COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to
THE FEDERAL TRADE COMMISSION
Notice of Proposed Routine Use; Request for Public Comment
Privacy Act of 1974; System of Records: FTC File No. P072104

By notice published on March 29, 2007, the Federal Trade Commission ("FTC") requested public comment on a proposed routine use permitting disclosure of FTC records governed by the Privacy Act of 1974 in cases of data security breach.[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to urge the Commission to narrow the scope of the exemption proposed and to notify the affected individual of the security breach before disclosure to any other entity.

Introduction

EPIC is a non-profit public interest research organization founded in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, free speech and constitutional values. For many years, EPIC has played a leading role on the issues related to data security, breach notification and enforcement of the Privacy Act of 1974. EPIC has testified before Congress, filed Federal Trade Commission complaints, and submitted comments to federal agencies urging the adoption of stronger privacy laws, security protections, and more effective technologies that would safeguard the personal and financial privacy of individuals.[2]

---

[1] Fed. Trade Comm'n, *Privacy Act of 1974; System of Records: Proposed routine use; request for public comment*, 72 Fed. Reg. 14,814 (Mar. 29, 2007) ["FTC Public Comment Notice"], *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/E7-5821.htm.

[2] *See* Marc Rotenberg, Exec. Dir., EPIC, *Testimony at a Joint Hearing on Social Security Numbers & Identity Theft, Before the H. Fin. Serv. Subcom. on Oversight & Investigations and the H. Ways & Means Subcom. on Social Security*, 104th Cong. (Nov. 8, 2001), *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Letter from Chris Jay Hoofnagle, Assoc. Dir., EPIC, and Daniel J. Solove, Assoc. Professor, George Washington Univ. Law Sch., to Fed. Trade Comm'n, Dec. 16, 2004, *available a*t http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that federal agencies could collect and required agencies to be transparent in their information practices.[3] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[4]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[5] It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[6] It thus sought to

---

(complaint to the FTC on databroker Choicepoint's questionable business practices and their potential effects on consumer privacy); Chris Jay Hoofnagle, Senior Counsel, EPIC, *Testimony at Hearing on Data Security: The Discussion Draft of Data Protection Legislation Before the Subcom. on Commerce, Trade, & Consumer Protection of the H. Comm. on Energy & Commerce*, 108th Cong. (July 29, 2005), *available at* http://epic.org/privacy/choicepoint/datasec7.28.05.html; Marc Rotenberg, Exec. Dir., EPIC, *Prepared Testimony and Statement for the Record at a Hearing on Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Ac, Before the H. Commerce Comm.*, 110th Cong. (Mar. 9, 2007), *available at* http://www.epic.org/privacy/iei/roten_hcom0307.pdf; EPIC*, Comments to the Federal Trade Commission on ID Workshop: Comment, P075402* (Mar. 23, 2007), *available at* http://www.epic.org/privacy/id_cards/epic_ftc_032307.pdf.

[3] S. Rep. No. 93-1183 at 1 (1974).

[4] *Doe v. Chao*, 540 U.S. 614, 618 (2004).

[5] S. Rep. No. 93-1183 at 1.

[6] Pub. L. No. 93-579 (1974).

"provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[7] Adherence to these requirements is critical for the Federal Trade Commission, as its decisions on consumer privacy affect every individual in the United States.

I. Exemption Must Be Narrowed to Minimum Required To Fulfill Its Purpose

The proposed routine use exemption covers a vast amount of data. The vague standards for disclosure of the data to a variety of agencies and personnel are not stringent enough to ensure the protection of the personal data disclosed. The exemption must be narrowed. This Privacy Act exemption is being proposed "for purposes of response and remedial efforts in the event of a breach of data contained in the protected systems."[8] The FTC must restrict the amount of data disclosed, and the number of people that the data is disclosed to, to the minimum necessary to fulfill the stated reason for this proposed exemption.

In January 2007, EPIC submitted comments to the Identity Theft Task Force that emphasized the need to establish better privacy and security practices to reduce the risk of identity theft, rather than simply expand law enforcement authority.[9] "The best long-term approach to the problem of identity theft is to minimize the collection of personal information and to develop alternative technologies and organizational practices," EPIC explained.[10] We were surprised, then, to read the Task Force's final report. It focused more on how to expand law enforcement authority to combat identity theft *after* the crime has been committed, than on creating stronger privacy and security practices to reduce

---

[7] *Id*.
[8] FTC Public Comment Notice at 14,815, *supra* note 1.
[9] EPIC, *Comments to the Federal Identity Theft Task Force, P065410* (Jan. 19, 2007), *available at* http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf.
[10] *Id*. at 19.

the risk of identity theft being committed.[11] The risk that we identified in the original recommendations to the federal Identity Theft Task Force will be exacerbated if the agency is permitted to share widely personal data with others that facilitated the crime of identity theft.

This routine use proposed by the FTC continues that misguided emphasis on expanding law enforcement authority in the context of identity theft crimes. According to the FTC, this routine use "will apply to all FTC records systems covered by the Privacy Act of 1974. The Act applies to agency systems of records about individuals that the agency maintains and retrieves by name or other personal identifier, such as its personnel and payroll systems and certain other FTC records systems."[12] If any or all of these systems are breached, then personal data protected by the Privacy Act will be disclosed "to such agencies, entities, and persons is reasonably necessary to assist in connection with the FTC's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm."[13] This could include employees in federal, state and local agencies, federal and state contractors and other commercial entities.

