Subcommittee on Commerce, Manufacturing and Trade
June 15, 2011 Hearing on Data Security and Breach Notification Legislation
Summary of Testimony of Robert W. Holleyman II (BSA)

BSA believes Congress must pass this year federal legislation that requires organizations to secure the sensitive personal information they hold, and to notify individuals when that security has been breached, can effectively enhance consumers' trust. BSA recommends that such legislation pursue the following objectives, which we are pleased to see reflected in the draft bill.

Establish a uniform national standard that preempts state laws—Forty-six States, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands had enacted data breach notification laws. This patchwork has created a compliance nightmare for businesses, as well as confusion for consumers who receive notices from a multiplicity of sources. We are heartened by the draft bill's inclusion in section 6 of language pre-empting state laws, and suggest that the scope of preemption be clarified to cover notification to government agencies as well as private parties.

Prevent excessive notification—Some breaches create great risks of harm to consumers, while others create little to no risk. Currently, most state data breach laws require notification even when no risk exists. Over notification is likely to confuse consumers, who will then fail to take appropriate action when they are truly at risk. We believe notification should be required only in those instances where an unauthorized disclosure presents a significant risk of material harm. We are pleased that section 3(f) of the draft bill takes a risk-based approach to breach notification. We recommend that the threshold be "*significant risk,*" to ensure that only genuine risk is notified.

Exclude data that has been rendered unusable, unreadable, or indecipherable—Data not be subject to breach notification if it has been rendered unusable, unreadable, or indecipherable through practices or methods, such as encryption, redaction, or access controls, which are widely-accepted as effective industry practices or industry standards. The draft bill's section 6(f)(2) provides a market-based incentive for the adoption of strong data security measures. We recommend however that this provision be made technology. As drafted, we are concerned that it may tilt the playing field by setting up a two-tiered approach: while encryption is explicitly listed in the draft bill, other methods would require the sanction of an FTC rulemaking.

Require the use of data security safeguards—in addition to requiring breach notification Congress should prevent breaches from happening in the first place, by requiring organizations that hold sensitive personal information to establish and implement data security policies and procedures. We support the fact that the draft bill does this in section 2. It is also important to avoid over-regulating data custody. While we support the draft bill's requirement that organizations protect the consumer data that they hold, we are concerned that the grant of authority to the FTC, in section 2(a)(1), to develop a body of regulations governing such corporate policies and procedures will in effect make the activity of data custody a regulated activity. The specificity of the data security requirements in the draft bill renders unnecessary the supplemental layer of regulation that would be created by the FTC under the draft bill. We should avoid creating a new compliance burden that does not offer increased data security.

Provide appropriate enforcement—BSA supports the draft bill's grant of authority to the FTC and State AGs to vigorously enforce to defend consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses. We strongly recommend the inclusion in the bill of a provision explicitly stating that it does not create a private right of action.

U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Commerce, Manufacturing and Trade

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

Testimony of Robert W. Holleyman II
President & CEO, Business Software Alliance

Wednesday, June 15, 2011

Chairman Bono Mack, Ranking Member Butterfield, thank you for holding this hearing today and for inviting me to testify. My name is Robert Holleyman. I am the President and CEO of the Business Software Alliance (BSA.) BSA is an association of the world's leading software and hardware companies. BSA's members create approximately 90% of the office productivity software in use in the U.S. and around the world.[1]

The Business Software Alliance and its member companies strongly support enacting a national data security and data breach notification law, because it is important that we maintain trust and confidence in digital commerce. The time to act is now. This is the fourth Congress to consider such legislation. The need is clear, as are the solutions. We urge you to pass a data security and data breach notification bill this Session.

Over the last 20 years, consumers, businesses and governments around the world have moved online to conduct business, and access and share information. This shift to a digital world has revolutionized personal interactions, education, commerce, government, healthcare, communications, science, entertainment and the arts, etc. It has delivered unprecedented efficiencies and considerable cost savings and it will continue to produce immense benefits to our global society. Looking ahead, into the just-dawning era of cloud computing, these revolutions will only intensify – accompanied by even greater economic and social benefits.

These changes bring with them a number of risks. We all face a variety of online threats, which can undermine trust in the digital environment.

