

Prepared Statement of
The Federal Trade Commission
“Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act,
and H.R. 1319, the Informed P2P User Act”

Before the
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
United States House of Representatives

Washington, D.C.
May 5, 2009

Chairman Rush, Ranking Member Radanovich, and members of the Subcommittee, I am Eileen Harrington, Acting Director of the Bureau of Consumer Protection at the Federal Trade Commission (“FTC” or “Commission”). I appreciate the opportunity to present the Commission’s testimony on data security and peer-to-peer (“P2P”) file-sharing technology, and to provide the Commission’s thoughts on proposed legislation in both these areas.¹

As the nation’s consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. Since 2001, the Commission has brought 25 law enforcement actions that challenged businesses that allegedly failed to adequately protect consumers’ personal information. These cases emphasize the importance of protecting against common security threats and the need for businesses to evaluate their security procedures on an ongoing basis. Additionally, through extensive consumer and business education, the Commission has promoted the importance of data security.

Similarly, since 2004, the FTC has worked to address the risks to consumers presented by P2P file-sharing software programs through three key efforts. First, FTC staff have worked with industry to improve the disclosure of risk information so that consumers can make informed choices regarding their use of P2P file-sharing programs. Second, the FTC has brought law enforcement actions related to P2P file-sharing programs. Finally, the agency has taken steps to educate consumers about the risks associated with these programs.

This testimony describes the Commission’s efforts in both areas. Part one of the testimony discusses the Commission’s data security program. First, it summarizes the Commission’s law enforcement actions to protect the security of consumers’ data. Second, it

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.

highlights key recommendations, rulemakings, and reports issued by the Commission. Third, it discusses the Commission's consumer and business education efforts and fourth, it describes initiatives to address emerging challenges in the data security area. Finally, it provides the Commission's views on H.R. 2221.

Part two of the Commission's testimony discusses the agency's work involving P2P file-sharing technology. First, it describe FTC staff's efforts to assist P2P file-sharing application developers to devise best practices to help prevent consumers from inadvertently sharing sensitive data over P2P networks. Second, it describes the Commission's efforts to educate consumers about the potential risks for downloading and using P2P file-sharing software. Finally, it discusses the Commission's views on H.R. 1319.

I. Data Security

Privacy has been one of the Commission's highest consumer protection priorities for more than a decade. The FTC has worked to address privacy issues through law enforcement, regulation, consumer and business education, and policy initiatives.² For example, the FTC has promulgated and enforced the Telemarketing Sales Rule ("TSR");³ helped to maintain and enforce the Do Not Call Registry⁴ to respond to consumer complaints about unsolicited and unwanted telemarketing; waged a multi-faceted war on identity theft;⁵ brought numerous

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

³ 16 C.F.R. Part 310.

⁴ The Do Not Call Registry was established by amendments to the TSR. *Id.* Information on the Do Not Call Registry, which is enforced by the FTC, the Federal Communications Commission, and the states, is available at <http://www.ftc.gov/donotcall>.

⁵ Information for consumers, businesses, law enforcement, and others, is available at the FTC's Identity Theft web site at <http://www.ftc.gov/bcp/edu/microsites/idtheft>.

enforcement actions to reduce the incidence of spam and spyware;⁶ and conducted numerous workshops and other research to examine privacy issues raised by emerging technologies and business practices.⁷ In 2006, the FTC established the Division of Privacy and Identity Protection, a division devoted exclusively to privacy-related issues.

A critical component of privacy is data security. If companies do not protect the sensitive consumer information that they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Accordingly, the Commission has undertaken substantial efforts to promote data security in the private sector.⁸

A. Law Enforcement

To promote data security through law enforcement, the Commission brings actions against businesses that fail to implement reasonable security measures to protect sensitive

⁶ For a list of spyware cases, *see* http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm. For spam cases, *see* www.ftc.gov/bcp/online/edcams/spam/press.htm.

⁷ *See, e.g.*, Federal Trade Commission, Comment Request, 73 Fed. Reg. 37,457 (Jul. 1, 2008) (notice of consumer research regarding consumer interaction with credit reporting agencies following incident of identity theft, and request for comments).

