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

Chairman Rush, Ranking Member Whitfield, and members of the Committee, I am David Vladeck, Director of the Bureau of Consumer Protection of the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on privacy.[1]

Privacy has been central to the Commission's consumer protection mission for more than a decade. Over the years, the Commission has employed a variety of strategies to protect consumer privacy, including law enforcement, regulation, outreach to consumers and businesses, and policy initiatives.[2] In 2006, recognizing the increasing importance of privacy to consumers and a healthy marketplace, the FTC established the Division of Privacy and Identity Protection, which is devoted exclusively to privacy-related issues.[3]

Although the FTC's commitment to consumer privacy has remained constant, its policy approaches have evolved over time. This testimony describes the Commission's efforts to protect consumer privacy over the past two decades, including its two main policy approaches: (1) promoting the fair information practices of notice, choice, access, and security (the "FTC Fair Information Practices approach"); and (2) protecting consumers from specific and tangible privacy harms (the "harm-based approach"). It then discusses recent developments, including

---

[1] This written statement represents 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.

[3] Prior to 2006, the Commission's Division of Financial Practices worked on privacy issues in addition to enforcing laws related to mortgage transactions, debt servicing, debt collection, fair lending, and payday lending. A different division was responsible for identity theft.

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 offline 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.

reviewed a series of reports, guidelines, and model codes regarding privacy practices issued since the mid-1970s by government agencies in the United States, Canada, and Europe. From this work, the FTC identified four widely accepted principles as the basis of its own Fair Information Practices approach: (1) businesses should provide **notice** of what information they collect from consumers and how they use it; (2) consumers should be given **choices** about how information collected from them may be used; (3) consumers should be able to **access** data collected about them; and (4) businesses should take reasonable steps to ensure the **security** of the information they collect from consumers. The Commission also identified **enforcement** – the use of a reliable mechanism to impose sanctions for noncompliance with the fair information principles – as a critical component of any self-regulatory program to ensure privacy online.[6]

To evaluate industry's compliance with these principles, the Commission examined website information practices and disclosures; conducted surveys of online privacy policies, commented on self-regulatory efforts, and issued reports to Congress. In 2000, the Commission reported to Congress that, although there had been improvement in industry self-regulatory efforts to develop and post privacy policies online, approximately one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security.[7] A majority of the Commission concluded that legislation requiring online businesses to comply with these principles, in conjunction with self-regulation, would allow the electronic marketplace to reach its full potential and give consumers the confidence they need to

---

[6] *See* Federal Trade Commission, Privacy Online: A Report to Congress (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23.shtm.

[7] *See* Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace (May 2000) at 13-14, *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

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 statements and practices. In February 1999, for example, the Commission alleged that GeoCities, one of the most visited websites at the time, had misrepresented the purposes for which it was collecting personal information from both children and adults.[10] In 2000, the Commission challenged a website's attempts to sell personal customer information, despite the representation in its privacy policy that such information would never be disclosed to a third party.[11] These cases stressed the importance of keeping promises about the use of

---

[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

consumer information and demonstrated the Commission's commitment to protecting online privacy.

B. The Harm-Based Approach

In the early 2000s, the FTC de-emphasized its fair information practices approach as the primary means of addressing privacy issues, and shifted its focus to a "harm-based approach" for protecting consumer privacy. The approach was designed to target harmful uses of information – those presenting risks to physical security or economic injury, or causing unwarranted intrusions in our daily lives – rather than imposing costly notice and choice for all uses of information.[12] The Commission's privacy agenda began to focus primarily on: (1) data security enforcement; (2) identity theft; (3) children's privacy; and (4) protecting consumers from spam, spyware, and telemarketing.

1. Data Security Enforcement

Maintaining and promoting data security in the private sector has been a key component of the FTC's privacy agenda. Through its substantial record of enforcement actions, the FTC has emphasized the importance of maintaining reasonable security for consumer data, so that it

---

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 privacy policies).

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

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

enforcement actions in this area addressed deceptive privacy statements – that is, the failure of companies to adhere to the promises they made to consumers regarding the security of their personal information.[18] Since 2005, the Commission has also alleged, in appropriate cases, that the failure to maintain reasonable security is an "unfair" practice that violates the FTC Act.[19]