Just ten years ago, the primary threats to security online were vandals and hackers. They chased notoriety and relished the challenge of beating security systems. Their calling cards were breaches, denial of service attacks to bring down popular sites such as eBay and CNN.

But the stakes are now higher: these activities are increasingly motivated by profit. The data mined from breaches can be used to send targeted spam, to impersonate unknowing individuals and steal finances. Increasingly organized criminal enterprises are using the Internet to distribute malware so they can make big money.

BSA commends you for bringing a focus on data security in the digital age. This is a matter of great concern for BSA member companies that engage in electronic commerce and provide much of the infrastructure to make e-commerce possible. Unauthorized disclosures of personal information erode public confidence in the online world. Cloud services are already an important component of how information is developed, managed and stored, and over the coming years we anticipate its importance will grow. But, electronic commerce and cloud computing cannot reach their full potential to contribute to U.S. economic growth without the trust of consumers and businesses. BSA believes that legislation, like the draft bill under consideration today, can be an important component in strengthening trust in the online environment.

[1] The Business Software Alliance (www.bsa.org) is the world's foremost advocate for the software industry, working in 80 countries to expand software markets and create conditions for innovation and growth. Governments and industry partners look to BSA for thoughtful approaches to key policy and legal issues, recognizing that software plays a critical role in driving economic and social progress in all nations. BSA's member companies invest billions of dollars a year in local economies, good jobs, and next-generation solutions that will help people around the world be more productive, connected, and secure. BSA members include Adobe, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, Cadence, CNC/Mastercam, Compuware, Corel, Dassault Systèmes SolidWorks Corporation, Dell, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, PTC, Progress Software, Quark, Quest Software, Rosetta Stone, Siemens, Sybase, Symantec, and The MathWorks.

1. The size and nature of the challenge

Even as consumers share more of their personal information on line, the security and confidentiality of their personal data is threatened: a recent survey of American adults found 68 percent of them were either "very concerned" or "extremely concerned" about identity theft.[2] Over the past several years, the number of significant security breaches has continued to increase.

- A recently released Ponemon study shows that the average cost of a data breach grew to $214 per record compromised in 2010, up from $204 per record in 2009, while the average security incident cost individual companies $7.2 million per breach in 2010, up from $6.43 million in 2007 and $4.7 million in 2006.[3]
- For the eleventh year in a row, identity theft tops the FTC list of U.S. consumer complaints. Of 1,339,265 complaints received in 2010, 250,854 – or 19 percent – were related to identity theft.[4]
- According to the non-partisan *Privacy Rights Clearinghouse*, data breaches have affected a staggering 533 million records containing sensitive personal information since 2005.[5]

As we look ahead, the vast amounts of information that will be stored in the cloud promise to be alluring targets for cybercriminals.

Illicit activity in connection with the Internet has evolved over the past decade. The history of hacking includes tales of both innocuous white-hatted do-gooders looking to help industry clients as well as malevolent thieves looking to steal information for profit. The hapless employee who carelessly loses – or allows to be stolen – a laptop filled with sensitive information to be stolen can also be the source of a breach.

Determining the actual impact of breaches has been difficult. A recent GAO study noted comprehensive data on the consequences of data breaches does not exist. What is clear and what matters most is that companies must do their best to protect the sensitive information of their customers – and they must respond responsibly when any breach does occur.

Today, though, the response to such attacks is complicated for businesses and confusing for customers because of the patchwork of sometimes conflicting state laws. Federal legislation can help clarify and improve the process and allow industry to do what it does best – focus on improving the security of online systems to prevent future attacks and diminish the harm of any actual breach.

2. Business response to the data security challenge

It is clear that organizations that hold sensitive data need to improve their risk management. But this does not necessarily require adopting extraordinary, excessively costly or particularly cumbersome

---

[2] http://arstechnica.com/security/news/2009/10/americans-fear-online-robberies-more-than-meatspace-muggings.ars

[3] http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

[4] http://ftc.gov/opa/2011/03/topcomplaints.shtm

[5] http://www.privacyrights.org/data-breach

security measures: a study conducted by Verizon, the U.S. Secret Service and the Netherlands' High Tech Crime Unit shows that, in 2010, 83 percent of breached organizations were targets of opportunity, and 96 percent of breaches could have been avoided through simple or intermediate controls.[6] In other words, reasonable diligence could make a considerable dent into this problem.

