PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Consumer Privacy

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

July 22, 2010

[1] This written statement presents the views of the Federal Trade Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any Commissioner.

[2] Information on the FTC's privacy initiatives generally may be found at http://www.ftc.gov/privacy/index.html.

Prior to 2006, the Commission's Division of Financial Pr 8h Commi

the FTC staff's Privacy Roundtables project – a major initiative to re-examine traditional approaches to privacy protection in light of new technologies and business models. It concludes by offering general comments on both Chairman Rush's and Chairman Boucher's proposed privacy legislation.

I. The FTC's Efforts to Protect Consumer Privacy

The FTC has a long track record of protecting consumer privacy. The Commission's early work on privacy issues dates back to its initial implementation in 1970 of the Fair Credit Reporting Act ("FCRA"),[4] which includes provisions to promote the accuracy of credit reporting information and protect the privacy of that information. With the emergence of the Internet and the growth of electronic commerce beginning in the mid-1990s, the FTC expanded its focus to include online privacy issues. Since then, both online and off-line privacy issues have been at the forefront of the Commission's agenda, as discussed in greater detail below.

A. The FTC's Fair Information Practices Approach

Beginning in the mid-1990s, the FTC began addressing consumer concerns about the privacy of personal information provided in connection with online transactions. The Commission developed an approach by building on earlier initiatives outlining the "Fair Information Practice Principles," which embodied the important underlying concepts of transparency, consumer autonomy, and accountability.[5] In developing its approach, the FTC

---

[4] 15 U.S.C. §§ 1681e-i.

[5] This work included the Department of Health, Education, and Welfare's 1973 report, *Records, Computers, and the Rights of Citizens*, *available at* http://aspe.hhs.gov/datacncl/1973privacy/c7.htm, and the Organisation for Economic Cooperation and Development's 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

participate fully in that marketplace.[8]

Although Congress did not pass the legislation recommended by the Commission, the Commission's efforts during this time, particularly its surveys, reports, and workshops, were widely credited with raising public awareness about privacy and leading companies to post privacy policies for the first time.[9] The Commission also encouraged self-regulatory efforts designed to benefit consumers, such as the development of best practices, improvements in privacy-enhancing technologies, and the creation of online privacy certification programs.

The Commission also brought law enforcement actions to hold companies accountable for their privacy

---

[8] *Id.* at 36-38.

[9] In 1999, Congress also passed the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6821-27, requiring all financial institutions to provide notice of their data practices and choice for sharing data with third parties

[10] *In the Matter of GeoCities, Inc.*, Docket No. C-3850 (Feb. 5 1999) (consent order).

[11] *FTC v. Toysmart.com LLC*, 00-CV-11341-RGS (D. Mass. filed July 10, 2000). *See also In the Matter of Liberty Fin. Cos.*, Docket No. C-3891 (Aug. 12, 1999) (consent order) (alleging that site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously); *FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 10, 2000) (consent order) (alleging that online auction site obtained consumer data from competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business); *FTC v. Rennert,* No. CV-S-00-0861-JBR (D. Nev. July 24, 2000) (consent order) (alleging that defendants

misrepresented their security practices and how they would use consumer information); *In the Matter of Educ. Research Ctr. of Am., Inc.; Student Marketing Group, Inc.*, Docket No. C-4079 (May 6, 2003) (consent order) (alleging that personal data collected from students for educational purposes was sold to commercial marketers); *In the Matter of The Nat'l Research Ctr. for College & Univ. Admissions*, Docket No. C-4071 (Jun. 28, 2003) (consent order) (same); *In the Matter of Gateway Learning Corp.*, Docket No. C-4120 (Sept. 10, 2004) (consent order) (alleging that company rented customer information to list brokers in violation of its privacy policy); *In the Matter of Vision I Properties, LLC*, Docket No. C-4135 (Apr. 19, 2005) (consent order) (alleging that a service provider disclosed customer information in violation of merchant

does not fall into the hands of identity thieves and other wrongdoers.

