guidelines, and without any advance notice to the respondents that their actions might violate § 5 of the FTC Act. The complaints and consent orders entered into in these cases provide limited guidance as to what a company should do (or not do) to avoid being the target of an unfairness action by the FTC if it experiences a security breach.

This Article proposes legislation that would give the Commission express authority to take action against companies that experience data security breaches, but only under well-defined regulations that the FTC would develop in collaboration with the affected industries and with input from all interested parties.

Data security and identity theft 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 procedures to provide the proper level of protection for sensitive consumer data. Enacting specific legislation, like that proposed in this Article, would go a long way toward achieving that goal.

---

276. *See* Javelin Strategy and Research, U.S. Identity Theft Losses Fall: Study (Feb. 1, 2007), http://www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study (indicating that 8.4 million Americans were the victims of identity theft last year, with total losses reaching $49 billion).

277. Identity theft can result from many different types of activities, including lost laptops, dumpster diving, theft of credit cards and individual identification, as well as data security breaches. *See supra* notes 111-20 and accompanying text.

278. For example, the largest data security breach incident ever reported involved retailer TJX Companies. It involved information on over forty-six million credit and debit cards stolen by hackers over a multiyear period. *See, e.g.*, TJX Companies, Inc., Annual Report (Form 10-K), at 8-10 (Mar. 28, 2007), *available at* http://ir.10kwizard.com/download.php?format=PDF&ipace=4772887&source=487; Press Release, TJX Companies, Inc., The TJX Companies, Inc. Victimized by Computer Systems Provides Information to Help Protect Consumers (Jan. 17, 2007). Despite this massive data loss, to date the Commission has taken no action against the company.