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

Statement of Justin Brookman
Director, Consumer Privacy
Center for Democracy & Technology

Before the House Committee of Energy and Commerce,
Subcommittee on Commerce, Manufacturing, and Trade

Hearing on
"The Threat of Data Theft to American Consumers"

May 4, 2011

Chairman Bono Mack, Ranking Member Butterfield, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), thank you for the opportunity to participate in this hearing on data breach. Members of the Subcommittee on Commerce, Manufacturing and Trade deserve praise for focusing on privacy and security issues at a time when incredible growth in the volume of consumer data is matched only by the risks that that data will be breached or misused. I would especially like to thank Chairman Bono Mack for showing leadership and commitment on the issue of consumer privacy.

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet. After a note regarding the scope of the data breach problem, this testimony will briefly describe the existing framework of federal and state data breach and security laws, as well as potential legislative proposals. CDT generally believes that any federal rules on data breach would best be enacted as part of comprehensive baseline privacy legislation that in no way weakens stronger state laws. Finally, this testimony will place the need for data breach rules in the broader context of long overdue baseline consumer privacy legislation.

I. Data Breach – A Longstanding Problem

At the time of this hearing, news reports are still circulating about two large recent data breaches. In late April, Sony Corp. announced that its Playstation Network had been hacked earlier that month, compromising an estimated 77 million accounts containing unencrypted personal information such as names, addresses, birth dates, login credentials in addition to potentially tens of thousands or even millions of credit card numbers.[1] On Monday night, Sony

[1] Alex Pham, Sony apologizes, says 10 million credit card accounts may have been exposed in network attack, *LA Times*, May 1, 2011, http://latimesblogs.latimes.com/technology/2011/05/sony-apologizes-says-10-million-credit-card-accounts-may-have-been-exposed-in-network-attack.html.

revealed that the breach had extended to its Sony Online network as well, taking the total number of affected accounts to over 100 million.[2] In early April, Epsilon – a major email marketing firm whose 2,500 clients include Best Buy, Capital One Financial, Citigroup, US Bank, JP Morgan Chase, Kroger, Target, Verizon and Walgreens – suffered a cyber attack that breached information on an estimated five million people.[3] The information lost in the Epsilon breach was evidently limited to the names and email addresses of Epsilon clients' customers. A recent report conservatively estimated the total number of email addresses compromised in the Epsilon breach to be 60 million.[4]

Although these two data breaches have grabbed headlines lately because of their recency, data breach is a major longstanding problem for consumers, businesses and government. According to Privacy Rights Clearinghouse, a staggering 600 million records have been breached due to the roughly 2,460 data breaches made public since 2005.[5] According to a 2010 Ponemon benchmark study, the cost of data breaches to businesses – in terms of preventing, detecting, and notifying individuals of breach, as well as legal defense and lost business opportunities – have risen considerably over the past several years.[6] Consumers whose personal information is lost or stolen in data breaches face increased risks of identity theft, spam and phishing attacks, reduced trust toward services on which they depend, and sometimes humiliating loss of privacy over sensitive medical conditions.

Given its growing scale and persistence, it is appropriate to question whether enough is being done to solve the data breach problem. Although some state and federal regulations require companies to notify affected consumers of a data breach, the financial and reputational cost of notification may not provide many companies with adequate incentive to properly protect consumers' data in the first place. Any federal action on data breach should be a mix of requirements and incentives for both companies and government bodies to install sufficient front-end data security measures, to minimize their holdings of consumer data that is no longer necessary for a specific, legitimate purpose, and to develop structures that monitor and control where consumer data resides. Finally, although data breach is an important problem, new rules on data breach would be best addressed as one part of comprehensive baseline consumer privacy legislation.

---

[2] Ian Sherr, Hackers Breach Second Sony Service, *Wall Street Journal*, May 2, 2011, http://online.wsj.com/article/SB10001424052748704436004576299491191920416.html?mod=e2tw.

[3] Matthew J. Schwartz, Epsilon Fell To Spear-Phishing Attack, *InformationWeek*, April 11, 2011, http://www.informationweek.com/news/security/attacks/229401372

[4] Les Luchter, Epsilon Confronts Possible $225M In Data Breach, *MediaPost News*, April 29, 2011, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=149603.

[5] Privacy Rights Clearinghouse, "Chronology of Data Breaches," last updated May 2, 2011, http://www.privacyrights.org/data-breach#CP.

