



**Testimony of Robert Holleyman
President and CEO
Business Software Alliance**

**Before the Subcommittee on Commerce, Trade and Consumer Protection
House Committee on Energy and Commerce**

**Legislative Hearing on
H.R. 2221, the "Data Accountability and Protection Act" and
H.R. 1319, the "Informed P2P User Act"**

May 5, 2009

Good afternoon. My name is Robert Holleyman. I am the President and CEO of the Business Software Alliance.¹ 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. We appreciate the opportunity to testify today on issues that are important to our member companies.

BSA commends you, Mr. Chairman, and Ranking Member Radanovich, for bringing a focus on data security and privacy 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. Electronic commerce cannot reach its full potential to contribute to global economic growth without the trust of consumers and businesses. BSA believes that legislation, like the two bills under consideration today, are important components in strengthening trust in the online environment.

I would like to address both of the important bills now before this Subcommittee: H.R. 2221, the "Data Accountability and Trust Act," and H.R. 1319, the "Informed P2P User Act." We support the objective of improving security and trust on-line. HR 2221 would make a substantial contribution to this goal and we support the purpose of the bill. H.R.

¹ The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Bentley Systems, CA, Cisco Systems, CNC Software/Mastercam, Corel, CyberLink, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Quark, Quest Software, Rosetta Stone, SAP, Siemens, Sybase, Symantec, and The MathWorks.

1319 focuses on one specific aspect of security issues: the threat posed by certain peer-to-peer file sharing programs. It is our sense that the definition in the bill would cover both legitimate multipurpose computer programs as well as those programs that are designed and distributed to enable illicit file sharing and have posed risks of inadvertent file sharing. Thus, we have serious reservations about the bill as drafted. We fear that it would have substantial unintended consequences for legitimate multipurpose products such as the ones BSA members develop and distribute.

H.R. 2221 – The Data Accountability and Trust Act

Consumers' trust in the security and confidentiality of their personal data is eroding. Over the past several years, the number of significant database security breaches has increased dramatically. The stakes are high and getting higher all the time.

- In January 2009, the Identity Theft Resource Center (ITRC) [reported](#) that the number of data breaches in 2008 increased 47% compared with 2007. A recently released Ponemon [study](#) shows that the average cost of a data breach grew to \$202 per record compromised in 2008, up from \$197 per record in 2007. And the average security incident cost individual companies \$6.6 million per breach in 2008, up from \$6.43 million in 2007 and \$4.7 million in 2006.
- For the ninth year in a row, identity theft tops the FTC list of U.S. consumer complaints. Of 1,223,370 complaints received in 2008, 313,982 – or 26 percent – were related to identity theft.
- According to the Better Business Bureau identity theft affects an estimated 10 million U.S. victims per year.
- According to the non-partisan *Privacy Rights Clearinghouse*, data breaches have affected a staggering 275 million records containing sensitive personal information since 2005.
- Earlier this year, Heartland Payment Systems, Inc. experienced what has been described as the single largest fraud-related data loss ever in United States history. Estimates now are that over 100,000,000 individual credit and debit card accounts were compromised. Since then, customers of more than 600 banks around the country have been victims of debit card fraud, with thieves using data stolen during the Heartland breach.
- Federal, state and local governments are responsible for 20% of all data breaches. Government is the third most targeted sector for cyber attacks and is responsible for 20 percent of all data breaches. The infiltration in particular of federal government networks and the possible theft or exploitation of our information is one of the most critical issues confronting our nation.

BSA believes that federal legislation that promotes improved protection of personal data, as well as notification to consumers when their data has been compromised, can effectively help restore consumer's trust.

Mr. Chairman, we believe that the "Data Accountability and Trust Act" (DATA) makes significant contributions towards achieving this goal. We support in particular the following five objectives.

BSA believes that the first objective of federal data security and data breach notification legislation should be to **establish a uniform national standard and provide preemption of state laws.**

The National Conference of State Legislatures (NCSL) indicated that, as of December 2008, forty-four states, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands had enacted data breach notification laws.² A number of states have also enacted laws that impose a minimum standard of care on organizations that collect and hold sensitive personal data about consumers. This patchwork of state laws has created a compliance nightmare for businesses. Importantly, it can also create confusion for consumers who receive notices from a multiplicity of sources.

Federal legislation establishing a uniform national framework would benefit businesses and consumers alike. Mr. Chairman, we congratulate you on providing the pre-emption of state laws in your bill, and suggest that the scope of preemption be clarified to cover notification to government agencies as well, since this type of notification is covered in your bill.

