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

Senate Committee on Banking, Housing, and Urban Affairs

June 21, 2011
Dirksen Senate Office Building, Room 538
Washington, DC

Mister Chairman and Members of the Committee, 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.

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

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.

There have been several cybersecurity proposals and legislation introduced recently. We are encouraged by these efforts, and they all represent significant steps forward in the protection of consumers' financial information. The current laws do not adequately protect consumers, and the gaps need to be filled by strong legislation. 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.

- In May, inadequate security measures at Citigroup exposed customer names, account numbers, and contact information for more than 360,000 customers.[1] 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]

[1] 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.
[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.

- On June 15, 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.

- In late May 2011, news reports revealed that a Bank of America insider had leaked the detailed personal information of many of the bank's customers.[5] As a result of the data breach, the affected customers have lost millions of dollars from their accounts.[6] This outcome is particularly troublesome considering that Bank of America is the largest bank in the U.S.[7]

- In January of 2009, weak network security caused a breach at Heartland Payment Systems, a credit card payment processing firm.[8] The company has settled with American Express, Mastercard, Visa, and Discover due to claims raised as a result of the data security breach.[9] It is estimated that millions of consumers' personal card numbers were stolen as a result of the breach.[10]

- 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.[11] The data breach resulted in the loss of personal information of approximately 5,000 consumers.[12]

- 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.[14] The company eventually settled, paying almost $10 million to states,[15] $24 million to Mastercard,[16] and $41 million to Visa.[17]

---

[5] 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

[6] *Id*.

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

[8] 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

[9] 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

[10] *Id*.

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

[12] *Id*.

[14] 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

[15] *Id*.

[16] 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

[17] 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

These problems are not unique to the financial sector. Other companies that have recently lost control of sensitive customer information include: Epsilon, Lockheed Martin, PlayStation, and the Southern California Medical-Legal Consultants. These breaches affected millions of consumers.[18]

According to the Identity Theft Resource Center, there have been at least 195 data breaches in 2011.[19] In 2010, there were 662 breaches and over 16 million records compromised.[20] 58 of those breaches occurred at financial institutions.[21] According to the Privacy Rights Clearinghouse, 500 million sensitive records have been breached since 2005.[22] The actual number is likely much higher, as many data breaches are never reported in the media.[23]

And of course breaches are not limited to the financial services sector. In just the last few weeks, data breaches have been reported at the CIA, the International Monetary Fund, and with the Senate's own computer network.

These problems are going to get worse. As more sensitive data moves into the cloud, as we become more dependent on electronic financial 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.

There are several risks to consumers from these data breaches. The most obvious risk is identity theft, which has been the number one consumer concern for the past decade.[24] EPIC has previously said that the financial services industry bears some blame

---

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

[19] Identity Theft Resource Center, 2011 Data Breach Stats 7 (June 7, 2011), http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202011.pdf.

[20] *Id*.

[21] Linda McGlasson, *2010 Data Breach Timeline*, (December 28, 2010), http://www.bankinfosecurity.com/articles.php?art_id=2378&opg=1.

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

[23] *Id*.

[24] Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2010, 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

for identity theft concerns because the credit granting system and electronic payment mechanisms are designed in a way that makes committing fraud easy.[25] The industry favors convenience over security because tolerating some identity theft is often more profitable for companies.[26]

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.[27] 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.[28]

Unfortunately, identity theft is only one risk from unauthorized access to personal information. [29] 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 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. 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.[30] 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.

To address similar problems in the communications sector, EPIC has recommend several security measures that telecommunications firms could use to protect the privacy of customer data.[31] These measures include: authentication 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.[32] Similar security measures should be applied in the financial sector.

Consumer Complaints in 2007, http://www.ftc.gov/opa/2008/02/fraud.shtm.

[25] EPIC, Identity Theft, http://epic.org/privacy/idtheft/ (last visited June 17, 2011).

[26] *Id*.

[27] *Id*.

[28] *Id*.

[29] 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.

[30] 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

[31] 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.

[32] *Id*.

It is also important to note the related cybersecurity risks for online voting systems, as there is similar potential for abuse. I bring this to your attention because there is now an effort to promote online voting in the United States over the Internet and by fax, even thought studies have shown that these networks lack the necessary security to ensure the integrity of online voting.[33] The recent spate of attacks on US financial institutions should set off warning bells for those who favor Internet-based voting.

Current Law

There are several legal frameworks that seek to address data protection in the financial sector. But in our view, none of them provide adequate safeguards for consumers, bank customers, depositors, and others who provide personal information to obtain financial services.

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999,[34] regulates financial institutions--businesses that are engaged in banking, insuring, stocks and bonds, financial advice, and investing. The GLBA requires these financial institutions to develop precautions to ensure the security and confidentiality of "customers' nonpublic personal information," to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[35]

The GLBA also codifies protections against pretexting, which is the practice of obtaining personal information through false pretenses.[36] While the GLBA imposes some data breach notification obligations on financial institutions, no specific deadline for notification is required.[37]

The GLBA is enforced by "the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to financial institutions and other persons subject to their jurisdiction under applicable law."[38] There is no private right of action.

