



**ELECTRONIC PRIVACY INFORMATION CENTER**

---

Testimony and Statement for the Record of

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

Hearing on "Cybersecurity and Data Protection in the Financial Sector"

Before the

Financial Institutions and Consumer Credit Subcommittee

of the

House Committee on Financial Services

September 14, 2011  
2129 Rayburn House Office Building,  
Washington, DC 20515

Madam Chair and Members of the Subcommittee, thank you for the opportunity to testify today concerning cybersecurity and data protection in the financial sector. 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.

EPIC is non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues. We work with a distinguished panel of advisors in the fields of law, technology, and public policy. We have a particular interest in promoting technical standards and legal safeguards that help safeguard personal information.<sup>1</sup> I also want to note that U.S. PIRG, a leading consumer advocacy organization, has expressed support for this statement. I would encourage the members of the Committee and their staff to communicate directly with U.S. PIRG as the legislative process moves forward.

We are grateful for the work of this Subcommittee on the critical issues of data security and privacy protection. In my testimony this morning, I will discuss the urgency of this problem, review several recent, high-profile data breaches in the financial sector, and make a few further points about forward-looking strategies for privacy protection. We also want to acknowledge the important enforcement efforts undertaken by federal agencies to protect American consumers, as well as the growing awareness across the financial services sector of the scope of the problem.

There have been several cybersecurity incidents over the past few months that highlight the threats to consumers in the financial services sector. These attacks on financial institutions produce both direct and indirect costs for consumers who must contend with the risk of identity theft and financial fraud, as well as whatever additional costs the companies pass along.

Also, current laws do not adequately protect consumers. In brief, legislation should apply breach notification regulations to financial institutions, should require authentication techniques that reduce the risk to consumers, and should not preempt stronger state laws. Additionally, we favor the development of cyber security policies that are open to public review and comment, that respect the role of the private sector, and that safeguard the rights of consumers and users.

### Scope of the Cybersecurity and Data Breach Problem in the Financial Sector

In recent months, there have been many high-profile data breaches in the financial sector. These breaches make clear an ongoing risk to consumers and underscore the need for stronger privacy legislation.

- Just last month, Citigroup suffered two breaches at its Japanese credit card unit, compromising the personal data of over 92,000 consumers.<sup>2</sup> This comes in the wake of one of the most widely reported data breaches of the year, where inadequate security measures at Citigroup exposed customer names, account numbers, and

---

<sup>1</sup> More information about EPIC is available at the web site <http://www.epic.org/>.

<sup>2</sup> Dan Goodin, *Citigroup Hit With Another Data Leak*, The Register, Aug. 9, 2011, [http://www.theregister.co.uk/2011/08/09/citigroup\\_data\\_breach\\_again/](http://www.theregister.co.uk/2011/08/09/citigroup_data_breach_again/).

contact information for more than 360,000 customers in May.<sup>3</sup> Citigroup waited almost a month before it notified its customers.<sup>4</sup> Experts have warned that this disclosure of customer data will make Citigroup customers especially vulnerable to phishing attacks and other acts of fraud.<sup>5</sup>

- In June 15 of this year, Automatic Data Processing Inc. ("ADP"), the largest payroll processor in the world, admitted that the personal data of one of its 550,000 corporate clients was breached, but did not disclose the company that was affected.<sup>6</sup>
- Also in May 2011, news reports revealed that a Bank of America insider had leaked the detailed personal information of many of the bank's customers.<sup>7</sup> As a result of the data breach, the affected customers have lost over \$10 million from their accounts.<sup>8</sup> This outcome is particularly troublesome considering that Bank of America is the largest bank in the U.S.<sup>9</sup>
- In January of 2009, weak network security caused a breach at Heartland Payment Systems, a credit card payment processing firm.<sup>10</sup> The company has settled with American Express, Mastercard, Visa, and Discover due to claims raised as a result of the data security breach.<sup>11</sup> It is estimated that millions of consumers' personal card numbers were stolen as a result of the breach.<sup>12</sup> At the time, Heartland claimed to have been compliant with every requirements of the Payment Card Industry Data Security Standard, leading many to cite the breach as an example of the failure of industry self-regulation to protect the private data of consumers.<sup>13</sup>

---

<sup>3</sup> Eric Dash, *Citi Says Many More Customers Had Data Stolen by Hackers*, N.Y. Times (June 16, 2011), [http://www.nytimes.com/2011/06/16/technology/16citi.html?\\_r=1](http://www.nytimes.com/2011/06/16/technology/16citi.html?_r=1).