The second objective of federal breach notification legislation should be to **prevent excessive notification.**

Not all breaches are created equal. 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. As a result, consumers are likely to become immune to over-notification, and fail to take appropriate action when they are truly at risk. A more effective notification provision would include language that would require notification only in those instances where an unauthorized disclosure presents a significant risk of material harm.

Mr. Chairman, your bill provides a risk-based approach to breach notification. We recommend for your consideration that the threshold be slightly raised from "*reasonable risk*" to "*significant risk*," to ensure that only genuine risk is notified.

Linked to the issue of risk-based notification is the third objective of federal breach notification legislation: **exclude data that has been rendered unusable, unreadable, or indecipherable.**

BSA believes that data security can be enhanced, without a significant and difficult-to-enforce regulatory system, simply by using a market-based incentive for the adoption of strong data security measures. This can be done through an exception to the proposed obligation to notify security breaches in cases where the data is protected, so that even if it "*gets out*" the information cannot be used.

BSA believes this can be achieved if the measure in question satisfies two conditions:

1. It must render data unusable, unreadable, or indecipherable to any party that gains unauthorized access.
2. It must also be widely accepted as an effective industry practice or an industry standard. Examples of such measures include, but are not limited to, encryption, redaction, or access controls.

² <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>

Under these two conditions, the data that has been accessed cannot actually be used to defraud or inflict harm on data subjects. A breach would not pose a risk to the data subjects. Therefore, the apparent breach does not require notification.

Mr. Chairman, H.R. 2221 provides a market-based incentive for the adoption of strong data security measures. We recommend however that this incentive be made technology neutral, so that innovators continue to develop new techniques and methods without feeling that legislation has favored one type of measure over another.

We are concerned that your bill may tilt the playing field by setting up a two-tiered approach: while encryption is explicitly listed in your bill, other methods require the sanction of an FTC rulemaking. This puts 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.

To address this concern, we would propose that you adopt an approach whereby the technology must: 1. Render the data "*unusable, unreadable, or indecipherable,*" and 2. Be "*widely accepted as an effective industry practice or an industry standard.*" Examples of such measures include, but are not limited to, encryption, redaction, or access controls. We believe this gives flexibility for businesses and innovators, but is demanding enough to provide a high degree of protection for consumers, today and tomorrow.

The fourth objective of federal data security legislation should be to **avoid imposing technology mandates and over-regulating data custody.**

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 you include in your bill a provision that bars the FTC from "*requir[ing] the deployment or use of any specific products or technologies, including any specific computer software or hardware.*"

We are also heartened that section 2 of your bill – which requires the implementation of security measures to prevent breaches from happening – is risk-based, directing data custodians to analyze and mitigate their risks through appropriate and reasonable measures.

However, we believe it would have been preferable for your bill to simply direct organizations holding consumer data to establish and implement policies and procedures regarding information security practices for the protection of that data. We are concerned that your bill's grant of authority to the FTC to enact a body of regulations governing such corporate policies and procedures will in effect make the activity of data custody a regulated activity. The potential is high to turn data custody – an activity that is for most companies, whether large or small, only incidental to their core business – into a stifling compliance burden, with little to gain in terms of increased data security.

Finally, the fifth and last objective of federal data security and data breach legislation should be to **provide for appropriate enforcement.**

BSA supports your bill's provision granting the FTC powers of enforcement. The BJ's Wholesale Club, DSW (Designer Shoe Warehouse) and Card System cases are just a few examples of the FTC's strong track record of defending consumers against businesses that

fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses. We also support your bill's inclusion of state Attorneys General as enforcers when the FTC has not acted.

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 bill is a basis for a private right of action for damages.

H.R. 1319 – The Informed P2P User Act

We applaud Representative Bono Mack and the other cosponsors of H.R. 1319 for focusing attention on the serious harm to consumers that may be caused by some peer-to-peer file sharing applications.

HR 1319's aim is to promote consumer trust and prevent intrusions into sensitive files that reside on a user's computer. It proposes to accomplish this goal by imposing certain notification requirements on "peer-to-peer file sharing programs." We believe that the bill is intended to address a specific type of peer-to-peer software: programs, like Limewire, Bearshare and BitTorrent, that are intended for illicit purposes, such as unauthorized sharing of copyrighted works such as software, music or movies. Often this nefarious use of peer-to-peer technologies also exposes users to identity theft and other intrusions of their privacy.

However, we are concerned that the language of the bill covers much more than this narrow category of software. Many multipurpose products would be subject to regulation under this bill.

