
Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on the Discussion Draft of H.R.____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach

Before the

House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

June 15, 2011
2322 Rayburn House Office Building
Washington, DC

Madame Chair and Members of the Committee, thank you for the opportunity to testify today on the SAFE Data Act. My name is Marc Rotenberg. I am executive director of the Electronic Privacy Information Center ("EPIC") and I teach privacy law at Georgetown University Law Center.

We are grateful for the work of this Committee on the critical issue of data security and privacy protection. In my testimony this morning, I will discuss the urgency of this problem, review the proposed legislation, and make a few further points about forward-looking strategies for privacy protection.

I also want to acknowledge two organization that have expressed support for this statement: the Consumer Federation of America and the U.S. PIRG. I would encourage the members of the Committee and their staff to communicate directly with these groups as the legislative process moves forward.

One key point to make at the outset is that almost all of the states have responded over the last few years to develop robust security breach notification legislation. Many of these laws can be traced back to the California notification law that was famously triggered in a matter that EPIC brought attention to involving the sale of data on American citizens to a criminal ring engaged in identity theft. That notification and the investigation that followed led to dramatic changes in the information broker practices in the United States. While there is clearly a lot more that needs to be done to safeguard personal data, you should not underestimate the enormous value of these breach notification statutes as well as the unintended problems that could result if federal law preempts more responsive state laws. For reasons I will discuss in more detail below, I recommend that you not adopt legislation that would preempt the ability of the states to develop more effective means to respond to these new problems.

Scope of the Data Breach Problem

In recent months, there have been a large number of high profile data breaches that illustrate the severity of the problem and necessity of comprehensive data breach legislation.

- A recent breach at Southern California Medical-Legal Consultants, a company representing medical providers for workers' compensation claims, disclosed personal data, including names and social security numbers, of approximately 300,000 people.[1]

[1] Press Release, Southern California Medical-Legal Consultants, Possible Data Breach Discovered and Contained (June 11, 2011), http://www.scmlc.com/press.htm.

- In May, a breach at Citigroup exposed customer names, account numbers, and contact information for more than 200,000 customers. Citigroup waited almost a month before it notified its customers.[2] Experts have warned that this disclosure of customer data will make Citigroup customers especially vulnerable to phishing attacks and other acts of fraud.[3]

- The PlayStation Network breach in April exposed personal data, including names, addresses, passwords, and possibly credit card data, of over 100 million users.[4]

- A breach at Epsilon, an internet marketing company, in late March, disclosed personal information, including names and email addresses, of millions of consumers. [5]

According to the Identity Theft Resource Center, there have been at least 195 data breaches in 2011.[6] In 2010, there were 662 breaches and over 16 million records compromised.

These problems are going to get worse. As more sensitive data moves into the cloud, as we become more dependent on electronic health records, and more companies store vast amounts of consumer data on remote servers, the risk that personal data will be improperly disclosed or accessed will necessarily increase.

Moreover, consumers and businesses that become increasingly dependent on these services are less likely to know when problems occur than if they were to lose their own laptop or experience a break-in.

Breach notification does not solve these problems. But it does help us to understand the extent of the problems so that better safeguards and practices can be developed.

---

2 Randall Smith, *Citi Defends Delay in Disclosing Hacking*, Wall St. J. (June 13, 2011), http://online.wsj.com/article/SB10001424052702304665904576382391531439656.html

3 Jeremy Kirk, *Citigroup Breach Exposed Data on 210,000 Customers*, PC World (June 9, 2011), http://www.pcworld.com/businesscenter/article/229868/citigroup_breach_exposed_data_on_210000_customers.html.

4 Liana B. Baker & Jim Finkle, *Sony Playstation Suffers Massive Data Breach*, Reuters (Apr. 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

5 Hayley Tsukayama, *Sony, Epsilon Support National Data Breach Bill*, Wash. Post. (June 3, 2011), http://www.washingtonpost.com/blogs/post-tech/post/sony-epsilon-support-national-data-breach-bill/2011/06/02/AG34tvHH_blog.html.

6 As of June 7th, 2011. The report also lists 11,030,619 records being compromised but does not include the record counts for the most recent data breaches. Identity Theft Resource Center, 2011 Data Breach Stats 7 (June 7, 2011), http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202011.pdf.