<sup>4</sup> Randall Smith, *Citi Defends Delay in Disclosing Hacking*, Wall St. J. (June 13, 2011), <http://online.wsj.com/article/SB10001424052702304665904576382391531439656.html>.

<sup>5</sup> 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](http://www.pcworld.com/businesscenter/article/229868/citigroup_breach_exposed_data_on_210000_customers.html).

<sup>6</sup> Maria Aspan, *ADP Says Investigating Data Breach*, Reuters (June 15, 2011), <http://www.reuters.com/article/2011/06/15/us-adp-breach-idUSTRE75E5BB20110615>.

<sup>7</sup> David Lazarus, *Bank of America Data Leak Destroys Trust*, L.A. Times (May 24, 2011), <http://articles.latimes.com/2011/may/24/business/la-fi-lazarus-20110524>.

<sup>8</sup> *Id.*

<sup>9</sup> National Information Center, *Top 50 Bank Holding Companies in the U.S.*, (March 31, 2011), <http://www.ffiec.gov/nicpubweb/nicweb/top50form.aspx>

<sup>10</sup> Taylor Buley, *Metadata: World's Biggest Data Breach*, Forbes (January 20, 2009), [http://www.forbes.com/2009/01/20/data-breach-metadata-tech-security-cz\\_tb\\_0120breach.html](http://www.forbes.com/2009/01/20/data-breach-metadata-tech-security-cz_tb_0120breach.html)

<sup>11</sup> Rachel Chitra, *Update 1- Heartland Payment, Discover Settle Data Breach Claims*, Reuters (September 1, 2010), <http://uk.reuters.com/article/2010/09/01/heartlandpayment-idUKSGE6800LT20100901>

<sup>12</sup> *Id.*

<sup>13</sup> Jaikumar Vijayan, *Update: Heartland breach shows why compliance is not enough*, ComputerWorld, Jan. 6, 2010, [http://www.computerworld.com/s/article/9143158/Update\\_Heartland\\_breach\\_shows\\_why\\_compliance\\_is\\_not\\_enough](http://www.computerworld.com/s/article/9143158/Update_Heartland_breach_shows_why_compliance_is_not_enough).

- In July of 2008, Wells Fargo, a financial services company and one of the four largest banks in the U.S., was breached by the illegal use of a bank access code.<sup>14</sup> The data breach resulted in the loss of personal information of approximately 5,000 consumers.<sup>15</sup>
- In 2007, TJX, the largest apparel off-price department store in the U.S., announced that it had been the victim of a data breach whereby the personal data of millions of customers was stolen by hackers.<sup>16</sup> The company eventually settled, paying almost \$10 million to states,<sup>17</sup> \$24 million to Mastercard,<sup>18</sup> and \$41 million to Visa.<sup>19</sup>

These problems are not unique to the financial sector. Last month, Purdue University reported that computer criminals had broken into a server containing the personal data of students who attended the university from 2000 through the summer of 2005, and the University of Wisconsin-Milwaukee discovered malware that may have compromised the data of thousands of students and researchers.<sup>20</sup> This summer also saw data breaches at the CIA, the International Monetary Fund, and the computer network of the United States Senate.<sup>21</sup>

Other companies that have recently lost control of sensitive consumer information include: Epsilon, Lockheed Martin, Sony, the Southern California Medical-Legal Consultants, South Carolina's Spartanburg Regional Healthcare System, and the Swedish Medical Center in Seattle. These breaches affected millions of consumers.<sup>22</sup>