⁸ The Commission also has participated in efforts to promote data security in the public sector. For example, the Chairman of the FTC co-chaired the President's Identity Theft Task Force, through which 17 federal agencies worked together to develop a strategic plan to combat identity theft. Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 10, 2006). The Task Force made specific recommendations to improve data security in the public sector. Pursuant to these recommendations, the Office of Management and Budget worked to educate all federal agencies on improving data security practices and is monitoring their performance in doing so. In addition, the Office of Personnel Management led an interagency initiative to eliminate unnecessary uses of Social Security numbers ("SSNs") in federal government human resource functions, while individual agencies are eliminating unnecessary uses of SSNs in other aspects of their work. For more information about the Task Force, *see infra* note 41.

consumer data. The FTC enforces several laws and rules that contain data security requirements. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, contains data security requirements for financial institutions.⁹ The Fair Credit Reporting Act ("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,¹⁰ and imposes safe disposal obligations on entities that maintain consumer report information.¹¹ In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices¹² 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.

⁹ 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.

¹⁰ 15 U.S.C. § 1681e.

¹¹ *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

¹² 15 U.S.C. § 45(a).

Since 2001, the Commission has used its authority under these laws to bring 25 cases against businesses that allegedly failed to protect consumers' personal information.¹³ These cases stand for several general principles.

First, businesses that make claims about data security should be sure that they are accurate. The Commission has brought several cases against companies that allegedly misrepresented their own security procedures. In actions against Microsoft,¹⁴ Petco,¹⁵ Tower Records,¹⁶ Life is good,¹⁷ and Premier Capital Lending,¹⁸ for example, the FTC challenged

¹³ See *United States v. Rental Research Svcs.*, No. _____ (D. Minn. Mar. 5, 2009); *Federal Trade Commission v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of CVS Caremark Corporation*, File No. 072 3119 (Feb. 19, 2009) (accepted for public comment); *In the Matter of Genica Corp.*, File No. 082 3113 (Feb. 5, 2009) (accepted for public comment); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008); *In the Matter of Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

¹⁴ *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002).

¹⁵ *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005).

¹⁶ *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004).

claims on the companies' websites that each had strong security procedures in place to protect consumer information. The FTC alleged that, contrary to these claims, the companies did not employ even the most basic security measures.

Second, businesses should protect against common technology threats. In a number of cases, the Commission has alleged that companies failed to protect their customer information from a simple and well-known type of attack – an SQL injection – designed to install hacker tools on the companies' computer networks.¹⁹ In addition, the Commission announced two cases last year – against retailer TJX and data brokers Reed Elsevier and Seisint – alleging that these companies failed to implement simple technologies to counteract certain basic security threats. For example, the Commission alleged that TJX failed to encrypt personal data being transmitted over various computer networks; did not limit wireless access to its networks; and failed to use readily-available security measures, such as firewalls, updated anti-virus software, and strong passwords.²⁰ Similarly, the Commission alleged that Reed Elsevier and Seisint failed to prevent unauthorized access to sensitive data because they allowed easy-to-guess passwords; failed to

¹⁷ *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008).

¹⁸ *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008).

¹⁹ *See, e.g., In the Matter of Genica Corp.*, File No. 082 3113 (Feb. 5, 2009) (accepted for public comment); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007).

²⁰ *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (Jul. 29, 2008).

require periodic changes of passwords; failed to suspend credentials after a certain number of unsuccessful log-in attempts; and allowed users to store credentials in vulnerable formats.²¹

Third, businesses must know with whom they are sharing customers' sensitive information. One of the Commission's most well-known security cases involved ChoicePoint, which sold 160,000 consumer files to identity thieves posing as clients. In its complaint, the Commission alleged that ChoicePoint lacked reasonable procedures to verify the legitimacy of its customers.²²

Fourth, businesses should not retain sensitive consumer information that they do not need. In cases announced against BJ's Warehouse,²³ DSW Shoe Warehouse,²⁴ and CardSystems Solutions,²⁵ for example, the Commission alleged that the companies stored unencrypted, full magnetic stripe information on payment cards²⁶ unnecessarily – long after the time of the transaction, when the companies no longer had a business need for the information. As a result, when thieves gained access to the companies' systems, they were able to obtain hundreds of thousands – in some cases millions – of credit card numbers and security codes.