[6] Ponemon Institute, "2010 Annual Study: U.S. Cost of a Data Breach," March 2011, http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf.

II. Existing Legal Framework for Data Breach

As of late 2010, 46 states and the District of Columbia have enacted legislation on the breach of personal information.[7] There are also several federal laws requiring notification to consumers in the event of a data breach. Although the state standards vary and the federal laws are incomplete in their coverage, most companies already do notify affected individuals in the event of a data breach as a practical matter. The great majority of data breach law focuses on notifying consumers after a data breach, without providing incentives and requirements regarding data collection and retention that could help prevent data breach from occurring in the first place.

Each of the state laws provides a general time frame in which the compromised entity must notify consumers of a breach (often simply the in the most expedient time possible and without unreasonable delay). Some states – such as New York[8] and Texas[9] – levy civil or criminal penalties on compromised entities for failing to promptly notify consumers of a breach, while other states – such as California[10] – do not. Some states – such as California,[11] but not New York or Texas – allow individuals to bring a private right of action for injuries suffered as a result of violations of the breach notification law. Most states – including California,[12] New York[13] and Texas[14] – provide for some exemption from breach notification requirements when breached private information is encrypted.

At the federal level, there are several laws and regulations requiring reasonable security and, sometimes, notification to the victims of data breach, typically containing the same basic elements of the state laws. The federal laws are something of a patchwork insofar as they cover some data in certain contexts, but not others, reflecting the sector-by-sector approach Congress has thus far taken with regard to privacy rules. For example, the Federal Information Security Management Act (FISMA),[15] the Privacy Act[16] and the Veterans Affairs Information Security Act[17] apply to the federal sector, but not the private sector. The Fair Credit Reporting Act (FCRA) applies to consumer reporting agencies,[18] the Gramm-Leach Bliley Act (GLBA) applies to covered financial institutions,[19] and the Health Insurance Portability and Accountability Act

[7] National Conference of State Legislatures, "State Security Breach Notification Laws," last updated October 12, 2010, http://www.ncsl.org/Default.aspx?TabId=13489.

[8] N.Y. Gen. Bus. Law 899-aa(d)(6).

[9] Tex. Bus. & Com. Code 521.151.

[10] Cal. Civ. Code 56.06, 1785.11.2, 1798.29, 1798.82.

[11] Cal. Civ. Code 1798.84(b).

[12] Cal. Civ. Code 1798.82(e).

[13] N.Y. Gen. Bus. Law 899-aa(b).

[14] Tex. Bus. & Com. Code 521.053(a).

[15] 44 U.S.C. 3541 *et seq*.

[16] 5 U.S.C. 552a *et seq*.

[17] 38 U.S.C. 5722 *et seq*.

[18] 15 U.S.C. 1681 *et seq*.

[19] 15 U.S.C. 6801 *et seq*.

(HIPAA) applies to covered health care entities.[20] Consumer data that is not covered under these laws are generally protected under the Federal Trade Commission (FTC) Act.[21]

Section 5 of the FTC Act prohibits deceptive and unfair practices in interstate commerce.[22] Although the FTC Act does not provide for notification to consumers in the event of a data breach, the FTC has at times used its authority to bring suits against for failing to adopt reasonable security procedures. In 2006, the FTC filed a complaint against CardSystems Solutions (CSS) after a hacker gained access to the credit card processing company and stole tens of millions of credit and debit card numbers.[23] The FTC complaint alleged that CSS engaged in a number of "practices that, taken together, failed provide reasonable and appropriate security for personal information stored on its computer network."[24] The FTC claimed these circumstances qualified as an unfair or deceptive practice under §5 of the FTC Act, but CSS settled quickly so the question never reached adjudication.

The FTC has recently extended its interpretation of §5 of the FTC Act to non-financial information. In 2010, the FTC filed a complaint against Twitter after security lapses gave hackers administrative control over its users' accounts.[25] Like the CSS complaint, the Twitter complaint charged that the social networking site engaged in several "practices that, taken together, failed to provide reasonable and appropriate security to: prevent unauthorized access to nonpublic user information and honor the privacy choices exercised by its users in designating certain tweets as nonpublic."[26] The FTC alleged that these practices qualified as unfair or deceptive under §5 of the FTC Act, though Twitter also settled with the FTC before the matter reached a court of law. CDT hopes FTC will continue to be clear that reasonable security standards apply to non-financial information, such as email addresses and accounts.