In its proposal to create this routine use exemption from the Privacy Act, the FTC does not propose specific standards or requirements to follow in case of a breach that would necessitate disclosure under this routine use. Rather, the FTC seeks the power to disclose data protected by the Privacy Act to the vague groups that the FTC finds "reasonably necessary to assist" the agency in "in connection with" its response to security breaches, that are "suspected or confirmed." It should not be that a data breach,

---

[11] President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (Apr. 2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf, http://www.idtheft.gov/reports/VolumeII.pdf.
[12] FTC Public Comment Notice at 14,815, *supra* note 1.
[13] *Id.*

or suspected breach, entitles even more people to view the personal data of the individuals affected by the security breach. Such mass disclosure is especially questionable in light of the financial nature of the data involved. Would the entire case file, including Social Security Numbers and credit card information, be released to all the "agencies, entities, and persons" that the FTC finds "reasonably necessary to assist" in its investigations?

In response to a security breach, some specific disclosures of certain information to other agencies for a particular purpose might be necessary. However, identity theft is a crime of opportunity. It results from the failure of organizations to adopt privacy and security practices that safeguard personal information. Minimizing the risk of identity theft is therefore most effectively achieved by reducing opportunities for the compromise of personal information. The Federal Trade Commission must narrow the scope of this routine use exemption. The FTC could create tiers of access, allowing specific categories of individuals limited access to the data, according to the needs of the investigation.

II. FTC Must Notify the Affected Individuals First

The consumer harm that results from the wrongful disclosure of personal information is very clear. For the seventh year in a row, identity theft is the No. 1 concern of U.S. consumers, according to the Federal Trade Commission's annual report.[14] More than 153 million data records of U.S. residents have been exposed due to security breaches since January 2005, according to a report from the Privacy Rights Clearinghouse.[15] Therefore, it is imperative that consumers be notified as soon as

[14] Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.
[15] Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm.

possible after a security breach results in their personal information being accessed by an unauthorized person. The FTC must create a policy where it informs the individual affected of the security breach before notifying any other agency, entity or individual.

There have been numerous instances where agencies or other entities have delayed notification to the consumers affected in a data breach. Often law enforcement, and other agencies and entities are told of the security compromise long before the individual affected. Sometimes the delay is blamed on law enforcement personnel. For example, almost 46 million credit and debit card numbers were stolen by hackers who accessed the computer systems at the TJX Companies over a period of several years, making it the biggest breach of personal data ever reported.[16] The computer system breaches began in July 2005 but weren't discovered until December 2006 – the financial data of millions were exposed for 17 months.[17] Breach notification to the consumers affected was delayed by the company until January 17, 2007, which meant consumers could not attempt to minimize or prevent harm from the disclosure until then.[18]

Last May, an information security breach by a Department of Veterans Affairs employee resulted in the theft from his Maryland home of unencrypted data affecting 26.5 million veterans, active-duty personnel, and their family members.[19] The laptop and an external hard drive contained unencrypted information that included millions of Social Security numbers, disability ratings and other personal information.[20] Though Maryland police began investigating the theft the day it occurred, May 3, and the FBI stepped in on

[16] TJX Cos., Annual Report (Form 10-K), at 8-10 (Mar. 28, 2007), *available at* http://ir.10kwizard.com/download.php?format=PDF&ipage=4772887&source=487.
[17] *Id.* at 7.
[18] Press Release, TJX Companies, The Tjx Companies, Inc. Victimized By Computer Systems Intrusion; Provides Information To Help Protect Customers (Jan. 17, 2007).
[19] *See* EPIC's Page on the Veterans Affairs Data Theft, http://www.epic.org/privacy/vatheft/.
[20] Statement, Dep't of Veterans Affairs, A Statement from the Department of Veterans Affairs (May 22, 2006).

May 17, the 26.5 million people affected were not notified until May 22, almost three weeks after their personal data was compromised.[21]

EPIC recommends that the FTC notify individuals affected immediately, before informing any other entity. In the rare event that law enforcement needs to delay consumer notification, this delay should be limited to no more than seven days, and should require formal notification to the agency head. Breach notification allows consumers the opportunity to minimize or prevent the occurrence of actual identity theft following a data breach. For example, a consumer can freeze his or her credit or carefully monitor credit records for possible identity theft once he or she has been notified that a data breach has occurred.[22] Consumers have the right to protect their personal and financial data; the FTC must allow them to do so. And it would be absurd to adopt a rule in a Privacy Act rulemaking that would permit a federal agency to widely disseminate personal information across the federal government directly implicating ongoing risks to a known individual without actually notifying the individual.

Conclusion

In its Federal Register notice, the FTC said it "believes that failure to take reasonable steps to help prevent, minimize the harm that may result from such a breach or compromise would jeopardize, rather than promote, the privacy of such individuals." We agree. In order to prevent and minimize the harm to consumers from a security breach, the FTC must notify the individual affected before disclosure to any other entity and the FTC must narrow the scope of the proposed Privacy Act exemption. The FTC must

---

[21] *Id.*

[22] Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, SECURING PRIVACY IN THE INTERNET AGE (2005), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=650162.

restrict the amount of data disclosed, and the number of people that the data is disclosed to, to the minimum necessary and notify the individual at risk as soon as possible or else the agency will jeopardize, rather than promote, the privacy of affected individuals.

Respectfully submitted,

_____

Marc Rotenberg
Executive Director

_____

Melissa Ngo
Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140