---

[33] Federal Voting Assistance Program, http://www.fvap.gov/index.html; *but see* Regenscheid, A. and Hastings, N., A Threat Analysis on UOCAVA Voting Systems, National Institute of Standards and Technology (2008) available at http://vote.nist.gov/uocava-threatanalysis-final.pdf; David Jefferson, Avi Rubin & Barbara Simons, A Comment on the May 2007 DoD Report on Voting Technologies for UOCAVA Citizens (2007) available at http://www.servesecurityreport.org/SERVE_Jr_v5.3.pdf.

[34] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq*.

[35] 15 U.S.C. § 6801(a)-(b).

[36] 15 U.S.C. §§ 6821-6827

[37] *See* Federal Deposit Insurance Corporation, Financial Institution Letter, *Final Guidance on Response Programs*, http://ithandbook.ffiec.gov/media/resources/3391/fdi-fil-27-2005.pdf (April 27. 2005).

[38] *Id*.

Many agencies, including the Federal Trade Commission (FTC)[40] are involved with enforcing the GLBA and other financial regulations. Other enforcement entities include the Commodity Futures Trading Commission, the Department of the Treasury, the Federal Deposit Insurance Corporation, the Securities and Exchange Commission, and the National Credit Union Administration. However, enforcement has been weak. [41]

Given the GLBA's weak data breach protections and lack of strong enforcement mechanisms, there is a clear need for further legislation in this area. The Gramm–Leach–Bliley Act burdens consumers because of the opt-out standard.[42] Instead, EPIC has suggested that financial institutions implement an opt-in approach for companies' use of personal information to minimize any unwanted or unknowing disclosures of information.[43] Additionally, we support the inclusion of a private right of action to strengthen enforcement and allow individuals to seek remedies.

However, it is important to note that the opt-out standard in Gramm-Leach-Bliley was tempered by the fact that the GLBA does not contain a preemption provision, which allowed states to enact stronger laws, as discussed below.[44]

EPIC appreciates the recent efforts of the Committee to update the privacy provisions in the financial services sector. The Committee considered the Data Security Acts of 2010 and 2007, but they did not leave the Committee. The Committee marked up The Credit Rating Agency Reform Act of 2006 that was signed into law and helped prevent the misuse of nonpublic information. The Committee also held hearings on August 5, 2009 to enhance the regulation of credit rating agencies and on March 3, 2009 concerning consumer protections in financial services.

State Data Breach Laws

As of October 12, 2010, forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have all enacted data breach notification laws.[45] Most states have followed the lead of California's data breach notification law.

---

[40] The FTC does not bring many enforcement actions under the GLBA. But, under Section 5 of the FTC Act, since 2001, the FTC has brought 34 cases against businesses that failed to protect consumers' personal information. The Commission has recently recommended that legislation be passed to require companies to implement reasonable procedures to protect consumer data.

[41] *See, e.g.,* Complaint to the Federal Trade Commission by AVM, www.workingre.com/workingre/AVM-Complaint-Washington.pdf (noting that "[w]hat is not understood is the lack of enforcement by the Federal Functional Regulators identified in Sec 505 of G-L-B Act"); Allan Holmes, *The Global State of Information Security*, CIO Magazine, September 15, 2006 at 82, 91(noting that in 20065, 17% of U.S. organizations reported being out of compliance with the GLBA).

[42] EPIC, The Gramm-Leach-Bliley Act, http://epic.org/privacy/glba/ (last visited June 17, 2011).

[43] *Id*.

[44] *See* 15 U.S.C. § 6807.

[45] NSCL, State Security Breach Notification Laws (last updated Oct. 12, 2010) http://www.ncsl.org/default.aspx?tabid=13489.

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.

Current Cybersecurity Proposals

As you aware, the White House has recently introduced a series of legislative proposals to strenghten cybersecurity and to create a comprehensive framework for security standards. Several of these initiatives we favor; about others we have expressed concern. We do believe that that *Personal Data Privacy and Security Act of 2011*, which has been introduced several times before is a step in the right direction.

This bill, introduced by Senator Leahy, is designed to prevent and mitigate identity theft, to require notice of security breaches, to enhance criminal penalties, and provide other protections against security breaches, fraudulent access, and misuse of personally identifiable information.[46]

Financial institutions are exempt from major provisions of the bill, including the section providing for transparency and accuracy of data collection, as well as the data privacy and security program for personally identifiable information.[47]

The security breach notification rules in the bill would apply to financial institutions, but there is a safe harbor provision and a financial fraud prevention exemption.[48] We think this bill is an important step forward, and support the application of breach notification rules to financial institutions. At the same time, we would like to see the elimination of exemptions that weaken the bill and we have specifically recommended that federal breach notification statutes operate as a floor and not a ceiling.

Secure and Fortify Electronic Data Act (SAFE Data Act)

The SAFE Data Act, introduced by Representative Bono Mack, is a bill designed "to protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach."