The FTC enforces several laws with data security requirements. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act, for example, contains data security requirements for financial institutions.[13] The FCRA requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[14] and imposes safe disposal obligations on entities that maintain consumer report information.[15] In addition, the Commission enforces the FTC Act's prohibition against unfair or deceptive acts or practices in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.[16]

Since 2001, the Commission has used its authority under these laws to bring 28 cases alleging that businesses failed to protect consumers' personal information.[17] The FTC's early

---

[13] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[14] 15 U.S.C. § 1681e.

[15] *Id.*, § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[16] 15 U.S.C. § 45(a). *See, e.g., In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order) (alleging deception); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order) (alleging unfairness).

[17] *See In the Matter of Twitter, Inc.*, FTC File No. 092 3093 (June 24, 2010) (consent order approved for public comment); *In the Matter of Dave & Buster's, Inc.*, Docket No. C-4291 (Jun. 8, 2010) (consent order); *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-NVW (D. Ariz. final order filed Mar. 15, 2010); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC

(N.D. Ga. final order filed Oct. 14, 2009);

LexisNexis, and more recently, Dave & Busters and Twitter, have involved such practices as the alleged failure to: (1) comply with posted privacy policies;[20] (2) take even the most basic steps to protect against common technology threats;[21] (3) dispose of data safely;[22] and (4) take reasonable steps to guard against sharing customer data with unauthorized third parties.[23] In each case, the Commission obtained significant relief, including requiring the companies to implement a comprehensive information security program and obtain regular third-party assessments [illegible]

---

[20] *See, e.g., In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *In the Matter of MTS Inc.*, FTC Docket No. C-4110 (May 28, 2004) (consent order); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[21] *See, e.g., In the Matter of Twitter, Inc.*, FTC File No. 092 3093 (June 24, 2010) (consent order approved for public comment); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008) (consent order); *In the Matter of Reed Elsevier, Inc.*, FTC Docket No. C-4226 (July 29, 2008) (consent order).

[22] *See, e.g., FTC v. Navone*, No. 2:08-CV-001842 (final order filed D. Nev. Dec. 30, 2009); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. final order filed Jan. 28, 2008); *In the Matter of CVS Caremark Corp.*, Docket No. C-4259 (June 18, 2009).

[23] *See, e.g., United States v. Rental Research Svcs.*, No. 09 CV 524 (D. Minn. final order filed Mar. 6, 2009); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (final order filed N.D. Ga. Oct. 14, 2009).

[24] In addition, beginning with the CVS case announced last year, the Commission has begun to challenge the reasonableness of security measures to protect *employee* data, in addition to customer data. *See, e.g., In the Matter of CVS Caremark Corp.*, Docket No. C-4259 (Jun. 18, 2009) (consent order).

[25] *See, e.g., FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. final order Dec. 29, 2009); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (final order filed N.D. Ga. Oct. 14, 2009).

Development

[30] *See* The President's Identity Theft Task Force Report (2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf

implementing rule,[33] the FTC has brought 15 actions against website operators that collect information from children without first obtaining their parents' consent. Through these actions, the FTC has obtained more than $3.2 million in civil penalties.[34] The Commission is currently conducting a comprehensive review of its COPPA Rule in light of changing technology, such as the increased use of mobile devices to access the Internet.[35]

4. Unwarranted Intrusions

The Commission has also acted to protect consumers from unwarranted intrusions into their daily lives, particularly in the areas of unwanted telemarketing calls, spam, and spyware. Perhaps the Commission's most well-known privacy initiative is the Do Not Call Registry, which has been an unqualified success. The Commission vigorously enforces the requirements of the Registry to ensure its ongoing effectiveness. The FTC has brought 64 actions alleging violations of the Do Not Call Rule. These actions have resulted in $39.9 million in civil penalties and $17.7 million in consumer redress or disgorgement. During the past year, the Commission has filed several new actions that attack the use of harassing "robocalls" – the automated delivery of prerecorded messages – to deliver deceptive telemarketing pitches that promise consumers extended auto warranties and credit card interest rate reduction services.[36]

---

[33] 15 U.S.C. §§ 6501-6508; 16 C.F.R. Part 312.