²¹ *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (Jul. 29, 2008).

²² *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006).

²³ *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sep. 20, 2005).

²⁴ *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006).

²⁵ *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sep. 5, 2006).

²⁶ Magnetic stripe information is particularly sensitive because it can be used to create counterfeit credit and debit cards that appear genuine in the authorization process.

Finally, businesses should dispose of sensitive consumer information properly. One of the Commission’s most recent cases – against CVS Caremark – illustrates this principle.²⁷ In that case, the Commission alleged that CVS Caremark failed to implement reasonable and appropriate procedures for handling personal information about customers and employees, particularly with respect to its practices for disposing of such information. The FTC’s action followed media reports that CVS Caremark pharmacies across the country were throwing trash that contained, among other things, pill bottles with patients’ names, medication instruction sheets with personal information, and payroll information, into open dumpsters. The FTC coordinated its investigation and settlement with the Department of Health and Human Services, which announced a separate agreement in which the company agreed to pay a \$2.25 million fine.²⁸

Some of these cases involved unfair or deceptive practices under the FTC Act, while others were brought under the GLB Act and the related Safeguards Rule or the FCRA. Although the Commission has brought its cases under different laws, all of the cases stand for the principle that companies must maintain reasonable and appropriate measures to protect sensitive consumer information.²⁹

²⁷ *In the Matter of CVS Caremark Corporation*, File No. 072 3119 (Feb. 19, 2009) (accepted for public comment).

²⁸ The FTC also has brought recent cases involving mortgage companies’ improper disposal of sensitive customer financial information. *See Federal Trade Commission v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007).

²⁹ What is “reasonable” will depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue. The principle recognizes that there cannot be “perfect” security, and that data breaches can occur even when a company maintains reasonable precautions to prevent them. At the same time,

B. Rulemakings and Recommendations

The Commission's efforts in the data security area also include rulemakings, reports, and recommendations to Congress. This testimony highlights four of these efforts.

First, a few weeks ago, the Commission issued a proposed rule that would require consumers to be notified when the security of their health information is breached.³⁰ The proposed rule arises from a mandate in the recently-enacted American Recovery and Reinvestment Act of 2009 (the "Recovery Act")³¹ designed to address new types of web-based entities that collect or handle consumers' sensitive health information. These entities include (1) those that offer personal health records ("PHRs"), which consumers can use as an electronic, individually-controlled repository for their medical information, and (2) online applications through which consumers can track and manage different kinds of information in their PHRs.³² These innovations have the potential to provide numerous benefits for consumers, but only if consumers have confidence that the security of their health information will be maintained.³³

companies that put consumer data at risk can be liable even in the absence of a known breach. The Commission will continue to apply the "reasonable procedures" principle in enforcing existing data security laws.

³⁰ See 74 Fed. Reg. 17,914 (Apr. 20, 2009). The Commission is accepting public comments through June 1, 2009, and will issue an interim final rule by August 17, 2009.

³¹ American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, __Stat.__.

³² For example, consumers can connect a device such as a pedometer to their computers and upload miles traveled into their personal health records.

³³ The Commission's proposed rule is part of a broader scheme set forth in the Recovery Act to address the privacy and security concerns raised by PHRs. Specifically, the Act requires the Department of Health and Human Services ("HHS") to do a study and report, in consultation with the FTC, on potential privacy, security, and breach notification requirements for PHR vendors and related entities that are not covered by the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) ("HIPAA"). In the interim, the

Consistent with the Recovery Act, the proposed rule requires PHR vendors and related entities to provide notice to consumers following a breach. The proposed rule further provides that if a service provider to one of these entities experiences a breach, it must notify the entity so that the entity can in turn notify consumers. The proposed rule contains additional requirements governing the standard for what triggers notice; the timing, method, and content of notice; and notice to the FTC and HHS.