---

<sup>14</sup> The Associated Press, *Wells Fargo Data Breach Revealed*, L. A. Times (August 13, 2008), <http://articles.latimes.com/2008/aug/13/business/fi-wells13>

<sup>15</sup> *Id.*

<sup>16</sup> Aarthi Sivaraman, *TJX Settles Data Breach Case with U.S. States*, Reuters (June 23, 2009), <http://www.reuters.com/article/2009/06/23/tjx-idUSN233656120090623>

<sup>17</sup> *Id.*

<sup>18</sup> Associated Press, *TJX to Pay Mastercard up to \$24M in Data Breach Settlement*, Boston Herald (April 2, 2008), <http://www.bostonherald.com/business/general/view.bg?articleid=1084541>

<sup>19</sup> Keith Regan, *TJX to Shell Out \$41M in Data Breach Settlement*, E-Commerce Times (November 30, 2007), <http://www.technewsworld.com/story/60554.html?wlc=1308577476>

<sup>20</sup> Journal and Courier, *Purdue warns ex-students of data breach*, Journal and Courier (Aug. 17, 2011), <http://www.jonline.com/article/20110817/NEWS0501/108170320/Purdue-warns-ex-students-data-breach>; ; Stanley A. Miller II, *UWM computers hacked; data on 75,000 exposed*, Milwaukee Journal Sentinel (Aug. 10, 2011), <http://www.jsonline.com/news/milwaukee/127459128.html>.

<sup>21</sup> The Economist, *An Anonymous Foe*, The Economist (June 16, 2011), <http://www.economist.com/node/18836210>.

<sup>22</sup> 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](http://www.washingtonpost.com/blogs/post-tech/post/sony-epsilon-support-national-data-breach-bill/2011/06/02/AG34tvHH_blog.html); Christopher Drew, *Stolen Data is Tracked to Hacking at Lockheed*, N.Y. Times (June 3, 2011), [http://www.nytimes.com/2011/06/04/technology/04security.html?\\_r=3](http://www.nytimes.com/2011/06/04/technology/04security.html?_r=3); Press Release, Southern California Medical-Legal Consultants, *Possible Data Breach Discovered and Contained* (June 11, 2011), <http://www.scmclc.com/press.htm>; 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>; SpartanburgRegional, *Letter to Patients*, (May 2011), <http://www.spartanburgregional.com/pages/patientnotice.aspx>; Carol M. Ostrom, *20,000 Swedish Employees Personal Data Breached*, The Seattle Times (July 20, 2011) [http://seattletimes.nwsourc.com/html/localnews/2015674739\\_databreach21m.html](http://seattletimes.nwsourc.com/html/localnews/2015674739_databreach21m.html).

Many of the data breaches in the non-financial sector still involve the loss of consumers' financial information. For example, gaming companies collect a great deal of financial information. The data breach that affected Sony's PlayStation Network in April exposed the credit card data of 77 million users.<sup>23</sup> The impact of the breach was likely worsened by the fact that Sony waited one week before notifying customers.<sup>24</sup> Examples like Sony's are particularly important because despite the risk to massive amounts of personal and financial data, the privacy risks of online gaming have received little attention from the media or from the federal government.

It is almost impossible to overstate the seriousness of the problem of data breach in the United States. The FBI ranks cyber-attacks as the third greatest threat currently facing the United States, eclipsed only by nuclear warfare and other weapons of mass destruction.<sup>25</sup> According to the Privacy Rights Clearinghouse 500 million sensitive records have been compromised since 2005.<sup>26</sup> The actual number is likely much higher, as many data breaches are never reported in the media.<sup>27</sup> (The Privacy Rights Clearinghouse provides extensive reporting on security breach incidents, including a detailed Chronology that analyzes by year breaches across a wide range of activities and organizations.)<sup>28</sup>

These problems are going to get worse. Indeed, 2011 has already been labeled the "year of the data breach."<sup>29</sup> Financial transactions have already largely moved away from paper, and they are increasingly moving away from the personal hard drive as well. One firm estimates that the global cloud computing market will grow nearly 300 percent by 2014.<sup>30</sup> As more sensitive data moves into the cloud, as we become more dependent on electronic financial records, and as 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.