III. Elements of Future Data Breach and Security Proposals

CDT has previously testified in favor of federal data breach and security legislation. We think such legislation could be a step forward to the extent that it goes beyond just breach notification and reasonable security, which are already required under the law, to include useful new

[20] 42 U.S.C. 1320d *et seq*.

[21] 15 U.S.C. 45(a) *et seq*.

[22] Id.

[23] Federal Trade Commission Complaint, *In the Matter of CardSystems Solutions, Inc.*, Docket No. C-4168, September 5, 2006, http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf.

[24] The CSS practices the FTC complaint identified included creating "unnecessary risks to the information by storing it in a vulnerable format for up to 30 days," failing to asses the vulnerability of its computer network to common and foreseeable attacks, failing to use strong passwords and other readily available defenses to such attacks, and failing to employ sufficient means to detect unauthorized access to personal information. *See* FTC Complaint, *In the Matter of CardSystems Solutions, Inc.,* Pg. 2., Para. 6.

[25] Federal Trade Commission Complaint, *In the Matter of Twitter, Inc.*, Docket No. C-, June 24, 2010, www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf.

[26] FTC complaint alleged that, among other things, Twitter failed to make administrative passwords difficult to guess, failed to suspend or disable administrative passwords after a reasonable number of unsuccessful login attempts, and failed to restrict employee access to user accounts according to the needs of the employees' jobs. *See* FTC Complaint, *In the Matter of Twitter, Inc.,* Pg. 4., Para. 11.

safeguards.[27] For example, the Data Accountability and Trust Act that was introduced last Congress by Representatives Rush, Barton, Stearns, Radanovich, and Schakowsky contained provisions on consumer access to data broker files in addition to security and breach notification requirements.[28] That bill would have created a nationwide data breach notification standard, which CDT supports so long as that standard is at least as effective as the laws already in place at the state level. If a federal law were to preempt state laws and replace them with a weak notification regime, the result would be a significant step backwards for consumers and data security. However, it is true that the current patchwork of notification standards can prove a challenge from an industry compliance perspective. In the interest of removing unnecessary compliance barriers, CDT supports the concept of a nationwide data breach notification standard. CDT believes that for a federal law to be as effective as the strongest state laws, the following elements would be necessary:

- **Appropriately-scoped preemption:** CDT has reservations about preempting state data security laws covering topics other than notification. The information security provisions of the Gramm-Leach-Bliley Act (GLB) preempted inconsistent state laws, but otherwise allowed for state-level experimentation on the difficult question of how to ensure sufficient attention and precautions with respect to data security. Any federal data breach notification regime should preserve a state's ability to come up with an idea that is truly a fresh approach. California's breach notification law, the first in the nation, was a classic example of this. Had GLB broadly preempted state privacy and data security laws, this very important legislation would not have been possible.

- **A "notify unless" notification trigger:** A notification trigger should permit notification to be avoided only when there is an affirmative determination that there exists no serious risk that personal information could be misused. In other works, the standard should be that, in the event of a breach, a company must notify unless such an affirmative determination can be made. A finding that appropriate technical safeguards prevent unauthorized access to the data should qualify as an affirmative determination that there is no significant risk is misuse.

  A "notify unless" trigger creates strong incentives for a company suffering a breach to get to the bottom of what happened –because if it can determine there is no real risk, it will not have to notify its customers.[29] A trigger that requires notification only in the event of an affirmative finding of risk would create the opposite incentive — a company might not want to investigate too closely, because finding evidence of risk would trigger the obligation to notify.

  A "safe harbor" provision that exempts companies that appropriately safeguard the data they hold through reasonable encryption will both incentivize companies to adopt better data security practices and help prevent needless consumer notification. It is important to note, however, that safeguards should not excuse notification when the circumstances of the

[27] Statement of David Sohn, Senior Policy Counsel of the Center for Democracy & Technology, before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, "Legisaltvie Hearing on H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act," May 5, 2009, http://www.cdt.org/files/pdfs/20090505_data_p2p.pdf.

[28] H.R. 2221, 111th Cong. (1st Sess. 2009). Introduced by Rep. Rush, co-sponsored by Reps. Barton, Radanovich, Schakowsky and Stearns. The House of Representatives passed DATA in the 111th Congress.