Second, the Commission in 2007 issued the Red Flags Rule, which requires businesses and organizations to detect and respond to “red flags” or signs of identity theft. The Red Flags Rule picks up where data security leaves off: It seeks to ensure that, in addition to protecting data collected from consumers, covered entities are on the lookout for signs of identity theft or attempted identity theft.³⁴ The Red Flags Rule follows from a mandate in the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”)³⁵ that the FTC, the Federal bank regulatory agencies, and the National Credit Union Administration jointly develop rules and guidelines for “financial institutions” and “creditors” to reduce the incidence and impact of identity theft.

The Red Flags Rule and accompanying guidelines require financial institutions and creditors that hold certain consumer accounts, or other accounts for which there is a reasonable

Act requires the Commission to issue a temporary breach notification rule (the proposed rule) applicable to these entities. The Act also requires HHS to promulgate final breach notification requirements for entities subject to HIPAA. Because many of the breach notification requirements applicable to FTC-regulated entities are the same as those applicable to HHS-regulated entities, the FTC is consulting with HHS to harmonize the agencies’ rules.

³⁴ 16 C.F.R. § 681.2.

³⁵ Pub. L. 108-159. The FACTA amended the Fair Credit Reporting Act (“FCRA”), 15 U.S.C. § 1681 *et seq.*

risk of identity theft, to develop and implement a written “Identity Theft Program” to help spot identity theft. In recent months, the FTC staff has undertaken substantial outreach efforts to educate financial institutions and creditors about the Rule.³⁶

Third, a critical component of maintaining data security is limiting the unnecessary use and display of Social Security numbers (“SSNs”), which can be particularly valuable to those seeking to perpetrate identity theft or other privacy harms. Last December, the Commission issued a report containing two key legislative recommendations to address this issue.³⁷ It recommended that Congress consider establishing national consumer authentication standards. This recommendation recognizes that the first step to minimizing the role of SSNs in identity theft is to make it more difficult for thieves to use them to open new accounts, access existing accounts, or obtain other benefits or services. Thus, the Commission recommended that Congress require private sector entities to establish reasonable procedures to authenticate new or existing customers to ensure that they are who they say they are.³⁸ Moreover, the report recommended that Congress consider creating national standards to reduce the public display and transmission of SSNs.

³⁶ This outreach has included developing a compliance guide for businesses, distributing general and industry-specific articles, speaking before numerous audiences, responding to individual inquiries by telephone and e-mail, and working with a number of trade associations that are developing model policies or specialized guidance for their members.

³⁷ See FTC Report, “Recommendations on Social Security Number Use in the Private Sector,” (December 2008), available at <http://www2.ftc.gov/opa/2008/12/ssnreport.shtm>.

³⁸ The report recommended that this requirement cover all private sector entities that maintain consumer accounts, other than financial institutions already subject to authentication requirements promulgated by bank regulatory agencies.

Finally, the Commission more broadly has recommended that Congress enact federal legislation to enhance data security across the private sector. In particular, the Commission has recommended legislation requiring all companies that hold sensitive consumer data to take reasonable measures to safeguard it and to notify consumers when the security of their information is breached.³⁹ In addition, the Commission has recommended that Congress provide it with authority to seek civil penalties in data security cases because of the deterrent value, as equitable remedies such as disgorgement and redress are often inadequate in these cases.⁴⁰ These recommendations also were made in an April 2007 report released by the President's Identity Theft Task Force, which was co-chaired by the Attorney General and the FTC Chairman,⁴¹ as well as in the report on SSNs described above.

³⁹ See Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, United States Senate, 109th Cong. (Jun. 16, 2005), available at <http://www.ftc.gov/os/2005/06/050616databreaches.pdf>.

⁴⁰ *Id.* See also Prepared Statement of the Federal Trade Commission Before the Subcomm. on Interstate Commerce, Trade, and Tourism of the S. Comm. on Commerce, Science, and Transportation Committee, 110th Cong. (Sep. 12, 2007) available at <http://www.ftc.gov/os/testimony/070912reauthorizationtestimony.pdf>; Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong. (Apr. 10, 2007) available at <http://www.ftc.gov/os/testimony/P040101FY2008BudgetandOngoingConsumerProtectionandCompetitionProgramsTestimonySenate04102007.pdf>.