There are several risks to consumers from these data breaches. The most obvious risk is identity theft, which according to the Federal Trade Commission, has been the number one consumer concern for the past decade.<sup>31</sup> EPIC has previously said that the financial services

---

<sup>23</sup> Liana B. Baker and Jim Finkle, *Sony PlayStation suffers massive data breach*, Reuters (April 26, 2011), <http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426>.

<sup>24</sup> *Id.*

<sup>25</sup> Rick C. Hodgin, *FBI ranks cyber attacks third most dangerous behind nuclear war and WMDs*, TG Daily (Jan. 7, 2009) <http://www.tgdaily.com/security-features/40861-fbi-ranks-cyber-attacks-third-most-dangerous-behind-nuclear-war-and-wmds>.

<sup>26</sup> Privacy Rights Clearinghouse, *500 Million Sensitive Records Breached Since 2005*, <http://www.privacyrights.org/500-million-records-breached> (August 26, 2010).

<sup>27</sup> *Id.*

<sup>28</sup> Privacy Rights Clearinghouse, *Chronology of Data Breaches*, <http://www.privacyrights.org/data-breach>.

<sup>29</sup> See, e.g., Laura Mather, *The Next New Cyberdefense Strategy: Monitor Everything*, TechNewsWorld (Aug. 27, 2011) <http://www.technewsworld.com/story/73162.html?wlc=1315672890>

<sup>30</sup> See Eugene A. Ludwig, *Data Insecurity is a Systemic Threat*, BankThink (Aug. 16, 2011) <http://www.americanbanker.com/bankthink/breach-hack-data-security-systemic-risk-1041244-1.html>.

<sup>31</sup> Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2010,

industry bears some blame for identity theft concerns because the credit granting system and electronic payment mechanisms are designed in a way that makes committing fraud easy.<sup>32</sup> The industry favors convenience over security because tolerating some identity theft is often more profitable for companies.<sup>33</sup>

We have also cautioned against the financial services industry's solution of requiring more personal information, including biometric systems, to authorize charges. These systems raise serious privacy and security risks.<sup>34</sup> Instead, we suggest that the best way to minimize the problem of identity theft is to reduce the industry's use of the social security number as a personal identifier.<sup>35</sup>

Unfortunately, identity theft is only one risk from unauthorized access to personal information.<sup>36</sup> Unauthorized access may be gained for other purposes that cause harm to the individual, such as stalking, corporate espionage, extortion, or to supply information that will be used in 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. Spear phishing is a more effective and targeted version of phishing as the source of the e-mails sent to the potential victims comes from a supposedly trusted or known source.<sup>37</sup> 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.

#### *New Threats to Web Site Security Certificates*

In addition to data breaches in the financial sector, consumers are facing a new threat to their private information from security breaches at companies that issue digital security certificates.<sup>38</sup> In August 2011, the web security firm DigiNotar, a holder of digital security certificates, revealed that it had been breached by a computer criminal who stole authentication certificates used by dozens of popular companies, including Google, Microsoft, Facebook, Twitter, and Yahoo, as well as government entities like Israel's Mossad, Britain's MI6, the CIA,

---

<http://www.ftc.gov/opa/2011/03/topcomplaints.shtm>; Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2009, <http://www.ftc.gov/opa/2010/02/2009fraud.shtm>; Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2008, <http://www.ftc.gov/opa/2009/02/2008cmpts.shtm>; Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2007, <http://www.ftc.gov/opa/2008/02/fraud.shtm>.

<sup>32</sup> EPIC, Identity Theft, <http://epic.org/privacy/idtheft/> (last visited June 17, 2011).