[34] For a list of the FTC's COPPA cases, see http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html.

[35] In spring 2010, the FTC announced it was seeking comment on a broad array of issues as part of its review of the COPPA Rule. *See* http://www.ftc.gov/privacy/privacyinitiatives/childrens_2010rulereview.html.

[36] *See, e.g., FTC v. Asia-Pacific Telecom, Inc*, No. 10 CV 3168 (N.D. Ill., filed May 24, 2010).

[37] 15 U.S.C. §§ 7701-7713.

[38] Detailed information regarding these actions is available at http://www.ftc

issues, and international outreach.

1. Consumer and Business Education

The FTC has done pioneering outreach to business and consumers, particularly in the area of consumer privacy and data security

[42] *See* http://www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alertaen la Línea have attracted nearly 12 million unique visits.

[43] *See Protecting Personal Information: A Guide For Business*, *available at* http://www.ftc.gov/infosecurity.

[44] *See* FTC Press Release, OnGuardOnline.gov Off to a Fast Start with Online Child Safety Campaign (Mar. 31, 2010), *available at* http://www.ftc.gov/opa/2010/03/netcetera.shtm.

[45] *See* http://www.onguardonline.gov/topics/social-networking-sites.aspx

kids better understand the ads they see online and offline.[46]

2. Research and Policymaking on Emerging Technology Issues

Over the past two decades, the Commission has hosted numerous workshops to examine the implications of new technologies on privacy, including forums on spam, spyware, radio-frequency identification (RFID), mobile marketing, contactless payment, peer-to-peer file sharing, and online behavioral advertising. These workshops often spur innovation and self-regulatory efforts. For example, the FTC has been assessing the privacy implications of online behavioral advertising for several years. In February 2009, the Commission staff released a report that set forth several principles to guide self-regulatory efforts in this area: (1) transparency and consumer control; (2) reasonable security and limited retention for consumer data; (3) affirmative express consent for material retroactive changes to privacy policies; and (4) affirmative express consent for (or prohibition against) the use of sensitive data.[47] This report was the catalyst for industry to institute a number of self-regulatory advances. While these efforts are still in their developmental stages, they are encouraging. We will continue to work with industry to improve consumer control and understanding of the evolving use of online behavioral advertising.

3. International Outreach

Another major privacy priority for the FTC has been cross-border privacy and international enforcement cooperation. The Commission's efforts in this area are gaining greater

---

[46] *See* FTC Press Release, FTC Helps Prepare Kids for a World Where Advertising is Everywhere (Apr. 28, 2010), *available at* http://www.ftc.gov/opa/2010/04/admongo1.shtm.

[47] FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

importance with the proliferation of cross-border data flows, cloud computing, and on-demand data processing that takes place across national borders. To protect consumers in this rapidly changing environment, the FTC participates in various international policy initiatives, including those in multilateral organizations such as the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation forum (APEC).

In APEC, the FTC actively promotes an initiative to establish a self-regulatory framework governing the privacy of data transfers throughout the APEC region. The FTC just announced that it was one of the first participants in the APEC cross-border Privacy Enforcement Arrangement, a multilateral cooperation network for APEC privacy enforcement authorities.

In a similar vein, earlier this year, the FTC, joined by a number of its international counterparts, launched the Global Privacy Enforcement Network, an informal initiative organized in cooperation with OECD, to strengthen cooperation in the enforcement of privacy laws.

Finally, the Commission is using its expanded powers under the U.S. SAFE WEB AD ()Tj 0.0000 0.00

---

[48] Pub. L. No. 109-455, 120 Stat. 3372 (2006) (codified in scattered sections of 15 U.S.C. and 12 U.S.C. § 3412(e))

[49] Companies self-certify to the U.S. Department of Commerce their compliance with a set of Safe Harbor privacy principles. If a company falsely claims to be part of this program, or fails to abide by its requirements, the FTC can challenge such actions under its deception

alleging that seven companies falsely claimed to be part of the Framework. The orders against six of these companies prohibit them from misrepresenting their participation in any privacy, security, or other compliance program.[50] The seventh case is still in litigation.[51]

II. Lessons Learned

Although the Commission plans to continue its ongoing enforcement, policy, and education initiatives, it recognizes that the traditional models governing consumer privacy have their limitations.