⁴¹ President Bush established the Task Force by Executive Order on May 10, 2006. It was comprised of 17 federal agencies and tasked with developing a comprehensive national strategy to combat identity theft. Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 10, 2006). The Task Force issued its Strategic Plan, including 31 recommended actions for preventing identity theft and mitigating its consequences, in April 2007. See The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Apr. 23, 2007, available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>. In September 2008, the Task Force issued a progress report on the implementation of the Strategic Plan recommendations, most of which have been completed. See The President's Identity Theft Task Force Report, Sep. 2008, available at <http://idtheft.gov/reports/IDTReport2008.pdf>.

C. Education

The Commission also promotes better data security practices through extensive use of consumer and business education. On the consumer education front, the Commission sponsors a multimedia website, OnGuard Online, designed to educate consumers about basic computer security.⁴² OnGuard Online was developed in partnership with other government agencies and the technology sector, and since its launch in 2005 has attracted nearly 10 million unique visits.

In addition, the Commission has engaged in wide-ranging efforts to educate consumers about identity theft, one of the harms that could result if their data is not adequately protected. For example, the FTC's identity theft primer⁴³ and victim recovery guide⁴⁴ are widely available in print and online. Since 2000, the Commission has distributed more than 9 million copies of the two publications, and recorded over 4 million visits to the Web versions. In addition, in February 2008, the U.S. Postal Service – in cooperation with the FTC – sent copies of the Commission's identity theft consumer education materials to more than 146 million residences and businesses in the United States.

The Commission recognizes that its consumer education efforts can be even more effective if it partners with local businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. For example, the Commission has launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend," which contains a consumer education kit that includes direct-to-consumer brochures,

⁴² See www.onguardonline.gov.

⁴³ *Avoid ID Theft: Deter, Detect, Defend*, available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.pdf>.

⁴⁴ *Take Charge: Fighting Back Against Identity Theft*, available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf>.

training materials, presentation slides, and videos for use by such groups. The Commission has developed a second consumer education toolkit with everything an organization needs to host a “Protect Your Identity Day.” Since the campaign launch in 2006, the FTC has distributed nearly 100,000 consumer education kits and over 26,000 Protect Your Identity Day kits.

The Commission directs its outreach to businesses as well. The FTC widely disseminates its business guide on data security, along with an online tutorial based on the guide.⁴⁵ These resources are designed to provide diverse businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. In addition, the FTC has held regional data security workshops for businesses in locations around the country, including workshops in Chicago, Los Angeles, Dallas and, just last week, New York. It also has released nine articles for businesses relating to basic data security issues for a non-legal audience. The articles have been reprinted in newsletters for local Chambers of Commerce and other business organizations.

D. Emerging Privacy and Data Security Issues

As part of its privacy program, the Commission examines new technologies and other developments to identify emerging privacy and data security issues affecting consumers. This testimony highlights three recent initiatives in this area, all of which bear on the security of consumers’ personal information.⁴⁶

⁴⁵ See www.ftc.gov/infosecurity.

⁴⁶ Other recent initiatives include, for example, a Town Hall on the privacy and security issues associated with contactless payment mechanisms and a Town Hall and staff report on mobile marketing. See Workshop Information Page, “Pay on the Go: Consumers and Contactless Payment,” available at <http://www2.ftc.gov/bcp/workshops/payonthego/index.shtml>; Workshop Information Page, “Beyond Voice: Mapping the Mobile Marketplace,” available at <http://www2.ftc.gov/bcp/workshops/mobilemarket/index.shtml>.

First, this February, the Commission staff released a report containing principles designed to serve as the basis for industry self-regulatory efforts to address the privacy and data security concerns raised by behavioral advertising.⁴⁷ Behavioral advertising is the practice of tracking an individual's online activities in order to deliver targeted advertising tailored to that individual's interests.⁴⁸ Although it may provide benefits to consumers in the form of advertising that is more relevant to their interests and the subsidization of free online content, it also raises privacy concerns. In particular, consumers may be uncomfortable about being tracked. Further, without adequate safeguards, consumer tracking data – which sometimes includes sensitive data about children, health, or a consumer's finances – could fall into the wrong hands or be used for unanticipated purposes.