[29] DATA had a "notify unless" formulation. See H.R. 2221 Sec. 3(f).

breach suggest that those safeguards are unlikely to be effective. For example, a breach involving encrypted data should generally be exempt from notification, but not when it appears that the encryption keys may have been breached as well.

- **Outside scrutiny:** Adopting a "notify unless" notification trigger is crucial. However, in the absence of any outside scrutiny of risk determinations, a company could have an incentive to err consistently on the side of finding little or no risk. Even if the affected individuals were eventually to become victims of identity theft, it would be difficult ever to trace those crimes back to the specific breach, since nobody other than the company and the identity thieves would be aware that the breach even occurred. In short, with nobody in a position to question dubious risk assessments, there could be a temptation to under-notify.

  CDT believes this problem could be greatly mitigated by requiring a company, when it determines a breach poses insufficient risk to warrant notification, to notify the FTC or other appropriate regulator and provide some explanation as to why the company believes there is no significant risk. No formal process for FTC review or approval of a company's determination would necessarily be required. Simply knowing that a brief explanation would need to be filed with the FTC, and that the FTC might respond if it spotted a pattern of behavior or otherwise became suspicious, may be all it would take to ensure that companies remain diligent in their risk determinations and weigh the inevitable judgment calls in an even-handed manner. CDT therefore recommends that any data breach law require that breaches judged to be non-risky still necessitate a submission of a brief written explanation to a regulatory body such as the FTC.

- **Strong enforcement:** A national data breach standard should allow for enforcement by the FTC and state attorneys general. The most important enforcement lever would be to provide the FTC and states the authority to levy penalties for existing data security and breach notification requirements.

- **No harm standard:** Debates about security breach notification requirements often center around whether or not notification should be required in the absence of a determined "harm" to the consumer, such as identity theft. CDT cautions against a federal framework that would limit notification to cases where particular harms or risks of particular harms can be identified. The "notify unless" formulation that CDT suggests excuses notification when there is no real risk of misuse, but does not require any showing that harm has occurred or is likely to occur. Nor does it require any analysis of what specific harms could occur; it would not say, for example, that notification depends on whether there is a risk of a particular harm such as identity theft or of a type of harm such as financial cost.

  Some companies may claim that a more narrowly focused harm standard ensures that consumers are not overwhelmed by unnecessary notices. However this argument incorrectly presupposes that the only purpose of breach notification is informing individuals of the steps they can take to protect themselves from specific threats such as identity theft. While this is in fact one purpose behind breach notification standards, it ignores the larger goal of the policy: reducing the number of data breaches by incentivizing companies to improve their data security practices. Indeed, a 2007 study of the impact of state-implemented breach laws conducted by the Samuelson Law, Technology, & Public Policy Clinic at the University of California, Berkeley found that "regardless of the risk of identity theft and alleged

individual apathy towards notices, the simple fact of having to publicly notify causes organizations to implement stronger security standards that protect personal information."[30]

As for federal security legislation, CDT believes that the numerous settlements achieved by the FTC demonstrate that Section 5 of the FTC Act already requires companies to implement reasonable security protocols to protect consumer data. We encourage the FTC to continue to aggressively bring data security enforcement actions, including cases around the treatment of non-financial consumer information, as in the Twitter settlement.[31] In order to make the FTC's actions more effective, CDT has long recommended equipping the FTC with stronger tools to protect consumers, such as greater resources and the ability to recover civil penalties.[32] We believe legislation granting the FTC such additional capacity could be potentially the most effective measure to incentivize companies to adequately safeguard consumer information. CDT would be skeptical of legislation that mandated specific technological data security solutions; such mandates would quickly become outdated as technologies change, and would not encourage (and may deter) companies from innovating new responses to evolving security threats. However, CDT is supportive of general reasonable security requirements as part of a comprehensive privacy law, in order to put to rest any doubts about the FTC's authority to require as much under its §5 unfairness authority.

IV. Future Data Breach and Security Proposals Should Be Part of Baseline Privacy Legislation

CDT strongly supports the enactment of a uniform set of baseline rules for personal information collected both online and off-line. Modern data flows often involve the collection and use of data derived and combined from both online and offline sources, and the rights of consumers and obligations of companies with respect to consumer data should apply to both as well. The Subcommittee should recognize that, from a consumer perspective, even a good federal breach notification requirement does not by itself offer much tangible progress over the status quo, since notification is already effectively the law of the land. To be of real benefit to consumers, data privacy and security legislation must include some additional protections. What is needed more than security and notification requirements is a data privacy law that incentivizes and requires companies to collect only as much personal information as necessary, be clear about with whom they're sharing information, and expunge information after it is no longer needed.