<sup>33</sup> *Id.*

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> 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>.

<sup>37</sup> Ross Kerber and Diane Bartz, *Analysis: Data Breach Shows New "Spear-Phishing" Risk*, Reuters (April 5, 2011), <http://www.reuters.com/article/2011/04/05/us-hackers-epsilon-idUSTRE7336DZ20110405>

<sup>38</sup> The Associated Press, *Hacking in the Netherlands Took Aim at Internet Giants*, New York Times (Sept. 5, 2011), <http://www.nytimes.com/2011/09/06/technology/hacking-in-the-netherlands-broadens-in-scope.html?hpw>.

and most of the Web sites of the Dutch government.<sup>39</sup> In total, fraudulent certificates for 531 domains were generated.<sup>40</sup>

Digital security certificates are used to authenticate Web sites and to ensure the security of communications between a Web site and a user's browser. With fraudulent security certificates, a computer criminal could direct users to fake websites and trick them into revealing their usernames, passwords, and other private information. For example, the holder of a fraudulent Google certificate could set up a website under a legitimate Google domain name. Consumers who visited such a site would put their personal information at risk. Technology experts believe the attack is connected to Iran, citing the presence of nationalist slogans in Farsi and the fact that only a government with control over an Internet service provider could direct Internet traffic to the spoofed Web sites.

The computer criminal allegedly responsible for the attacks calls himself the "Comodohacker," a reference to a breach at Comodo, another holder of digital certificates, for which he claimed credit. Though he claims to be an independent, Iranian software engineering student, Comodohacker admits to sharing the information he uncovers with Iran.<sup>41</sup>

In the years ahead, the threat posed to consumers by fraudulent security certificates will increase. Indeed, only a few days ago the digital certificate firm GlobalSign had its Web site breached by a computer criminal.<sup>42</sup> As a result of these threats, consumers are exposed to a "new and extremely dangerous cyber crime threat"<sup>43</sup> when they interact with companies, like those in the financial sector, that are involved in the collection of sensitive information.

### General Recommendations

In our view, none of the current legal frameworks provide adequate safeguards for consumers, bank customers, depositors, and others who provide personal information to obtain financial services.

In general, EPIC supports cyber security laws that feature an opt-in approach for companies' use of personal information, that allow for private rights of action for consumers, and that do not pre-empt state data breach legislation. To address similar data breach problems in the communications sector, EPIC has recommend several security measures that telecommunications firms could use to protect the privacy of customer data.<sup>44</sup> These measures include: authentication

---

<sup>39</sup> *Id.*

<sup>40</sup> Gregg Keizer, *Hackers steal SSL certificates for CIA, MI6, Mossad*, ComputerWorld (Sept. 4, 2011), [http://www.computerworld.com/s/article/9219727/Hackers\\_steal\\_SSL\\_certificates\\_for\\_CIA\\_MI6\\_Mossad](http://www.computerworld.com/s/article/9219727/Hackers_steal_SSL_certificates_for_CIA_MI6_Mossad).

<sup>41</sup> Somini Sengupta, *Hacker Rattles Security Circles*, NY Times (Sept. 11, 2011), <http://www.nytimes.com/2011/09/12/technology/hacker-rattles-internet-security-circles.html>.

<sup>42</sup> *Id.*

<sup>43</sup> Matt Liebowitz, *Cracked digital certificates endanger 'web of trust'*, MSNBC.com (Sept. 7, 2011) [http://www.msnbc.msn.com/id/44430823/ns/technology\\_and\\_science-security/t/cracked-digital-certificates-endanger-web-trust/#.Tm5gmo6omVo](http://www.msnbc.msn.com/id/44430823/ns/technology_and_science-security/t/cracked-digital-certificates-endanger-web-trust/#.Tm5gmo6omVo).