These cases, against well-known companies such as Microsoft, ChoicePoint, CVS,

---

(N.D. Ga. final order filed Oct. 14, 2009); *In the Matter of James B. Nutter & Co.,* FTC Docket No. C-4258 (June 12, 2009) (consent order); *United States v. Rental Research Servs., Inc.,* No. 0:09-CV-00524 (D. Minn. final order filed Mar. 6, 2009); *FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. final order filed Dec. 30, 2009); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. final order Mar. 17, 2008); *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 (Jun. 18, 2009) (consent order); *In the Matter of Genica Corp.*, Docket No. C-4252 (Mar. 16, 2009) (consent order); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order); *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); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order); *In the Matter of Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008) (consent order); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006) (consent order); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006) (consent order); *In the Matter of DSW, Inc*., FTC Docket No. C-4157 (Mar. 7, 2006) (consent order); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005) (consent order); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. C-9319 (Apr. 12, 2005) (consent order); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005) (consent order); *In the Matter of MTS Inc.*, FTC Docket No. C-4110 (May 28, 2004) (consent order); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003) (consent order); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[18] *See In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003) (consent order); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[19] *See In the Matter of BJ's Wholesale Club, Inc.*, File No. 042 3160 (Sept. 20, 2005) (consent order).

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 of the effectiveness of that program.[24] In some cases, the Commission also obtained substantial monetary penalties or relief.[25] The Commission's robust enforcement actions have sent a strong signal to industry about the importance of data security, while providing guidance about how to

---

[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).

accomplish this goal.[26]

2. Identity Theft

Another important part of the Commission's privacy agenda has been protecting consumers from identity theft, which victimizes millions of consumers every year. In 1998, Congress enacted the Identity Theft Assumption and Deterrence Act ("the Act"), which provided the FTC with a specific role in combating identity theft.[27] To fulfill the Act's mandate, the Commission created a telephone hotline and dedicated website to collect complaints and assist victims, through which approximately 20,000 consumers contact the FTC every week. The FTC also maintains and promotes a centralized database of victim complaints that serves as an investigative tool for over 1,700 law enforcement agencies.

The Commission also played a lead role in the President's Identity Theft Task Force ("Task Force"). The Task Force, comprised of 17 federal agencies and co-chaired by the FTC's Chairman, was established by President Bush in May 2006 to develop a comprehensive national strategy to combat identity theft.[28] In April 2007, the Task Force published its national strategy, recommending 31 initiatives to reduce the incidence and impact of identity theft.[29] The FTC, along with the other Task Force agencies, has been actively implementing these initiatives and

---

[26] Developments in state law have also played a major role in data security. The passage of state data breach notification laws beginning in 2003 required increased transparency for companies that had suffered data breaches and thus further enhanced the Commission's data security enforcement efforts. *See, e.g.,* Cal. Civ. Code §§ 1798.29, 1798.82-1789.84 (West 2003).

[27] 18 U.S.C. § 1028 note.

[28] Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 15, 2006).

[29] *See* The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

submitted a final report in September 2008.[30] Among other things, the Commission has trained victim assistance counselors, federal and state prosecutors, and law enforcement officials; developed and published an Identity Theft Victim Statement of Rights; and worked closely with the American Bar Association on a *pro bono* legal assistance program for identity theft victims.

Finally, the Commission has worked to implement the identity theft protections of the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act").[31] Among other things, the FTC has acted aggressively to enforce consumers' right under the FACT Act to receive a free credit report every twelve months from each of the nationwide consumer reporting agencies, so they can spot incipient signs of identity theft. For example, the Commission has brought action against a company offering a so-called "free" credit report that was actually tied to the purchase of a credit monitoring service.[32]

3. Children's Privacy

The Commission has also undertaken an aggressive agenda to protect children's privacy. Since the enactment of the Children's Online Privacy Protection Act in 1998 ("COPPA") and its

---

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

[31] Pub. L. 108-159.

[32] *FTC v. Consumerinfo.com, Inc.,* SACV05-801AHS(MLGx) (C.D. Cal. final order filed Jan. 8, 2007).

To provide further clarity to consumers, Congress recently enacted legislation requiring entities that advertise "free" credit reports to disclose that such reports are available pursuant to federal law at www.annualcreditreport.com. *See* Pub. L. 111-24, *codified at* 15 U.S.C. § 1681j(g). The FTC has promulgated a rule to implement this requirement, 16 C.F.R. § 610, and this week issued eighteen warning letters to companies alleging failures to comply with the rule.

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).

