FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

January 23, 2015

To: Subcommittee on Commerce, Manufacturing, and Trade Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "What are the Elements of Sound Data Breach Legislation?"

On Tuesday, January 27, 2015, at 10:00 a.m. in room 2123 of the Rayburn House Office Building, the Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing titled "What are the Elements of Sound Data Breach Legislation?"

I. BACKGROUND

Public reports of data breaches have become increasingly common. Since 2005, the Privacy Rights Clearinghouse has identified more than 932 million records containing consumers' personal information that have been compromised as a result of more than 4,400 data breaches.[1] According to the Online Trust Alliance, over 90 percent of data breaches in the first half of 2014 could have been prevented had businesses implemented security best practices.[2]

Data breaches can severely compromise the financial well-being of individuals. Breaches can also threaten individual privacy, particularly if sensitive information pertaining to health, children, or location is accessed. For example, after the recent breach of Sony Pictures Entertainment thousands of internal documents were publicly released. These documents included private e-mails, detailed performance reviews for hundreds of employees, a list of all employees who were fired or laid off in 2013 and the reasons they were let go, employee

---

[1] Privacy Rights Clearinghouse, *Chronology of Data Breaches* (online at www.privacyrights.org/data-breach#CP) (accessed Jan. 16, 2015).

[2] Online Trust Alliance, Security and Privacy Enhancing Best Practices (Jan. 21, 2015) (online at www.otalliance.org/system/files/files/resource/documents/ota2015-bestpractices.pdf).

criminal background checks, salary negotiations, and doctors' letters explaining the medical rationale for leaves of absence.[3]

A wide array of entities have experienced data breaches, including information brokers, colleges and universities, retailers, financial institutions, and government agencies.[4] Breaches occur due to a variety of causes, including hacking, lost or stolen computing equipment, dishonest insiders, improper storage and disposal of paper records, and simple negligence.[5] Commercial data breaches can also occur through state-affiliated cyberattacks designed to harm national defense capabilities or obtain trade secrets.[6]

Currently, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach notification laws.[7] In 2002, California became the first state to pass a data breach law.[8] California's law, which has since been used as a model for many other states' laws, requires notification when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[9] Data breach laws vary, sometimes significantly from state to state, but generally contain provisions regarding the following elements: (1) who must comply with the law; (2) a definition of "personal information" and "breach of security;" (3) what constitutes a breach; (4) requirements for breach notification; (5) exemptions and safe harbors; and (6) penalties, enforcement authorities, and remedies.[10]

II. LEGISLATIVE EFFORTS IN PREVIOUS CONGRESSES

Currently, there is no comprehensive federal law that requires all companies that hold consumer's personal information to implement reasonable measures to protect that data. There is

---

[3] *The Cyberattack on Sony Pictures Made Employees Collateral Damage*, Washington Post (Dec. 3, 2014) (online at www.washingtonpost.com/blogs/the-switch/wp/2014/12/03/the-cyberattack-on-sony-pictures-made-employees-collateral-damage/).

[4] Privacy Rights Clearinghouse, *Chronology of Data Breaches* (online at www.privacyrights.org/data-breach#CP) (accessed Jan. 16, 2015).

[5] Verizon Enterprise Solutions RISK Team, *2014 Data Breach Investigations Report* (online at www.verizonenterprise.com/DBIR/2014/) (accessed Jan. 19, 2015).

[6] *Id*.

[7] National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 12, 2015) (online at www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

[8] Gina Stevens, *Data Security Breach Notification Laws*, Congressional Research Service (Apr. 10, 2012) (R42475).

[9] *Id*.; Cal. Civil Code §1798.29, 1798.80-1789.84

[10] National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 12, 2015) (online at www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

also no federal law that requires companies that experience a data breach to provide notice to those consumers whose personal information has been compromised.

A. The Data Accountability and Trust Act ("DATA")

The House of Representatives has, on a bipartisan basis, repeatedly considered enactment of federal information security and breach notification legislation. Most notably, in the 111th Congress, the House passed H.R. 2221, the Data Accountability and Trust Act, by a voice vote in December 2009. Introduced by then-Subcommittee Chairman Bobby Rush, along with Reps. Stearns, Barton, Schakowsky, and Radanovich, H.R. 2221 aimed to reduce the number of data breaches and provide new rights to individuals whose personal information is compromised when a breach occurs. The Senate, however, failed to act on the bill before the end of the 111th Congress.

H.R. 2221 contained two major requirements: (1) an entity holding data containing consumers' personal information had to adopt reasonable and appropriate security measures to protect such data; and (2) that same entity had to notify affected consumers and the Federal Trade Commission in the event of a breach unless the entity determined there was no reasonable risk of identity theft, fraud, or other unlawful conduct. In addition, the bill required information brokers to implement reasonable procedures to ensure data accuracy and provide consumers with access to information and the ability to dispute inaccurate information in certain circumstances. The bill further required companies to provide individuals with free monitoring services to detect the misuse of their personal information following a breach.