For its part, the technology industry has important responsibilities to respond to this.

First, each and every day our members focus on the trustworthiness of the information technology products, systems and services. As governments, critical infrastructure providers, businesses and consumers worldwide depend upon these technologies, our members undertake significant efforts to reduce their vulnerabilities, improve their resistance to attack and protect their integrity.

Users can be exposed to cybersecurity risks in a great many ways, including when they use counterfeit or unlicensed technologies. Users of counterfeit hardware or software have no assurance of their trustworthiness, and in many cases intentional vulnerabilities – i.e. malware –are found in counterfeits.[7]

Second, our members work diligently to develop security technologies to defend against evolving threats. Users of technology rely on BSA members for innovative solutions that provide layered defenses – from protection at the data and document level to the network and perimeter level – that are adapted to the threats they face and the value of the assets they need to protect.

And finally, our members educate and raise public awareness of cyber risks and how users can protect themselves. Many of our members have developed their own substantial programs to convey these messages, and many offer free security checkup tools. In addition, several BSA members play a leading role in the National Cyber Security Alliance (NCSA),[8] a non-profit organization supported by public and private sector partners. NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school.

3. Objectives of federal data security and breach notification legislation

BSA believes federal legislation that requires organizations to secure the sensitive personal information they hold, and to notify individuals when that security has been breached, can effectively enhance consumers' trust. Federal legislation establishing a uniform national framework would benefit businesses and consumers alike. It would replace state laws that are generally good, but that are now creating confusion and difficulties. This uniformity would best serve the interests of businesses, but it is important to note that it would also best serve those of consumers by guaranteeing a high level of protection not just in the response to a breach, but also in its prevention.

BSA recommends that federal data security and breach notification legislation pursue the following objectives, which we are pleased to see reflected in the draft bill.

---

[6] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

[7] See for example the 2006 IDC White Paper on "The Risks of Obtaining and Using Pirated Software." It showed that 25% of the Web sites that were reviewed for the study that offered counterfeit product keys, pirated software, key generators or "crack" tools attempted to install either malicious or potentially unwanted software. It also showed that 11% of the key generators and crack tools downloaded from Web sites and 59% of the key generators and crack tools downloaded from peer-to-peer networks contained either malicious or potentially unwanted software.

[8] http://www.staysafeonline.org

Establish a uniform national standard that preempts state laws

The National Conference of State Legislatures (NCSL) indicated that, as of October 2010, forty-six States, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands had enacted data breach notification laws.[9] This patchwork has created a compliance nightmare for businesses. As businesses may in good faith comply in different ways, this in turn creates confusion for consumers who receive notices from a multiplicity of sources.

For example, most state laws exempt encrypted data from the obligation to notify because they rightly consider that such a breach does not create a risk of harm. However, some jurisdictions including the District of Columbia, Wisconsin and New Hampshire require notification even when the data was encrypted. This jeopardizes the legal benefit for businesses of encrypting data. It also creates the likelihood that residents of other states will get notified even if their data was encrypted, and thus even if they are not at risk.

We are heartened by the draft bill's inclusion in section 6 of language pre-empting state laws, and suggest that the scope of preemption be clarified to cover notification to government agencies as well as private parties.

Prevent excessive notification

Not all breaches are of equal importance. Some create great risks of harm to consumers from identity theft and fraud, while other breaches create little to no risk. Currently, most state data breach laws require notification in all instances, even when no risk results from the breach. Over notification is likely to confuse consumers, who will then fail to take appropriate action when they are truly at risk.

We believe notification should be required only in those instances where an unauthorized disclosure presents a significant risk of material harm. We are pleased that section 3(f) of the draft bill takes a risk-based approach to breach notification. We recommend that the threshold be "*significant risk,*" to ensure that only genuine risk is notified.

Exclude data that has been rendered unusable, unreadable, or indecipherable

We also recommend that data not be subject to breach notification if it has been rendered unusable, unreadable, or indecipherable through practices or methods, such as encryption, redaction, or access controls, which are widely-accepted as effective industry practices or industry standards.

