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

[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 mar000 [illegible] 515.6400 TDe

[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/conline/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 practices in cases where a business makes f in case

[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).

[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.

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

ovd toai400 TD(pe of a)Tj000 TD(ts200 TD(t w)Tj15e of a)Tj000 TDTD(pe of a)Tj000 TDr5t w

[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 cards[26] 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(e)Tj2800 0.0000 TD(re)p. 5,ble

---

[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

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 con

[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," (De

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 we

[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.

[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*

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.

See Workshop Information Pag

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 F0.

[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.

processing documents and PDFs. Independent experts hired by the FTC[56] 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.

[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.