Structure of the SAFE Data Act

Section 2 of the SAFE Data Act sets forth new Data Security Requirements that require companies to assess and address vulnerabilities within their systems and participate in data minimization practices.

Section 3 of the SAFE Data Act includes provisions on data breach notification that create deadlines for notification of law enforcement and consumers. Law enforcement must be notified within 48 hours of discovery. Companies must assess the scope of the breach, identify the nature of the breach, and address the vulnerabilities that created the breach. Within 48 hours of conducting this assessment, companies may have to notify consumers.

Section 3, the Application and Enforcement section of the SAFE Data Act, allows for enforcement by the Federal Trade Commission and state attorneys general. It does not provide for a private right of action or statutory damages scheme.

Section 6 of the SAFE Data Act, entitled Effect on Other Laws, includes a provision that states that this bill would preempt all state information security laws generally and state created civil actions for data breach specifically.

Important Changes from Earlier Bill

The SAFE Data Act is based on similar legislation that has been considered and favorably reported by this Committee in the past. There are two significant changes in this bill that we support.

First, we support the data minimization provision. It has become clear that one of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks do occur is to collect less sensitive personal information at the outset. It is the credit card numbers, the bank account numbers, the social security numbers, and the passwords that draw the attention of computer criminals. Reducing the target size reduces the vulnerability.

On data minimization, we would urge you to go further. Instead of simply a data minimization plan, we would recommend a data minimization requirement. There are many examples of this already in privacy law. For example, the Video Privacy Protection Act requires businesses to:

> Destroy personally identifiable information as soon as practicable, but not later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pendin requests or orders for access to such information . . .

Other privacy bills include similar requirement.[7]

[7] *See e.g.* Gramm-Leach-Bliley Financial Services Modernization Act, Title V of the Financial Services

The simple message to business should be "if you can't protect it, don't collect it."

Second, we support the 48-hour requirement for breach notification. Earlier versions of the bill allowed companies to wait 7 days, in some instances 60 days, before notifying those whose personal data was compromised. That is too long. The shorter time period will require companies to respond quickly when there is a problem. This shorter period will also allow consumers to react more quickly and take preventative or mitigating actions.

Additional Improvements

*Method of Notification*

The bill currently proposes the use of either written notification or email notification when an obligation to provide notification arises. I would suggest that you include an additional obligation to provide a text message where possible. A text message would not be an effective substitute for written notification or email, because it is essentially ephemeral. But is a very effective technique for notification and it could help make people aware that they should look for a notice that might arrive in the mail or show up in the email box.

In a similar spirit, where the bill speaks of providing notification by means of a web site, it may be appropriate to add "or social network presence." Many organizations today are interacting with users though popular social network services such as Facebook. In many configurations, the data remains with Facebook, so there is no direct data collection by third parties. But in other circumstances, for application developers and advertisers for example, third party companies obtain information from users through Facebook. If security breaches arise in these circumstances, notification by means of the social network service may be the most effective way to reach the target population.

*Public Record Defense*

The definition of "personal information" in the bill expressly exempts "public record information" available from federal, state, or local government systems and was acquired by the company that suffered the breach for such purposes. The theory underlying this provision, I imagine, is that there could be no additional harm to the individual of the breach of this information if it is already available to the public. But this is the wrong way to understand the problem and the affirmative defense will undercut the purpose of the bill.

If an organization suffers a security breach of confidential information or of "public information" it has a problem that needs to be corrected. If no action is taken to

---

Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. §§ 6801, 6809, 6821, and 6827).

correct the problem, it is quite likely the breach will occur again. That is why the security obligation should apply even when there is no immediate harm to the individual: The problem remains. Also, I would not assume the fact that personal information may be found through public data sources that the information disclosed in a data breach is equivalent. It is quite likely, particularly in the information broker industry, that the "public" information contained in a particular data record is far more detailed than any record that would be available in a singe government record system.

*Treatment of Personally Identifiable Information*

One of the key provision of the bill is the definition of "Personal Information." This definition is critical because, as with most privacy bills, this definition will determine when the obligations of the Act should be applied and when they can be pretty much ignored.

