KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

CDT ISSUE BRIEF ON FEDERAL DATA BREACH NOTIFICATION LEGISLATION

January 27, 2015

A September 2014 Ponemon study found that 60% of U.S. companies have experienced more than one data breach in the past two years, and that data breaches increased in frequency over the past year.[1] This report, in addition to news of hacks into major retail chains', entertainment studios' and banks' databases, underscores the need for stronger laws that mandate both breach notification procedures and measures to avoid breaches before they occur. Nearly every state has a data breach law that incorporates notification and security provisions.[2] Last Congress saw the introduction of multiple bills that would create a federal standard for data security and breach notification. However, those bills offered wildly divergent approaches to breach notification and security law.

The following issue brief will outline CDT's recommendations for federal data breach legislation. The brief will begin with an overview on what principles should (and should not) guide federal legislation, and will follow with a discussion of the elements that should be included in any data breach proposal.

I. Guiding Principles

We support creating federal data breach legislation, so long as it goes beyond existing protections to include new safeguards. Federal legislation must:

1. **First, do no harm:** Consumer protection law and state data breach notification laws already require reasonable data security and notice to consumers of data breaches. Federal legislation shouldn't replace the existing framework with weaker overall protections, like narrower notification triggers, a lack of outside scrutiny, or less robust enforcement.

2. **Provide consumers with new protections.** Legislation shouldn't stop at just breach notification and reasonable security standards. New protections, such as a broader scope of covered information, increased consumer access to data

[1] Morgan Kennedy, *Ponemon Institute Releases Second Annual Study on Data Breach Preparedness*, Inside Privacy Blog (Oct. 1, 2014), http://www.insideprivacy.com/data-security/data-breaches/ponemon-institute-releases-second-annual-study-on-data-breach-preparedness/?utm_source=twitterfeed&utm_medium=twitter.

[2] *Data Breach Charts,* BakerLaw.com, http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf (last visited Jan. 26, 2015).

broker records, and explicit security and security program requirements, are needed to ensure that consumer protections evolve with technology.

3. **Provide stronger incentives** to companies to safeguard personal information. Current laws typically don't place monetary consequences on companies who fail to use reasonable security, apart from the costs of breach notification (most FTC security enforcement cases have resulted in zero fines[3]). New legislation must offer incentives — both positive reinforcements and negative consequences — to encourage better security.

4. **Don't prevent states from innovating** on privacy protection. Federal legislation that broadly preempts existing state data security and breach laws would be a massive step backwards in securing American consumers' data. States need the flexibility to enforce general purpose consumer protection statutes, and should be able to pass specific legislation, including breach notification legislation, on categories of data not covered by federal law.

II. Specific Elements of Federal Data Breach and Security Proposals

Legislators have started drafting national proposals for data breach law to respond to the current patchwork of federal privacy legislation regulating some sectors and not others. Multiple bills were introduced in the last Congress, including:

- The Data Security and Breach Notification Act (Rockefeller, D-WV)[4]
- The Personal Data Protection and Breach Accountability Act (Blumenthal, D-CT)[5]
- The Data Security and Breach Notification Act (Toomey, R-PA)[6]
- The Personal Data Privacy and Security Act (Leahy, D-VT) and accompanying House Bill H.R. 3990 (Shea-Porter, D-NH)[7]
- The Data Security Act (Carper, D-DE, and Blunt, R-MO)[8], and
- The Data Accountability and Trust "DATA" Act (Rush, D-IL)[9].

Additionally, President Obama revealed a data breach legislative proposal, The Personal Data Notification & Protection Act, in January 2015.[10] All this attention highlights how important this issue is – however, in order to be truly effective, any federal data breach law or provision within a comprehensive privacy law should, at a. minimum, include:

---

[3] *Legal Resources,* FTC.gov, http://www.business.ftc.gov/legal-resources/29/35 (last visited Jan. 26, 2015).

[4] The Data Security and Breach Notification Act, S. 1976, 113th Cong. (2014).

[5] The Personal Data Protection and Breach Accountability Act, S. 1995, 113th Cong. (2014).

[6] The Data Security and Breach Notification Act, S. 1193, 113th Cong. (2013).

[7] The Personal Data Privacy and Security Act, S. 1897, 113th Cong. (2014).