<sup>44</sup> EPIC, *Petition to the Federal Communications Commission for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information* (Aug. 30, 2005) at 15, available at <http://epic.org/privacy/iei/cpnipet.html>.

by consumer-set passwords instead of biographic identifiers like date of birth or social security number; audit trails that record all instances where a customer's record is accessed; encryption of stored data; notice to the affected individuals and the relevant agency when there is a security breach; and limiting data retention by either deleting call records after they are no longer needed or divorcing identification data from the transactional data.<sup>45</sup> Similar security measures should be applied in the financial sector.

Data breach notification laws can also help us understand the extent of the data breach problem so that better safeguards and practices can be developed. EPIC supports notification laws that contain data minimization, that require short time periods for notification, that contain a sufficiently broad definition of "Personally Information," and that take advantage of social networks and text messaging for notification.

Finally, we favor the development of cyber security policies that are open to public review and comment, that respect the role of the private sector, and that safeguard the rights of consumers and users.

I will briefly outline each of these recommendations below.

#### *Opt-In Standard*

EPIC has previously suggested that laws such as the Gramm-Leach-Bliley Act ("GLBA") can be improved by giving consumers the option to opt-out of some sharing of personal financial information.<sup>46</sup> Currently, GLBA gives consumers the right to opt-out from a limited amount of nonpublic personal information sharing. Specifically, a consumer can direct the financial institution to not share information with unaffiliated companies.

These types of opt-out approaches unfairly place the burden on the individual to protect privacy and thus weaken customer power to control their financial information. Most privacy and opt-out policies are usually convoluted, confusing, and misleading since they are created by entities whose interests are better served when there is no effective notice. Instead, financial institutions should implement an opt-in approach to the use of personal information because this minimizes any unwanted or unknowing disclosure of information and places the burden of responsibility on those actors who will gain from the disclosure of information.

#### *Private Right of Action*

EPIC supports data protection laws that contain a private right of action for consumers.<sup>47</sup> Private rights of action strengthen enforcement and allow individuals to seek remedies.

---

<sup>45</sup> *Id.*

<sup>46</sup> *Hearing on "Cybersecurity and Data Protection in the Financial Sector,"* (June 21, 2011) (Testimony of Marc Rotenberg, EPIC, to Senate Committee on Banking, Housing, and Urban Affairs), *available at* [http://epic.org/privacy/testimony/EPIC\\_Senate\\_Banking\\_Testimony%20\\_6\\_21\\_11.pdf](http://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf); *see also* EPIC, The Gramm-Leach-Bliley Act, <http://epic.org/privacy/glba/> (last visited September 11, 2011).

<sup>47</sup> *See Hearing on "Cybersecurity and Data Protection in the Financial Sector,"* (June 21, 2011) (Testimony of Marc Rotenberg, EPIC, to Senate Committee on Banking, Housing, and Urban Affairs), *available at*



Additionally, because it is often difficult to place a dollar value on data breaches and privacy infringements, it is important that any 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 rights of action. 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.<sup>48</sup>

### *Data Breach Notification*

EPIC supports notification bills that contain data minimization provisions.<sup>49</sup> 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 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 this vulnerability. The simple message to business should be “if you can’t protect it, don’t collect it.”

Data minimization provisions like those found in the Secure and Fortify Electronic Data Act (“SAFE Data Act”) are a good start, but 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 no 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 pending requests or orders for access to such information . . . .<sup>50</sup>

Second, EPIC supports short time period requirements for notification. EPIC previously testified before the House Commerce Committee in support of the SAFE Data Act’s 48-hour requirement for breach notification.<sup>51</sup> Short time periods require companies to respond quickly

---

[http://epic.org/privacy/testimony/EPIC\\_Senate\\_Banking\\_Testimony%20\\_6\\_21\\_11.pdf](http://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf).

<sup>48</sup> 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).

<sup>49</sup> See *Legislative Hearing on “Discussion Draft of H.R. \_\_\_\_\_, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach”* (June 15, 2011) (Testimony of Marc Rotenberg, EPIC, to House Committee on Energy and Commerce and Subcommittee on Commerce, Manufacturing, and Trade), available at [http://epic.org/privacy/testimony/EPIC\\_Testimony\\_House\\_Commerce\\_6-11\\_Final.pdf](http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf).