As currently drafted, the bill sets out a narrow definition for Personal Information, as compared with other privacy statutes. For example, the bill seems to suggest that a social security number would not be personally identifiable if it is possessed without the associated person's name. The bill also ignores other popular identifiers, such as a user ID for Facebook, which points as readily to a unique individual as would a driver's license or a social security number.

The definition is also narrow in light of the 2009 FTC on Internet advertising that noted that there are many ways to track Internet users, including the use of "IP address" that can uniquely identify a user's computer, much as phone number will uniquely identify a cell phone. In many cases, this is also a form of personal information that should be subject to the bill's requirements.

I would suggest a construction that would define Personal Information as information that "identifies or could identify a particular person," followed by the examples cited in the bill as illustrations, with the qualifying phrase "including, but not limited to." This approach is technology neutral, less dependent on the rulemaking process, and more likely to adapt over time.

*Strengthen Notification*

The bill addresses preemption and the circumstances under which the federal law would overwrite possibly more effective state information security legislation. As currently drafted, the bill preempts state laws that either have similar security obligations as well as state laws that provide for security breach notification. The bill does leave in place state trespass, contract and tort law, as well as claims involving fraud.

My own view is that it would be a mistake to adopt a preemption provision of this type. Businesses understandably will prefer a single national standard. That is the argument for preemption. However privacy laws have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish. This approach to

consumer protection is based upon our federalism form of government that allows the states to experiment with new legislative approaches to emerging issues.

The breach notification provision should be strengthened and clarified. The bill states that if the company determines that there is no "reasonable risk of identity theft, fraud, or other unlawful conduct" the notification of customers is not required. The bill should be modified to make clear that it imposes a presumption in favor of notification. The ability to assess the risk and make a decision about breach notification should not rest in the hands of the entity that allowed the breach to occur. We recommend that the right to assess the severity of the breach be placed in the hands of either an independent regulatory agency (the Federal Trade Commission) or the consumers. Routine notification should be required.

As we have explained in previous testimony,[8] identity theft is only one risk from unauthorized access to personal information. Unauthorized access may be gained for other purposes that cause harm to the individual, such as stalking, obtaining information for debt collectors, corporate espionage, extortion, or to supply information that will be used for future phishing or fraud activities. The recent breach at Citigroup is a good example of this. The information originally obtained in the breach may not have included social security numbers, credit card numbers, or other traditional tools of identity theft, but it was enough to leave consumers vulnerable to phishing attacks. In instances such as this, consumers should be notified so that they can take proper precautions against future attacks and possible fallout from the data breach.

In other circumstances, a reasonableness standard might be appropriate. The problem here is that the company will decide itself, having suffered the breach, *whether there is reasonable risk of harm to others* and there will be no effective way to review this decision if the company guesses wrong. That is an approach that will invite greater secrecy and less accountability. Companies often cannot tell whether a security breach may result in identity theft. The motives of a person who gained access are not always clear. Identity theft can also occur months or even years after a security breach.

Placing the decision about whether or not to notify customers in the hands of the company is also problematic because companies are often reluctant to disclose breaches to customers. Sony, for instance, waited a week to notify customers of its data breach.[9] Citibank waited a month. [10]

Because it is difficult to gauge the risk of identity theft, because there are harms other than identity theft which may result from security breaches, and because there is already evidence that companies will go to great lengths to avoid giving security breach

---

[8] EPIC, *Testimony for the Legislative Hearing on "Data Security: The Discussion Draft of Data Protection Legislation"*(July 29, 2005), http://epic.org/privacy/choicepoint/datasec7.28.05.html.

[9] Missouri Attorney General Chris Koster, *Attorney General Koster Says Sony Failed to Warn Consumers About Playstation Network Breach,* Attorney General's News Release (April 28, 2011), http://ago.mo.gov/newsreleases/2011/AG_Koster_says_Sony_failed_to_warn_consumers/.

10 Randall Smith, *Citi Defends Delay in Disclosing Hacking*, Wall St. J. (June 13, 2011), http://online.wsj.com/article/SB10001424052702304665904576382391531439656.html

notices, we recommend eliminating the language that gives companies discretion not to give notice based on a determination whether the breach "may result in identity theft."