[8] The Data Security Act, S. 1927, 113th Cong. (2014).

[9] The Data Accountability and Trust "DATA" Act, H.R. 4400, 113th Cong. (2014).

[10] Press Release, The White House, FACT SHEET: Safeguarding American Consumers & Families (Jan. 12, 2015) (on file with author).

- **Appropriately scoped preemption:** All of the aforementioned bills allow for varying degrees of federal preemption of state law relating to data protection and breach notification.[11]We agree with this measure, so long as (a) the substantive protections are sufficiently robust and (b) states are allowed to iterate to provide new protections for otherwise unregulated data. Having multiple and inconsistent rules on when and how to notify of a breach would be confusing and difficult for companies to implement. We don't, however, believe in federal preemption of state laws beyond the specific information covered in the bill. If a state wants to protect information not addressed by the federal law (such as medical records or other sensitive personal information), it must be allowed to. Overly broad provisions preempting privacy and security generally would hinder state legislators' ability to develop laws that best serve their constituents. Similarly, some preemption provisions are worded so broadly that they could be interpreted to interfere with state legal prohibitions on deceptive and unfair practices such as general purpose state consumer protection laws. These laws should be explicitly excluded from preemption.

- **A broad definition of covered information:** Breach notification bills originally were developed to inform consumers about the exposure of financial information, which could result in fraud. However, some states have expanded notification laws to cover other types of personal information, including non-financial online accounts. As consumers store more and more personal information in the cloud, businesses should let them know if those accounts get hacked — even if financial fraud isn't at risk. Recent controversies around illegitimate access to personal photos (iCloud) and emails (Sony) prove that people want and expect good security for all their personal information. Breach notification laws should be expanded to keep up with that expectation.

- **No requirement of objective "harm":** Many recently introduced bills exempt companies from the notification requirement if they do not identify a specific harm that has or will result from the breach. For example, S. 1897 creates a safe harbor for companies if its risk assessment produces no "significant risk that a breach has resulted in, or will result in, identity theft, economic loss or harm, or physical harm to affected individuals."[12] Similarly, S. 1976 would exempt companies from the notification obligation if it establishes that the breach poses "no reasonable risk of identity theft, fraud, or other unlawful conduct."[13]

  Requiring notification only in the event that a specific "harm" has been observed would undermine a federal breach notification regime. One primary purpose of data breach notification is to reduce the number of breaches by incentivizing companies to improve their data security practices. Restricting their analyses of what constitutes "risk" to pre-determined harms would significantly diminish this incentive by excusing notification requirements in many if not most data breach incidents.

[11] *Id.*

[12] The Personal Data Privacy and Security Act, S. 1897, 113th Cong. (2014).

[13] The Data Security and Breach Notification Act, S. 1976, 113th Cong. (2014).

This could also prevent consumers from being informed of breaches that, although not linked to particular harm, still pose a risk of data misuse or embarrassment. A harm standard makes little sense when applied to breaches of personal information such as photos and email. Consumers still want to know if online accounts are compromised, however, even if there is no likelihood of financial loss.

- **A "notify unless" trigger:** Any breach notification provision should require consumer notification by default unless the company makes an *affirmative determination* that there exists no serious risk that data will be illegitimately accessed or misused. This should require finding that the appropriate technical safeguards are in place to avoid unauthorized access to the data — thus incentivizing companies to fully investigate data breaches, encouraging them to get to the bottom of a breach in hopes of avoiding the costly, time-consuming and embarrassing consumer notification process. A "notify if" requirement, however — which requires notification *only* upon an affirmative finding of risk — would have the opposite effect: companies likely wouldn't investigate breaches closely for fear of finding evidence of risk that would trigger the notification obligation. Some proposed bills have appeared to adopt this "notify if" standard, only requiring consumer notification of a breach when a covered entity reasonably believes a data breach has caused or will cause identity theft or other actual financial harm.[14]

  A "notify unless" standard would effectively grant safe harbor protections to companies that choose to implement reasonable encryption protocols to safeguard personal information. Companies would be incentivized to create strong front-end data protection strategies. However companies would still have to notify consumers if the company's examination determines that the chosen safeguards are unlikely to be effective under the circumstances (such as when the encryption keys have been breached).