In addition, since the enactment of the CAN-SPAM Act in 2003,[37] the Commission has brought dozens of law enforcement actions challenging spam, including cases involving deceptive spam, failure to honor opt-out requests, and failure to comply with requirements for adult labeling of spam messages.[38] For example, in June 2009, the FTC moved quickly to shut down a rogue Internet Service Provider ("ISP") that knowingly hosted and actively participated in the distribution of illegal spam, child pornography, and other harmful electronic content. The FTC complaint alleged that the defendant actively recruited and colluded with criminals seeking to distribute illegal, malicious, and harmful electronic content.[39] After the Commission shut down this ISP, there was a temporary 30 percent drop in spam worldwide.[40] Finally, since 2004, the Commission has brought 15 spyware cases, targeting programs foisting voluminous pop-up ads on consumers and subjecting them to nefarious programs that track their keystrokes and online activities.[41]

C. Ongoing Outreach and Policy Initiatives

While the Commission's consumer privacy models have evolved throughout the years, its activities in a number of areas have remained constant. In addition to enforcement, these include consumer and business education, research and policymaking on emerging technology

---

[37] 15 U.S.C. §§ 7701-7713.

[38] Detailed information regarding these actions is available at http://www.ftc.gov/bcp/conline/edcams/spam/press.htm.

[39] *FTC v. Pricewert, LLC*, No. 09-CV-2407 (N.D. Cal. final order issued Apr. 4, 2010).

[40] *See* Official Google Enterprise Blog, Q2 2009 Spam Trends, *available at* http://googleenterprise.blogspot.com/2009/07/q2-2009-spam-trends.html.

[41] Detailed information regarding each of these law enforcement actions is available at http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm.

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. The Commission's well-known OnGuard Online website educates consumers about threats such as spyware, phishing, laptop security, and identity theft.[42] The FTC also developed a guide to help small and medium-sized businesses implement appropriate data security for the personal information they collect and maintain.[43]

The FTC has also developed resources specifically for children, parents, and teachers to help kids stay safe online. In response to the Broadband Data Improvement Act of 2008, the FTC produced the brochure *Net Cetera: Chatting with Kids About Being Online* to give adults practical tips to help children navigate the online world.[44] In less than 10 months, the Commission already has distributed more than 3.8 million copies of its *Net Cetera* brochure to schools and communities nationwide. The Commission also offers specific guidance for certain types of Internet services, including, for example, social networking and peer-to-peer file sharing.[45] In addition, the Commission recently launched Admongo.gov, a campaign to help

---

[42] *See* http://www.onguardonline.gov. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alertaena 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 Act of 2006[48] to promote cooperation in cross-border law enforcement, including in the privacy area. The FTC has also brought a number of cases relating to the U.S.-EU Safe Harbor Framework, which enables U.S. companies to transfer personal data from Europe to the U.S. consistent with European privacy law.[49] For example, last fall, the Commission announced enforcement actions

---

[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 and complicated privacy policies and then make numerous choices about the collection and use of their data. Indeed, privacy policies have become complicated legal documents that often seem designed to limit companies' liability, rather than to inform consumers about their information practices.

The harm-based model has principally focused on financial or other tangible harm rather than the exposure of personal information where there is no financial or measurable consequence from that exposure.[52] Yet there are situations in which consumers do not want personal

---

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.

information to be shared even where there may be no risk of financial harm. For example, a consumer may not want information about his or her medical condition to be available to third-party marketers, even if receiving advertising based on that condition might not cause a financial harm. In addition, some have criticized the harm-based model as being inherently reactive – addressing harms to consumers after they occur, rather than taking preventative measures before the information is collected, used, or shared in ways that are contrary to consumer expectations.[53]

In addition, there are questions about whether these models can keep pace with the rapid developments in such areas as online behavioral advertising, cloud computing, mobile services, and social networking. For example, is it realistic to expect consumers to read privacy notices on their mobile devices? How can consumer harm be clearly defined in an environment where data may be used for multiple, unanticipated purposes now or in the future?

III. The FTC Privacy Roundtables

To explore the privacy challenges posed by emerging technology and business practices, the Commission announced late last year that it would examine consumer privacy in a series of public roundtables.[54] Through these roundtables, held in December 2009, and January and March 2010, the Commission obtained input from a broad array of stakeholders on existing approaches, developments in the marketplace, and potential new ideas.[55]

---

[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); the European Commission is undertaking a review of the 1995 Data Protection Directive (*see*

The roundtables generated significant public interest. Over 200 representatives of industry, consumer groups, academia, and government agencies participated in the roundtables, and the Commission received over 100 written comments.

Several common themes emerged from these comments and the roundtable discussions. First, consumers do not understand the extent to which companies are collecting, using, aggregating, storing, and sharing their personal information. For example, as evidence of this invisible data collection and use, commenters and panelists pointed to enormous increases in data processing and storage capabilities; advances in online profiling and targeting; and the opaque business practices of data brokers, which are not understood by consumers. In addition, as commenters noted, consumers rarely realize that, when a company discloses that it shares information with affiliates, the company could have hundreds of affiliates.