These conditions will ensure that data that has been illicitly accessed cannot actually be used to defraud or inflict harm on data subjects. As the apparent breach would not pose a risk to the consumer, it should not require notification. Such an exemption would also be technology neutral and flexible, allowing innovators to continue to develop new techniques and methods without fearing that legislation and regulations have favored one type of measure over another.

The draft bill's section 6(f)(2) provides a market-based incentive for the adoption of strong data security measures. We recommend however that this provision be made technology. As drafted, we are

[9] http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

concerned that it may tilt the playing field by setting up a two-tiered approach: while encryption is explicitly listed in the draft bill, other methods would require the sanction of an FTC rulemaking. This would put the FTC, which may not have the adequate technological or business expertise, in the difficult position of deciding what technologies are sufficiently secure to protect what types of data in what environment. In any case, the need for an innovating company to obtain this FTC sanction, before it can convince potential customers that they can use a new technology or method, is likely to chill such innovation.

We recommend that the legislation itself provide an exemption, for unusable, unreadable or indecipherable data, that is available to any widely-accepted effective industry practice or industry standard. The vigilant oversight of the FTC will ensure that the marketplace continuously adapts to "*effective industry practices or industry standards.*"

Require the use of data security safeguards

Requiring breach notification is fair to consumers who need to know they are at risk. We believe, however that more can be done to prevent breaches from happening in the first place, by requiring organizations that hold sensitive personal information to establish and implement data security policies and procedures. We support the fact that the draft bill does this in section 2.

Such a requirement should be flexible, reasonable and appropriate, and take into account the size, scope and nature of the organization's activities and the cost of implementing safeguards.

We think it would be appropriate to deem in compliance with the draft bill's data security requirements those organizations that comply with recognized industry standards for data security risk management. Such standards include ISO/IEC 27001, the Standard of Good Practice of the Information Security Forum, or the COBIT framework created by the Information Systems Audit and Control Association (ISACA.) This would simply extend to recognized industry standards the safe harbor created by the draft bill in section 2(a)(3), which applies to organizations whose data security obligations are already regulated by other federal laws with equivalent requirements.

It is particularly important to avoid imposing technology mandates. Organizations must be able to deploy appropriate and cutting edge security measures and technologies to effectively protect themselves and their customers' sensitive data against current and future threats. This would not be possible if the law mandated the use of specific products or technologies. Laws and regulations should focus instead on requiring the implementation of reasonable and appropriate security measures. We are pleased that section 4(b)(3) of the draft bill bars the FTC from "*requir[ing] the deployment or use of any specific products or technologies, including any specific computer software or hardware.*"

It is also important to avoid over-regulating data custody. While we support the draft bill's requirement that organizations protect the consumer data that they hold, we are concerned that the grant of authority to the FTC, in section 2(a)(1), to develop a body of regulations governing such corporate policies and procedures will in effect make the activity of data custody a regulated activity. The specificity of the data security requirements in the draft bill, and the existence of industry standards for data security risk management – such as ISO/IEC 27001, the Standard of Good Practice, or COBIT – render unnecessary the supplemental layer of regulation that would be created by the FTC under the draft bill. We should avoid creating a new compliance burden that does not offer increased data security.

We believe that the FTC enforcement actions will be sufficient to ensure that effective action is actually taken by companies to secure their systems and data.

Provide appropriate enforcement

Legislation should ensure that vigorous enforcement can take place to defend consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses.

The FTC has a strong track record in that respect, and BSA supports the draft bill granting to the FTC powers of enforcement in section 4(b).

We also support the inclusion of state Attorneys General as enforcers when the FTC has not acted. We support the draft bill's requirement, in section 4(c), that state AGs bring their civil actions under the bill in federal court. Federal jurisdiction will improve consistency in the application of federal legislation throughout the country.

BSA believes it is also important to prevent excessive litigation. The judicial system is not a desirable forum to determine the adequacy of data security measures. Moreover, allowing private lawsuits as a result of the occurrence of a data breach would create the risk that some data custodians refrain from notifying consumers in case of breaches, for fear of opening themselves to lawsuits. Therefore, we strongly urge you to include a provision explicitly stating that nothing in the draft bill is a basis for a private right of action for damages, as the Administration has proposed.