The problem that the bill's sponsors have identified is real. The persons who build, and maintain illicit peer-to-peer services make their money by selling advertising and installing spyware and other security threats as part of their software. A key feature of many of these services is that through default functions they establish shared folders from which others can take works. These folders are hard to find on the user's system once they have been installed. Moreover many file-sharing programs are designed to continue to run in the background, even when a user has taken steps to shut it down. Merely closing the window in which it appears, like with other programs, does not stop the program. Finally, disabling file-sharing functions is deliberately hard and complex. In some instances it takes as many as ten or more steps, involving the "advanced" settings on a computer, which is meant to make the average user very hesitant about taking those steps.

But peer-to-peer software covers a broad range of products that enable users in different locations to share files. For example, it enables engineers in Chicago and Palm Springs to work collaboratively on the drawings for a new bridge or airport. It enables colleagues at different locations to collaborate on a presentation or report. Internet telephony is another important and beneficial application of peer-to-peer technology. These software solutions do not pose the kind of risks to users' privacy that motivated this bill. So peer-to-peer software as such is neither good nor bad. Much depends on how the specific tool is designed and used.

Even more importantly, the definition of “peer-to-peer file sharing program” in the bill is not limited to peer-to-peer technology. It covers any software that exchanges information with other computers, including servers and websites. As the bill is now drafted, we believe that it would cover any software that is “Internet aware” – that is, capable of sending and receiving information on the Internet.

Here are some examples of software that appear to be included in the bill’s definition of “peer-to-peer file sharing program”:

- Operating systems and applications that are capable of determining whether updates are available, downloading the updates, and installing them automatically.
- Operating systems and applications that include a “crash analysis” feature.
- “Groupware” or collaboration tools.
- Web browsers.
- Anti-virus and anti-spyware programs that depend on up-to-date definition files.

We believe the bill in its current form could have substantial and immediate unintended consequences for consumers and developers of general-purpose software products. It could require developers to ensure that their Internet-aware products **disable** features such as automatic updates and crash analysis by default. BSA members and other software developers may well have to redesign their installation procedures to ensure that proper notices are displayed not only at the time that the software is installed, but also at the point in time when any “file-sharing” feature is activated. Under the terms of the bill, all software developers must provide a means to prevent the installation of such features and a means to uninstall them later.

This feature-by feature approach applied to the broad range of beneficial products now covered would be burdensome not only to developers, but to users as well. It would create abundant opportunities for consumer confusion and frustration when expected features are turned off by default. Moreover, leaving automatic updates off by default could result in many customers failing to receive security patches and updates, thus making their computers vulnerable to known security problems.

BSA recommends that the bill be modified to focus narrowly on the kind of software that has, in the past, been shown to create risks to consumers of unintentional exposure of personal information. These are peer-to-peer file sharing applications that are used primarily to exchange copyrighted works that belong to third parties among users of the same application. We recommend that the definition of “peer-to-peer file sharing program” be amended in the following ways:

- The definition should **include** only those programs that are used primarily to transmit or request copies of third-party copyrighted works.
- The definition should **include** only those programs that are used to transmit to, or request copies from, other computers running the same or a compatible peer-to-peer file sharing program.
- The definition should **exclude** programs or features that are used to transmit information to websites and other servers as distinguished from other personal computers on a P2P network.
- The definition should **exclude** programs that are installed onto computers by original equipment manufacturers. OEMs do not install the kinds of programs that are known risks for unintentional disclosure that have prompted this bill.

- The definition should **exclude** programs or features that transmit or request information for purposes that are internal to the functioning and maintenance of the program, such as caching information, updating the program or diagnosing problems with the software.

In addition, BSA recommends that the prohibitions in section 2 of the bill be modified in the following ways:

- The notice and consent requirement should be clarified to ensure that it is **limited to initial installation** of the software and configuration of the software that is part of the installation process.
- The provisions relating to deactivating or uninstalling individual features of a program should be clarified to ensure that **providing either a means of uninstalling or a means of deactivating a feature is sufficient**. As currently drafted the bill could be read to require both.

We believe any legislation such as HR 1319 must balance two key goals: promoting trust by protecting consumer security, and ensuring that technological innovation can continue at a pace dictated by the marketplace and the ingenuity of our engineers to common benefit of users and consumers. In finding this right balance we urge you to make sure that good technologies are not put at-risk by the need to stop bad actors. In other words, ensure that unintended consequences are identified and addressed before this bill becomes law.

* * * *

Mr. Chairman and members of the subcommittee, BSA appreciates the opportunity to provide its input on these two bills. We share the subcommittee's goals of helping to enhance data security, inform and empower consumers, and mitigate the harm from data breach. We are happy to work with you to craft the necessary changes to the bills as the legislative process moves forward.