B. The Secure and Fortify Electronic (SAFE) Data Act

In the 112th Congress, the Subcommittee considered legislation known as the Secure and Fortify Electronic Data Act, or the SAFE Data Act, which was introduced as H.R. 2577 by then-Subcommittee Chairman Mary Bono Mack. The SAFE Data Act, as passed out of the Subcommittee, is markedly different in a number of key respects from the bipartisan H.R. 2221, including:

- applying information security and breach notification requirements to a limited set of data through a narrow definition of "personal information;"
- relieving covered persons from having an obligation to provide basic standards of protection for publicly available information;
- exempting cable operators from complying with the Communication Act's privacy requirements;
- narrowing the scope of those covered by the bill to businesses that collect personal information in the course of doing business;
- not including additional requirements for information brokers to protect consumers, such as requiring data accuracy, access, and dispute resolution; and

- prohibiting the FTC from promulgating rules on data minimization.

The Subcommittee held a hearing on a discussion draft of the SAFE Data Act on June 15, 2011, and forwarded the bill to the full Committee after a markup on July 20, 2011, during which Democratic members expressed several concerns.[11] The bill was not considered by the full Committee and no further action occurred on H.R. 2577 in the 112th Congress.

III. FEDERAL AGENCY AUTHORITY

A. Federal Trade Commission

The Federal Trade Commission (FTC) possesses broad jurisdiction under Section 5 of the FTC Act to prohibit "unfair or deceptive acts or practices in or affecting commerce" by a wide variety of individuals and entities.[12] The Commission also has the authority to enforce information security provisions in several statutes, including the Fair Credit Reporting Act (FCRA) at 15 U.S.C. 1681, the Children's Online Privacy Protection Act (COPPA) at 15 U.S.C. 6501, Gramm-Leach-Bliley (GLB) Act at 15 U.S.C. 6801, and the Health Information Technology (HITECH) provisions of the American Recovery and Reinvestment Act at 42 U.S.C. 17937 and 17954. In recent years, the FTC has filed complaints against and entered into settlements with several companies charged with failing to protect consumers' personal information.[13]

In addition, the FTC has specific authority related to identity theft. Under the Identity Theft Assumption and Deterrence Act of 1998, the FTC is the central clearinghouse for identity theft complaints, responsible for logging and acknowledging individuals' complaints, providing informational materials to those individuals, and referring complaints to appropriate entities, including credit reporting agencies and law enforcement.[14]

B. Federal Communications Commission

The Federal Communications Commission (FCC) is the regulatory agency for the media and telecommunications industries, including wired and wireless communications networks,

---

[11] *See* Subcommittee on Commerce, Manufacturing, and Trade, *Hearing on a Discussion Draft of H.R. __, the "Secure and Fortify Electronic Data Act,"* 112th Cong. (June 15, 2011); Subcommittee on Commerce, Manufacturing, and Trade, *Markup of H.R. 2577, the "Secure and Fortify Electronic Data Act,"* 112th Cong. (July 20, 2011).

[12] 15 U.S.C. 45(a).

[13] *See* Federal Trade Commission, *Making Sure Companies Keep Their Privacy Promises to Consumers* (online at www.ftc.gov/opa/reporter/privacy/privacypromises.shtml) (accessed Jan. 22, 2015).

[14] 18 U.S.C. § 1028.

cable and satellite TV, broadcast TV and radio, and cable set-top boxes.[15] Telecommunications companies and satellite and cable providers are subject to privacy provisions in the Communications Act and corresponding regulations.[16] In contrast to the FTC, which generally is limited to enforcement authority, the FCC has both regulatory and enforcement authority. The FCC efforts in this area are focused on the protection of customers' personal information that is uniquely available to communications providers through the operation of their networks.

IV. WITNESSES

Jennifer Glasgow
Global Privacy and Public Policy Executive
Acxiom Corporation

Elizabeth Hyman
Executive Vice President, Public Advocacy
CompTIA

Brian Dodge
Executive Vice President, Communications and Strategic Initiatives
Retail Industry Leaders Association

Woodrow Hartzog
Associate Professor
Cumberland School of Law
Samford University

[15] Jennifer Tatel, *et al.*, *The FCC's Role in Mobile Privacy: FCC Privacy Regulation "101,"* IAPP Global Privacy Summit (Mar. 6, 2014) (online at privacyassociation.org/media/presentations/14Summit/S14_FCC_Role_Privacy_PPT.pdf).

[16] 47 U.S.C. §§ 222 (telecommunications carriers), 338 (satellite carriers), and 551 (cable operators).