The Bill applies to "personal information," which includes a "financial account number, or credit or debit card number, and any required security code, access code, or

[46] Personal Privacy Data and Security Act of 2011, S.1151 (2011-2012).
[47] *Id*. at Sec. 201 (transparency and accuracy of data collection); Sec 302 (data privacy and security program for PII).
[48] *Id*. at Sec 311 and 312

password that is necessary to permit access to an individual's financial account." As such, any person who "owns or possesses data containing personal information related to that commercial activity…to establish and implement policies and procedures regarding information security practices for the treatment and protection" of that information.

However, any entity governed under title V of the Gramm-Leach-Bliley Act (GLBA) is exempt from any requirements of the SAFE Data Act for any activities governed by the GLBA.

The Act also includes requirements for data breach notification, including special requirements for third party agents and service providers.

EPIC testified last week in the House Commerce Committee about this Act.[49] EPIC supported recent changes in the bill that would require companies to act more quickly in case of breach and encourage minimization of data collection. EPIC also recommended changes in the bill to strengthen enforcement, require notification, protect identifiers linked to individuals, and ensure that state governments are able to respond on behalf of consumers as new problems emerge.

Department of Commerce Cybersecurity Green Paper

The Department of Commerce has released a Green Paper that will eventually lead to the development of "public policies and private sector norms whose voluntary adoption could improve the overall cybersecurity posture of private sector infrastructure operators, software and service providers, and users outside the critical infrastructure."

The Paper states that security standards will increase the reliability of online transactions, and references the "National Strategy for Trusted Identities in Cyberspace" (NSTIC) as a means to maintain security in sensitive transactions, including banking. The Green Paper does not otherwise impose regulate the financial industry.

White House Draft Cybersecurity Legislation

The White House Cybersecurity Legislative Proposal seeks to "improve critical infrastructure protection by bolstering public-private partnerships with improved authority for the Federal government to provide voluntary assistance to companies and increase information sharing."[50]

---

[49] *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.

[50] *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"].

The Proposal includes a national standard for data breach notification. Any entity that collects "sensitive personally identifiable information" (SPII) must commit to data breach notification, which pre-empts all state notification laws, whenever the SPII is "reasonably believed to have been…accessed or acquired, unless there is no reasonable risk of harm or fraud to such individual."[51] The White House Proposal defines SPII to include "a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code," or a combination of elements that includes any of the aforementioned information.

The section on "Critical Infrastructure Cybersecurity Plans" is also relevant to the work of this Committee. The Administration deems the financial sector—along with the electricity grid and transportation networks—to be part of the critical infrastructure.[52] The Administration states that it seeks to "ensure that critical-infrastructure operators are accountable for their cybersecurity."[53]

The proposal envisions that the Department of Homeland Security (DHS) will work with the private sector to ensure that critical infrastructure operators, such as financial sector institutions, "develop their own frameworks for addressing cyber threats."[54] A third-party, commercial auditor—and the Securities and Exchange Commission, if applicable—will then review the institutions' "cybsercurity risk mitigation plans" to ensure that the plan is sufficient.[55] If the plan is inadequate, DHS can modify the plan or work with the institution to improve it.[56]

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].[59] 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."[60] This would seem to include the financial services industry in its broad sweep.

---

[51] Letter from Jacob J. Lew, Director, Executive Office of the President Office of Management and Budget, to the Honorable John Boehner, Speaker of the House of Representatives and Joseph R. Biden, President of the Senate (May 12, 2011), *available at* http://www.whitehouse.gov%2Fsites%2Fdefault%2Ffiles%2Fomb%2Flegislative%2Fletters%2FCybersecurity-letters-to-congress-house-signed.pdf.

[52] Press Release, The White House, Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Id.*

[59] White House Legislative Proposal, *supra* note 39 at 22.

[60] *Id*. at 20. Emphasis added.

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],"[61] we would warn the Committee 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.

Analysis

The legislative proposals in the House and Senate exempt financial institutions covered by the GLBA from much of the significant provisions of the proposals. However, they do contain breach notification rules that would apply to banks, which would help fill the gap left by the GLBA, provided that these rules are coupled with strong meaningful enforcement from federal agencies.

In contrast, the White House Cybersecurity Proposal does not specifically exempt financial institutions or GLBA covered entities from its proposed regulations. Therefore, banks could be covered under the Proposal.

In general we favor the development of cyber security policies that are open to public review and comment, that respect the role of the of the private sector, and that 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 it's way twenty years 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.

Preemption

The Senate and House data breach bills preempt state laws that have similar security obligations as well as state laws that provide for data breach notification. If enacted, the federal laws would preempt more effective state information security legislation and foreclose future legislative innovation at the state level.

My own view is that it would be a mistake to adopt preemption provisions of this

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

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. [63]

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.[64] 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.

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.

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 broadly favor Administration efforts to promote cybersecurity. But we caution against Government overreaching that leads to increased monitoring of private

[63] *See e.g.* Cal. Civ. Code 1798.82 (2011).
[64] 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/

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.