Fair Information Practices (FIPPs) must be the foundation of any comprehensive privacy framework. FIPPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. The most recent formulation of the FIPPs by the Department of

[30] Samuelson Law, Technology, & Public Policy Clinic, "Security Breach Notification Laws: Views from Chief Security Officers," University of California-Berkeley School of Law, December 2007, http://www.law.berkeley.edu/files/cso_study.pdf.

[31] *See* FTC Complaint, *In the Matter of Twitter, Inc.*

[32] Statement of Ari Schwartz, Deputy Director of the Center for Democracy & Technology, before the Senate Committee on Commerce, Science, Trade and Tourism, "Reauthorization of the Federal Trade Commission," September 12, 2007, http://old.cdt.org/privacy/20070912schwartz-testimony.pdf.

Homeland Security offers a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy legislation.[33] Those principles are:

- Transparency
- Purpose Specification
- Use Limitation
- Data Minimization
- Data Accuracy
- Individual Participation
- Security
- Accountability

Although data security, individual access to personal information, and notification of breaches are important safeguards under the FIPPs, it is crucial that baseline consumer privacy legislation not give short thrift to the other FIPPs, such as data minimization. Companies should collect only that data which are directly relevant and necessary to accomplish a specified purpose, and data should only be retained for as long as is necessary to fulfill a specified purpose. Unlike breach notification, data minimization is a pre-breach remedy and should be an obligation of all companies that collect personal information. Requiring companies to get rid of unneeded consumer data would reduce the impact of data breaches, and potentially result in fewer targets for identity thieves.

For example, in December of last year, the drug store chain Walgreens experienced a data breach incident, and sent notifications not just to current customers, but also to persons who had previously unsubscribed from Walgreens email lists.[34] Even though those persons had elected to terminate their relationship with Walgreens, the company retained those person's email addresses for undefined purposes. Four months later, Walgreens' customer data was again compromised as a result of the Epsilon security breach. Again, the company sent notifications to prior customers who had unsubscribed from Walgreens marketing lists.[35] While it is admirable that the company in both cases informed previous customers about the potential exposure of their data, it remains unresolved why the company retained that data in the first place. Our current legal framework has failed to require or even encourage companies to adopt data minimization procedures, and we therefore believe that requiring reasonable data minimization would result in less consumer information being exposed through data security breaches.

Comprehensive privacy legislation should also provide consumers with reasonable access to the information that companies possess about them. When companies collect, maintain, and transfer 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

[33] U.S. Department of Homeland Security, "Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," December 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[34] Bob Sullivan, Hackers steal Walgreens e-mail list, attack consumers, *MSNBC Technolog*, December 10, 2010, http://technolog.msnbc.msn.com/_news/2010/12/10/5624759-hackers-steal-walgreens-e-mail-list-attack-consumers.

[35] Dissent, "Why unsubscribing might not have protected you from the Epsilon breach," PogoWasRight.org, April 5, 2011, http://www.pogowasright.org/?p=22239.

and misuse, and also provide needed transparency to consumers about the wide range of entities that possess and use information about them.

As data flows have grown more complex, companies must have safeguards in place to monitor them. The fact that major data breaches continue to occur demonstrate that current practices for collecting and storing consumer data have outstripped the practices for keeping it safe. The most effective solution will not lie in an isolated effort to apply encryption to data or to quickly notify consumers of a data breach. Rather, the law should provide companies with a range of incentives and requirements that encourage them to establish internal privacy policies that seamlessly protect data throughout the data's lifecycle.[36] A comprehensive data protection framework coupled with strong enforcement is that solution, and for this reason CDT is has previously testified before this Committee in support of the flexible, forward-looking BEST PRACTICES Act[37] introduced by Representative Rush. CDT looks forward to working with both chambers to improve the bills and enact strong privacy protections for American consumers.

V. CONCLUSION

CDT would like to thank Chairman Bono Mack for calling this hearing on such an important topic, and for the opportunity to testify today.

For more information, contact Justin Brookman, justin@cdt.org at (202) 637-9800.

[36] Center for Democracy & Technology, "The Role of Privacy by Design in Protecting Consumer Privacy," January 28, 2010, http://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy.

[37] H.R. 611, 112th Cong. (1st Sess. 2011).