<sup>50</sup> Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (Nov. 5, 1988), *codified at* 18 U.S.C. 2710.

<sup>51</sup> See *Legislative Hearing on “Discussion Draft of H.R. \_\_\_\_\_, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach”* (June 15, 2011) (Testimony of Marc

when there is a problem and allow consumers to react more quickly and take preventative or mitigating actions.

Notification laws should also contain a sufficiently broad definition of “Personal Information.” This definition is critical because, as with most privacy bills, this definition will determine when the obligations of a notification law should be applied and when they can be basically ignored. EPIC has previously suggested that bills such as the SAFE Data Act should define Personal Information as information that “identifies or could identify a particular person,” followed by the examples cited in the Act as illustrations, with those illustrations qualified by the phrase “including, but not limited to.”<sup>52</sup> This approach is technology neutral, less dependent on the rulemaking process, and more likely to adapt over time.

Additionally, the definition of Personal Information should *not* exempt “public record information” available from federal, state, or local government systems that was acquired by the company that suffered the breach for public purposes. 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 correct the problem, it is quite likely the breach will occur again. Thus, even when there is no immediate harm to the individual, the problem remains and the security obligation should apply. Also, I would not assume that a data breach of public information merely discloses the equivalent of what could be found through public data sources. 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 single government record system.

Finally, breach notification laws should take advantage of text messaging and social networks as methods of notification. A text message would not be an effective substitute for written notification or email, because it is essentially ephemeral. But it is an effective way of quickly notifying consumers of the problem and of making them 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 a 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 through 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.

### *Preemption*

Many Senate and House data breach bills, such as the SAFE Data Act, preempt state laws that have similar security obligations as well as state laws that provide for data breach

---

Rotenberg, EPIC, to House Committee on Energy and Commerce and Subcommittee on Commerce, Manufacturing, and Trade), available at [http://epic.org/privacy/testimony/EPIC\\_Testimony\\_House\\_Commerce\\_6-11\\_Final.pdf](http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf).

<sup>52</sup> *Id.*

notification. If enacted, the federal laws would preempt more effective state information security legislation and foreclose future legislative innovation at the state level.

EPIC's view is that it would be a mistake to adopt preemption provisions 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. 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.<sup>53</sup>

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, for example, has recently updated its data breach notification law to specify the information that should be provided by data holders to individuals in the event of a breach and to require that the state Attorney General be notified in the event of a large breach.<sup>54</sup> Massachusetts is also considered updates to its data breach law in response to new threats.<sup>55</sup> It is very 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.

#### *White House Draft Cybersecurity Legislation*

The White House has recently unveiled a Cybersecurity Legislative Proposal that seeks to "improve critical infrastructure protection by bolstering public-private partnerships with

---

<sup>53</sup> See e.g. Cal. Civ. Code 1798.82 (2011).

<sup>54</sup> See EPIC, California Passes Updated Data Breach Legislation, <http://epic.org/2011/09/california-passes-updated-data.html> (last visited September 11, 2011).

<sup>55</sup> Jason Gavejian, *California and Massachusetts Legislatures Push Data Breach and Security Bills*, 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/>.

improved authority for the Federal government to provide voluntary assistance to companies and increase information sharing.”<sup>56</sup>

The Proposal would grant DHS the authority to develop and conduct risk assessments of Critical Information Infrastructure (CII) and foster the development...of essential information security technologies and capabilities for protecting federal systems and [CII].<sup>57</sup> CII is defined as “any physical or virtual information system that controls, processes, transmits, receives, or stores electronic information in any form...that is vital to the functioning of critical infrastructure, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, *national economic security*, or national public health or safety, or owned or operated by or on behalf of a state, local, tribal, or territorial government entity.”<sup>58</sup> This would seem to include the financial services industry in its broad sweep.