- **Outside scrutiny:** Companies should be required to report *all* breaches to a central regulatory authority, such as the FTC, regardless of whether it has been determined that the breach poses a risk to consumers. No formal process for review or approval of a company's determination would necessarily be required, but simply knowing that a regulatory body requires a brief explanation (and that body may respond if it noticed dangerous patterns or other concerns) will provide external accountability and push companies to be vigilant when securing consumers' data.

- **Strong enforcement:** A national enforcement standard should allow for enforcement by the FTC, state attorneys general, and consumers backed up by significant penalty authority. Today, the FTC and most states can pursue bad data security practices under the prohibition of unfair business practices found in Section 5 of the FTC Act and most state consumer protection laws. However, the FTC cannot obtain civil penalties for most data breach cases; most settlements

[14] The Data Security and Breach Notification Act, S. 1193, 113th Cong. (2013).

end with the company paying nothing.[15] The penalty should be proportionate to the company's resources and the nature of the data breach, but we do not support an arbitrary ceiling on penalties that would unfairly favor large companies with the capacity to more easily pay a sliver of revenues for bad security practices as a cost of doing business. We also support a private right of action to allow consumers to act directly without waiting for regulators to pursue bad security practices that compromise their personal information.

- **Requirement for security policies and principles:** Federal data security law should explicitly require reasonable data security practices as well as include front-end security processes to protect against data breaches. Currently, the FTC and state Attorneys General interpret statutory prohibitions on "unfair business practices" as a requirement for reasonable security; however, some companies have questioned that interpretation, and at least two have challenged that interpretation in court.[16] Data security legislation should also require that companies have dedicated processes in place to evaluate appropriate security safeguards. Today, despite reasonable incentives to safeguard personal data, many companies do not appear to internalize the risks of a data breach; requiring a data security program would force companies to recognize the significant risks inherent in poor data security practices. However, CDT does not support mandating a specific data security protocol (such as a particular type of encryption); given the pace by which data collection advances it is important that laws are flexible enough to avoid being inapplicable to future data collection practices. A "reasonable security" standard, though not perfect, may be more effective at evolving with changing technology.

- **Consumer access to data broker files:** Empowering consumers is paramount to our mission to preserve the user-controlled nature of the Internet, and thus we urge legislators to incorporate consumer access and correction controls in data breach provisions. When information brokers collect, maintain, and sell personal data to third parties, enabling individual consumers to access their personal data files and point out possible errors can provide an important safeguard against inaccuracy and misuse. Data broker access would also provide external accountability to data collection and sharing practices, accountability that is largely missing today due to the opacity of many companies' privacy practices. An access-and-correction regime is well established under sector specific federal privacy laws for some data brokers, such as the Fair Credit Reporting Act (FCRA). Data broker access has also historically been an element of many proposed federal bills, like the Data Accountability and Trust Act.[17] We strongly

[15] Civil penalties are only available for violation of specific statues such as the Fair Credit Reporting Act. For example in 2006, consumer data broker ChoicePoint settled with the FTC after the agency alleged it had "violated the Fair Credit Reporting Act (FCRA) by furnishing consumer reports – credit histories – to subscribers who did not have a permissible purpose to obtain them, and by failing to maintain reasonable procedures to verify both their identities and how they intended to use the information." *See* Press Release, Federal Trade Commission, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006) (on file with author).

[16] *See* G.S. Hans, *CDT Files Brief in Wyndham Supporting FTC Regulation of Data Security* CENTER FOR DEMOCRACY & TECHNOLOGY BLOG (Nov. 13, 2014), https://cdt.org/blog/cdt-files-brief-in-wyndham-supporting-ftc-regulation-of-data-security/; *See also* Press Release, Federal Trade Commission, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013) (on file with author).

[17] The Data Accountability and Trust "DATA" Act, H.R. 4400, 113th Cong. (2014).

support establishing similar consumer access rights within a larger baseline privacy law, but we would also support a narrower approach that incorporates some limited set of consumer protections into a federal law on data security and breach notification.

For more information about comprehensive privacy legislation, please visit our online resource.

For more information on CDT's data breach legislation recommendations, contact:

Justin Brookman
Director, Consumer Privacy
Center for Democracy & Technology
justin@cdt.org
202.407.8812

Alex Bradshaw
Plesser Fellow
Center for Democracy & Technology
alex@cdt.org
202.407.8822