To address these concerns, the FTC staff principles provide for transparency, consumer control, and reasonable security for consumer behavioral data. They also call for companies to obtain affirmative express consent from consumers before they (1) use data in a manner that is materially different than promised at the time of collection; and (2) collect and use “sensitive” consumer data for behavioral advertising. Staff will continue to examine this marketplace and take actions to protect consumers as appropriate.

⁴⁷ See Press Release, “FTC Staff Revises Online Behavioral Advertising Principles,” Feb. 12, 2009, available at <http://www2.ftc.gov/opa/2009/02/behavad.shtm>.

⁴⁸ An example of how behavioral advertising might work is as follows: a consumer visits a travel website and searches for airline flights to New York City. The consumer does not purchase any tickets, but later visits the website of a local newspaper to read about the Washington Nationals baseball team. While on the newspaper's website, the consumer receives an advertisement from an airline featuring flights to New York City.

Second, the Commission recognizes that, as more data flows across geographic borders, protecting that data will require international cooperation. In March 2009, FTC staff held a two-day international conference titled “Securing Personal Data in the Global Economy.”⁴⁹ The conference was co-organized with the Asia-Pacific Economic Cooperation forum and the Organisation for Economic Co-operation and Development. It addressed how companies can manage data security in a global environment where data can be stored and accessed from multiple jurisdictions. The Commission will continue to partner with international organizations and its foreign counterparts to maintain data security across borders without restricting information flows that benefit consumers.

Third, the FTC is examining the practice of cloud computing, which is defined broadly as the provision of internet-based computer services. Cloud computing allows businesses and consumers to use software and hardware located on remote networks operated by third parties. Because cloud computing reduces the need for businesses and consumers to purchase software and hardware themselves, it may be a less costly way for them to manage, store, and use data. Although cloud computing is still an emerging business model, the Commission is seeking to understand its privacy and data security implications for consumers. The Commission also is considering a petition submitted by the Electronic Privacy Information Center in March 2009 raising data security concerns about Google’s provision of cloud services to consumers.⁵⁰

⁴⁹ See Workshop Information Page, “Securing Personal Data in the Global Economy,” available at <http://www2.ftc.gov/bcp/workshops/personaldataglobal/index.shtm>.

⁵⁰ See EPIC Complaint Before the Federal Trade Commission, In the Matter of Google, Inc., and Cloud Computing Services, Mar. 19, 2009, available at <http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf>.

E. H.R. 2221.

Finally, the Commission appreciates the opportunity to comment on H.R. 2221. The Commission strongly supports the goals of the legislation to require companies to (1) implement reasonable security policies and procedures and (2) provide notification to consumers when there is a security breach. The Commission also supports the legislation's provisions that would give the Commission the authority to obtain civil penalties for violations.⁵¹

The Commission would like to make two recommendations in particular at this time. First, the Commission recommends that the proposed legislation not be limited to security of *electronic* information, because the breach of sensitive data stored in paper format can be just as harmful to consumers.⁵² In addition, the data broker provisions of the proposed legislation establish a procedure for customers to obtain access to and dispute information held by a broker. The Commission believes it is important to ensure that these provisions (1) are compatible with, and do not displace, the protections afforded to consumers under the FCRA; and (2) are targeted to uses of information that raise concerns for consumers and are not already covered by the FCRA.⁵³ The Commission looks forward to working with Congress on this legislation.

⁵¹ As noted above, these provisions are consistent with prior Commission legislative recommendations.

⁵² According to one recent survey, a significant number of breaches involve paper documents. See Ponemon Institute, *Security of Paper Documents in the Workplace*, (Oct. 2008), available at <http://www.ponemon.org/data-security>.