The FTC Fair Information Practices model has put too much burden on consumers to read and understand lengthy 5.0000 0.0000 TD ((nth case)Tj 38.8800 0.0f8000 0.0000 .0000 Tc (See)Tj c

---

authority.

[50] *See In the Matter of Directors Desk LLC*, FTC Docket No. C-4281 (Jan. 12, 2010); *In the Matter of World Innovators, Inc.*, FTC Docket No. C-4282 (Jan. 12, 2010); *In the Matter of Collectify LLC*, FTC Docket No. C-4272 (Nov. 9, 2009); *In the Matter of ExpatEdge Partners, LLC*, FTC Docket No. C-4269 (Nov. 9, 2009); *In the Matter of Onyx Graphics, Inc.*, FTC Docket No. C-4270 (Nov. 9, 2009); *In the Matter of Progressive Gaitways LLC*, FTC Docket No. C-4271 (Nov. 9, 2009)

[51] *See FTC v. Kavarni*, Civil Action No. 09-CV-5276 (C.D. Cal. filed July 31, 2009).

[52] *See* Speech of Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Cleveland, Ohio, October 4, 2001, *available at* http://www.ftc.gov/speeches/muris/privisp1002.shtm.

[53] *See* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1, 5 (2003).

[54] *See* FTC Press Release, FTC to Host Public Roundtables to Address Evolving Privacy Issues (Sept. 15, 2009), *available at* http://www.ftc.gov/opa/2009/09/privacyrt.shtm.

[55] Similar efforts are underway around the world. For example, the OECD is preparing to review its 1980 Privacy Guidelines (*see* http://www.oecd.org/document/39/0,3343,en_2649_34255_44946983_1_1_1_1,00.html

supposedly anonymous information continue to evolve, the distinction between personally identifiable information ("PII") and non-PII is losing its significance. Thus, information practices and restrictions that rely on this distinction may be losing their relevance.

Fourth, commenters and roundtable participants noted the tremendous benefits from the free flow of information. Consumers receive free content and services and businesses are able to innovate and develop new services through the acquisition, exchange and use of consumer information. Commenters and participants noted that regulators should be cautious about restricting such information exchange and use, as doing so risks depriving consumers of benefits of free content and services.

Fifth, commenters and roundtable participants voiced concerns about the limitations of the FTC Fair Information Practices model. Many argued that the model places too high a burden on consumers to read and understand lengthy privacy policies and then ostensibly to exercise meaningful choices based on them. Some participants also called for the adoption of other substantive data protections – including those in earlier iterations of the Fair Information Practice Principles – that impose obligations on companies, not consumers, to protect privacy. Such participants argued that consumers should not have to choose basic privacy protections, such as not retaining data for long

about how their data is collected and used. Simplifying choice would address concerns that consumers bear a heavy burden in having to read and understand lengthy privacy policies, and to exercise meaningful choices based on those policies. One w

businesses on privacy. If legislation is enacted, the Commission believes that it is important that it incorporate the need for simplified disclosures at a relevant point for consumers. The FTC rulemaking authority could provide guidance for this requirement.

Second, sharing of individuals' data among companies affiliated through common ownership should not necessarily be exempt from consent requirements. As noted in the Commission's behavioral advertising report and at the Commission's roundtables, consumers often do not understand relationships between companies based on corporate control. Thus, if a company states that it does not share data with third parties, consumers may be surprised if that company shared data with dozens, or even hundreds, of affiliates.[57] The Commission suggests that any privacy

[57] *See* University of California at Berkeley, School of Information, KnowPrivacy, June 2009, at 28, *available at* http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.