EPIC welcomes the White House's efforts to strengthen our nation's cybersecurity and privacy protections for financial information. While the White House states that “[p]rotecting civil liberties and privacy rights remain fundamental objectives in the implementation of the [Cybersecurity Legislation],”<sup>59</sup> we would warn the Subcommittee about the provisions giving control over “critical information infrastructure” (CII) to the DHS. The definition of CII is quite broad and it is important to ensure that any cybersecurity proposal does not lead to increased government monitoring of private information.

Furthermore, it is important to reiterate that cyber security policies should allow for public review and comment, respect the role of the of the private sector, and safeguard the rights of consumers and users. I make this point because there is the very real risk that in the realm of cyber security much of the authority for legal compliance and technical standard-setting could be too easily turned over the National Security Agency. Already the NSA has suggested that the government may need to monitor private networks and assist in the development of key technical standards.

This would be a grave mistake. In fact, if the NSA had had its way twenty years ago in the battle over cryptography standards for the Internet, it is quite likely that the vulnerability of US networks to attack would be much greater than it is today. This should be of particular concern to those watching closely the recent cyber security developments in the financial services sector.

### *Department of the Treasury’s Financial Crimes Enforcement Network Reporting Proposal*

---

<sup>56</sup> See White House: Legislative Language, Law Enforcement Provisions Related to Computer Security (May 12, 2011), available at <http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf>. [hereinafter “White House Legislative Proposal”].

<sup>57</sup> White House Legislative Proposal, *supra* note 39 at 22.

<sup>58</sup> *Id.* at 20. Emphasis added.

<sup>59</sup> The White House, *The Comprehensive National Cybersecurity Initiative*, <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative> (last visited June 20, 2011).

The Treasury Department's Financial Crimes Enforcement Network recently proposed new regulations that would require banks to report all international electronic money transfers.<sup>60</sup> The regulation would significantly expand the transfer of bank record information to the US Treasury Department and law enforcement agencies. Where such data collection is necessary, EPIC favors a narrowly focused approach in which the government knows beforehand which data is associated with terrorist financing, and pursues only that data.

## Conclusion

Financial privacy protections need to be strengthened in the U.S. The rise in significant data breaches and the problem of I.D. theft indicate clearly that more must be done in this area to protect financial data. Moreover, the emergence of attacks on issuers of digital certificates, raises new concerns about online security.

We support legislation that strengthens safeguards for consumer information and promotes data minimization practices. Specifically, we urge the adoption of techniques that minimize the collection of personally identifiable information. These techniques reduce the risk of cyber attack and minimize the risk to consumers when attacks occur.

We also support strong notification requirements so that consumers are not left out of the loop when breaches occur. Private rights of action and statutory damages provisions are also important to empower consumers and increase enforcement. Companies also 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.

We broadly favor Administration efforts to promote cybersecurity. But we caution against Government overreaching that leads to increased monitoring of private communications or technical standard-setting that makes communications and databases more vulnerable to attack.

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



---

<sup>60</sup> See EPIC, *US Government Seeks to Monitor All Money Transfers*, <http://epic.org/2010/09/us-government-seeks-to-monitor.html> (last visited September 11, 2011).

United States House of Representatives  
Committee on Financial Services

"TRUTH IN TESTIMONY" DISCLOSURE FORM

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee on Financial Services require the disclosure of the following information. A copy of this form should be attached to your written testimony.

<b>1. Name:</b>	<b>2. Organization or organizations you are representing:</b>
MARC ROTENBERG	ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
<b>3. Business Address and telephone number:</b>	
	
<b>4. Have <u>you</u> received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?</b>	<b>5. Have any of the <u>organizations you are representing</u> received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?</b>
<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<b>6. If you answered .yes. to either item 4 or 5, please list the source and amount of each grant or contract, and indicate whether the recipient of such grant was you or the organization(s) you are representing. You may list additional grants or contracts on additional sheets.</b>	
N/A	
<b>7. Signature:</b> 	

Please attach a copy of this form to your written testimony.