⁵³ Data brokers that collect and sell data to third parties for purposes of making eligibility decisions about consumers - most notably for credit, insurance, or employment - would generally be consumer reporting agencies subject to the access and correction provisions of the FCRA. See 15 U.S.C. § 1681 *et seq.*

II. Peer-to-Peer File Sharing

Since 2004, the FTC has worked to address the risks to consumers presented by P2P file-sharing software programs. In that time, FTC staff has worked with industry to improve the disclosure of risk information on P2P file-sharing software web sites, brought law enforcement actions related to P2P file-sharing,⁵⁴ and taken steps to educate consumers about risks associated with the software. In December 2004, the FTC held a public workshop to consider the consumer protection, competition, and intellectual property issues raised by P2P file-sharing. The workshop featured more than forty representatives from the P2P file-sharing software industry, entertainment industry, high-technology research firms, government agencies, academic institutions, and consumer groups. In June 2005, the FTC released a staff report based on the information received in connection with the workshop.⁵⁵

A. Reducing Sensitive Information on P2P Networks

Although P2P technologies make possible significant operational benefits to computing, provide individual users with easy and fast access to content, and enable new business models, they have been associated not only with copyright piracy but also with significant data security risks. Indeed, recent headlines have highlighted disturbing instances of sensitive documents

⁵⁴ *FTC v. Cashier Myricks Jr.*, Civ. No. CV05-7013-CAS (FMOx) (C.D. Cal., filed Sep. 27, 2005) (suit against the operator of the web site MP3DownloadCity.com for making allegedly deceptive claims that it was “100% LEGAL” for consumers to use the file-sharing programs he promoted to download and share music, movies, and computer games); *FTC v. Odysseus Marketing, Inc.*, Civ. No. 05-330 (D.N.H., filed Sep. 21, 2005) (suit against the operator web site that encouraged consumers to download free software that they falsely claimed would allow consumers to engage in anonymous P2P file-sharing).

⁵⁵ *P2P File-Sharing Technology: Consumer Protection and Competition Issues*, Federal Trade Commission Staff Report (June 2005), available at www.ftc.gov/reports/p2p05/050623p2prpt.pdf.

being shared via P2P networks. These have included documents disclosing avionics details of the President's helicopter, financial information of a Supreme Court Justice, and many thousands of tax returns and medical records of ordinary citizens. Sensitive documents may become available on P2P networks because they have been inadvertently shared by consumers and businesses using file-sharing software, or because of malware. Regardless of how this information makes its way to the networks, the Commission is working to reduce its availability by: coordinating with the P2P technology industry to implement safeguards to minimize inadvertent file sharing; initiating law enforcement investigations against companies that fail to take reasonable and appropriate measures to prevent sensitive data from being shared on P2P networks; and educating consumers and businesses about the risks associated with using P2P file-sharing programs and other online activities so that they can better protect themselves.

B. Reasonable and Appropriate Security Measures

Organizations that maintain sensitive consumer data have a duty to protect the data, and that includes taking reasonable and appropriate measures to prevent the sensitive data from exposure on P2P networks. P2P file-sharing applications that connect computers to open file-sharing networks are not likely to be appropriate to install on computers used to store and access sensitive documents. Businesses responsible for the confidential information of others must have in place procedures to control effectively the ability of their employees and contractors to install such applications on computers with sensitive information, and should educate their employees and contractors about safe computing and data-handling practices. The FTC is investigating instances where companies may have exposed, through P2P software, the sensitive data of thousands of consumers.

C. Protections Against Inadvertent File Sharing – Industry Best Practices and Developments

FTC staff has taken an active role in assisting P2P file-sharing software developers in devising best practices to help prevent consumers from inadvertently sharing personal or sensitive data over P2P networks. In July 2008, the Distributed Computing Industry Association (“DCIA”) published Voluntary Best Practices containing useful safeguards against inadvertent file sharing. These safeguards, which apply to the functionality of the software programs themselves, include: warnings to application users and notices about the number and types of files being shared; default settings that limit what is shared upon installation of an application; controls for users to stop sharing any file or folder; protections against any user attempt to share sensitive folders or file types; and simple means to disable the file-sharing functionality. Starting in February 2009, DCIA members began providing the FTC staff with reports outlining the ways in which they believe their applications comply with the best practices. FTC staff is currently assessing, with the assistance of an independent P2P technology expert, whether the member companies’ applications, and those of other developers, comply with those best practices.