Second, commenters and panelists raised concerns about the tendency for companies storing data to find new uses for that data. As a result, consumers' data may be used in ways that they never contemplated.

Third, commenters and roundtable participants pointed out that, as tools to re-identify

---

http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm); and the International Data Protection Commissioners' Conference released a set of draft privacy guidelines (*see* http://www.privacyconference2009.org/dpas_space/Resolucion/index-iden-idphp.php). The FTC is closely following these international developments, recognizing that the market for consumer data is becoming increasingly globalized and consumer data is more easily accessed, processed, and transferred across national borders.

In addition, following the FTC roundtables, the Department of Commerce also held a workshop and issued a Notice of Inquiry on the related subject of privacy and innovation, in which the FTC has submitted a comment. *See In the Matter of Privacy and Innovation in the Information Economy*, Docket No.100402174-0175-01, Comments of the Federal Trade Commission (June 2008), *available at* http://www.ftc.gov/os/2010/06/100623ntiacomments.pdf.

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 longer than it is needed, that should be built into everyday business practices.

Sixth, many commenters called upon the Commission to support a more expansive view of privacy harms that goes beyond economic or tangible harms. There are some privacy harms, these participants argued, that pose real threats to consumers – such as exposure of information about health conditions or sexual orientation – but cannot be assigned a dollar value.

Finally, many participants highlighted industry efforts to improve transparency for

consumers about the collection and use of their information. At the same time, commenters questioned whether the tools are consistent and simple enough for consumers to embrace and use effectively.

IV. The Proposed Legislation

Chairman Rush and Chairman Boucher have each proposed legislation to advance the goal of improving privacy protections in the commercial marketplace. The Commission shares the goal of protecting consumer privacy and appreciates the opportunity to comment on the proposed legislation. Both legislative proposals include some key policy objectives that the Commission supports. For example, both proposals include requirements for reasonable data security for customer information, a measure which the Commission has long encouraged, as described above. The Commission also supports the proposals' data accuracy requirements, especially where the data will be used for decisions about consumers' eligibility for important benefits and services.

Further, both proposals give the FTC limited rulemaking authority under the Administrative Procedures Act (APA).[56] If Congress enacts privacy legislation, the Commission agrees that such legislation should provide APA rulemaking authority to the Commission. In particular, at the FTC's privacy roundtables, many stakeholders expressed concern about the significant difficulties associated with providing effective privacy disclosures. The content, timing, and scope of privacy disclosures required by the legislation would benefit from broad stakeholder input and consumer testing, which can be accomplished in an APA rulemaking.

Both proposals also include measures to simplify consumers' ability to exercise choice

[56] 5 U.S.C. § 552 *et seq.*

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 way to simplify choice is to recognize that consumers do not need to exercise it for certain commonly accepted business practices – those that fall within reasonable consumer expectations. For example, it is unnecessary, and even distracting, to ask a consumer to consent to sharing his or her address information with a shipping company for purposes of shipping a product that the consumer has requested. By eliminating the need to exercise choice for such practices, consumers can focus on the choices that really matter to them, and on uses of data that they would not expect when they engage in a transaction.

To this end, the proposals exempt companies from having to secure consumers' consent to share their data for "operational" or "transactional" purposes, such as fulfillment. The Commission supports this general approach, especially if it allows more meaningful consent for uses of data beyond these purposes. The challenge will be to define "operational" or "transactional" purposes in a way that tracks consumers' reasonable expectations. Commission staff would be pleased to provide technical comments on these definitions.

If Congress enacts legislation in this area, the Commission urges it to consider some additional issues that are either not addressed in one or both proposals or that we recommend be modified. First, although it is important that companies make information about their privacy practices available to consumers, the Commission believes that any disclosure should emphasize important information consumers need to make choices, at a time when the consumer is making them. Short, clear disclosures could also enable consumers to compare privacy protections offered by different companies more easily and thus could promote competition among

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. 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 legislation take this issue into consideration.

Third, the Commission has concerns about the safe harbor mechanism contained in the proposed legislation, under which the FTC could approve multiple industry-led "choice programs." One of the key themes that emerged from the privacy roundtables was the need for simplicity in the exercise of privacy choices. Creating multiple consent mechanisms that may differ in important ways risks adding to consumer confusion.

The Commission looks forward to working with Congress to address these issues and others to accomplish our shared objective of improving consumer privacy, while supporting beneficial uses of information and technological innovation.

V. Conclusion

The Commission is grateful for the opportunity to provide an overview of its activities in the privacy arena and to present these general comments on the legislative proposals. We look forward to continuing this important dialogue with Congress and this Subcommittee.

---

[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.