*Private Right of Action*

We support the inclusion of provisions allowing enforcement by the Federal Trade Commission and state attorneys general, but would recommend expanding this to include a private right of action for customers. It is often difficult to place a dollar value on data breaches and privacy infringements, so it is important that this private right of action also include a statutory damages provision. This would empower consumers to enforce the law themselves and create a strong disincentive for the irresponsible handling of consumer data. Not only would this provide the opportunity for individuals who have been harmed by security breaches to have their day in court, it would also provide a necessary backstop to the current enforcement scheme which relies almost entirely on the Federal Trade Commission, acting on its own discretion and without any form of judicial review, to enforce private rights.

For these reasons, many state laws include private right of action provisions. California, Hawaii, Louisiana, and Washington, for instance, include provisions in their state data breach laws that allow consumers to bring a civil action and recover damages.[11]

*Avoid a Federal "Ceiling" on Breach Notification*

We also recommend that the preemption clause in the bill be dropped or modified so that this federal bill creates a "floor" instead of a ceiling. It is important that states be permitted to legislate in this area. As discussed already, most states have comprehensive data breach legislation. Often, this legislation establishes a private right of action, statutory damage scheme, and notification requirements. [12]

Because states enjoy a unique perspective that allows them to craft innovative programs to protect consumers, they should be permitted to continue to operate as "laboratories of democracy" in the privacy and data security arena. State legislatures are closer to their constituents and the entities they regulate; they are the first to see trends and problems, and are well-suited to address new challenges and opportunities that arise from evolving technologies and business practices. This is why privacy bills have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish.

There is an additional reason that we believe weighs against preemption in the information security field: these problems are rapidly changing and the states need the ability to respond as new challenges emerge. California and Massachusetts have recently considered updating their data breach legislation in response to new threats.[13] It is very

[11] Cal. Civ. Code 1798.82 (2011), Haw. Rev. Stat. § 487N-2 (2011), La. Rev. Stat. § 51:3071 et seq.(2011), Wash. Rev. Code § 19.255.010, 42, 56, 590 (2011).
[12] *See e.g.* Cal. Civ. Code 1798.82 (2011).
[13] Jason Gavejian, *California and Massachusetts Legislatures Push Data Breach and Security Bills,*

likely that the states will continue to face new challenges in this field. Placing all of the authority to respond here in Washington in one agency would be, as some in the security field are likely to say, a "critical failure point." The temptation to establish a national standard for breach notification should be resisted, particularly given the rapidly changing nature of the problem.

Looking ahead

While it is clearly important to inform individuals when their personal information in the possession of others has been improperly accessed or disclosed, it is time to ask whether the remedies that are provided are effective or meaningful. Consumers have become increasingly frustrated by the breach notifications that encourage them to sign up for credit monitoring services. Why should they bear the burden for the mistakes of others?

A number of states have recognized that at least part of the solution is to change the default setting for the disclosure of credit data. Laws that "freeze" the disclosure of the credit information pending a choice of the consumers to release simply establish an opt-in that is the commonsense approach for disclosing sensitive personal data.

Conclusion

Data breaches remain one of the greatest concerns for Internet users in the United States. Many companies have poor security practices and collect far more information than they need or can safeguard. But since there are few consequences for poor security practices, they can obtain all the value from the user data and leave it to the consumers to deal with the consequences.

Consumers are also often left out of the loop when breaches occur. They are not informed that their data has been disclosed, so they cannot take mitigating actions to try to minimize the damage. It is important that this problem is corrected with a strong notification requirement. The SAFE Data act should also empower consumers with a private right of action and statutory damages.

Companies need to know that they will be expected to protect the data they collect and that, when they fail to do so, there will be consequences. Legislation for information security and breach notification is needed, but it should not preempt stronger state measures and it should not rely solely on FTC rulemaking authority.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

---

Workplace Privacy, Data Management, and Security Report (May 3, 2011), http://www.workplaceprivacyreport.com/2011/05/articles/workplace-privacy/california-and-massachusetts-legislatures-push-data-breach-and-security-bills/