Even prior to DCIA publishing its “best practices” document, FTC staff observed some improvements in P2P application interface design that should help to protect many consumers against inadvertent sharing of personal documents. Following the Committee’s previous hearing in July 2007, Lime Wire implemented safeguards in its user interface to reduce the risk that users would inadvertently share documents likely to contain sensitive, personal information. For example, as of spring 2008, users of new versions of the LimeWire application could not share their entire hard drives. Warnings would appear to deter users from sharing a “My Documents” folder, and default settings would prevent the sharing of sensitive file types such as word

processing documents and PDFs. Independent experts hired by the FTC⁵⁶ concluded that even though the interface could still be improved, Lime Wire had provided safer defaults and enhanced protections against inadvertent sharing of user-originated files.⁵⁷ Those safeguards appear to have been carried through to, or improved upon in, the current version of the LimeWire application.⁵⁸

D. Consumer Education

In February 2008, the FTC updated its consumer alert entitled, “P2P File-Sharing: Evaluate the Risks.”⁵⁹ The alert warns consumers about the potential risks from downloading and using P2P file-sharing software, including the risk of inadvertently sharing files or receiving spyware, viruses, infringing materials, or unwanted pornography mislabeled as something else. The alert recommends that consumers carefully set up the file-sharing software so that they do not open access to information on their hard drives such as tax returns, e-mail messages, medical records, photos, or other personal documents.

In addition, the FTC’s Internet education web site, OnGuardOnline.gov, contains downloadable information about the risks of P2P file-sharing software, including quick facts about P2P file-sharing, an interactive quiz, and additional lessons, resources, and activities from

⁵⁶ The FTC contracted with Dr. Nathaniel Good and Aaron Krekelberg, experts on human-computer interface design in P2P file-sharing applications. Good and Krekelberg wrote the widely-cited article, *Usability and Privacy: a Study of KaZaA P2P File-Sharing* (2003).

⁵⁷ User-originated files are those stored on the user’s computer that were not downloaded from the P2P network.

⁵⁸ We recognize that P2P technologies have often been misused for copyright infringement itself, a matter that is outside our bailiwick.

⁵⁹ Available at www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt128.shtm.

i-SAFE, an organization involved in Internet-safety education.⁶⁰ In addition to providing information on topics such as P2P file-sharing, social networking, identity theft, phishing, spyware, and spam, OnGuardOnline features up-to-date articles from the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), including a piece entitled "Risks of File Sharing." OnGuardOnline has had nearly ten million unique visits since its launch. The Commission is pleased to report that some file-sharing software distributors are providing links to the FTC's consumer education materials on P2P file sharing.

E. Legislative Steps to Address Inadvertent File Sharing

Although many P2P file-sharing program developers have voluntarily implemented safeguards against the risk of inadvertent sharing of user-originated files in current versions of their programs, the FTC is supportive of legislation that mandates distributors of P2P file-sharing programs provide timely, clear, and conspicuous notice and obtain consent from consumers regarding the essential aspects of those programs. In this regard, H.R. 1319 may provide useful protections for consumers. It permits the FTC to obtain civil penalties against the distributors who do not meet a baseline standard of providing clear and conspicuous notice, in advance, to consumers about what files a P2P program will share, and for obtaining consent from consumers before making those files available on a P2P network. The proposed legislation also has provisions that should help network administrators keep P2P file-sharing applications that are inappropriate and potentially dangerous off their computer systems and would give the Commission authority to seek civil penalties for violations. The agency has worked with

⁶⁰ See www.onguardonline.gov.

Committee staff on previous versions of the bill and looks forward to working with Committee staff regarding the proposed legislation.

Conclusion

The FTC is committed to ensuring the security of consumers' personal information and will continue to assess the risks associated with P2P file-sharing technology. The FTC thanks this Subcommittee for focusing attention on these important issues, and for the opportunity to describe how the agency has most recently addressed them.