

United States Federal Personal Data Privacy Bills

by Rebecca Herold, CISSP, CISM, CISA, FLMI

With most of the states in the United States having passed privacy breach notification legislation, and several federal breach notification bills of various flavors looming on the horizon, the issue of how to not only better protect personal information but also respond to breaches of personal information certainly should be on organizations' radar. There was a spate of bill writing activity during the summer of 2005, just before the August U.S. congress recess, and personal information security was at the top of the agenda. Three federal bills were proposed at that time addressing the protection of personal information.

 Vermont Senator Patrick Leahy, a sponsor of the Personal Data Privacy and Security Act of 2005, on June 29, 2005 said in a press release "We are seeing a rise in organized rings that target personal data to sell in online virtual bazaars. Insecure databases are now the low-hanging fruit for hackers looking to steal identities and commit fraud." For more information about this press release, see <http://leahy.senate.gov/press/200506/062905a.html>.

The most likely to pass of the proposed federal bills is the Personal Data Privacy and Security Act (PDPSA) of 2005 (http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s1332pcs.txt.pdf)—a bill “to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.” This bill has the broadest scope of the three bills and would create new safeguard requirements and restrictions for how personal information can be used. It would also impose criminal penalties for organizations and entities that violate it.

The History of United States Federal Privacy Bills

Trying to create a federal law to protect personal information is not a new endeavor. One of the earliest of the many proposed “privacy” bills, alternatively called “data protection” and “data security” bills, within the U.S. congress was H.R. 126, the “Individual Privacy Protection Act of 1989” introduced January 3, 1989 by Rep. Cardiss Collins (IL) “To amend the Privacy Act of 1974 in order to improve the protection of individual information and to reestablish a permanent Privacy Protection Commission as an independent entity in the Federal Government, and for other purposes.” This bill died in committee; however, privacy concerns did not die along with it. Members of congress started listening more to their constituents, and many more bills were introduced to protect personal information and privacy with each subsequent session of Congress. For example, the Fair Credit Reporting Act (FCRA) requires credit report information to be used only for certain purposes. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to safeguard personal information and prohibits them from sharing their customers' information with third parties without giving the customers the option to say no. And the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare entities to establish specific privacy and administrative, technical, and operational information safeguards for defined protected health information (PHI).

The progression of the privacy protection bills continues. There were at least 362 federal bills proposed in 2005 that covered the protection and privacy of personal information in one way or another. The following sidebar lists just ten of those proposed bills that generated waves in the press.

Sample of Proposed United States Privacy-Related Bills in 2005

H.R. 82, Social Security On-line Privacy Protection Act—Introduced 1/4/2005 by Rep. Rodney Frelinghuysen (NJ); prohibits an interactive computer service from disclosing to a third party an individual's Social Security number or related personally identifiable information without the individual's prior informed written consent. The bill also requires such service to permit an individual to revoke any consent at any time.

S. 29, Social Security Number Misuse Prevention Act—Introduced 1/24/2005 by Sen. Dianne Feinstein (CA); amends the Federal criminal code to prohibit the display, sale, or purchase of Social Security numbers without the affirmatively expressed consent of the individual, except in specified circumstances.

S. 116, Privacy Act of 2005—Introduced 1/24/2005 by Sen. Dianne Feinstein (CA); to require the consent of an individual prior to the sale and marketing of such individual's personally identifiable information, and for other purposes

S. 751, Notification of Risk to Personal Data Act—Introduced 4/11/2005 by Sen. Dianne Feinstein (CA); requires a business or government entity to notify an individual in writing or email when it is believed that personal information has been compromised, with the exception of situations relating to criminal investigation or national security purposes.

S. 768, Comprehensive Identity Theft Prevention Act—Introduced 4/12/3005 by Sen. Charles Schumer (NY); creates a new Federal Trade Commission (FTC) office of identity theft to help victims restore their identities.

S. 1216, Financial Privacy Breach Notification Act of 2005—Introduced 6/9/2005 by Sen. Jon Corzine (NJ); amends GLBA to require a financial institution to promptly notify the following entities whenever a breach of personal information has occurred at such institution: each customer affected by such breach; certain consumer reporting agencies; and appropriate law enforcement agencies. Furthermore, it requires any person that maintains personal information for or on behalf of a financial institution to promptly notify the institution of any case in which such customer information has been breached.

S. 1326, Notification of Risk to Personal Data Act—Introduced 6/28/2005 by Sen. Jeff Sessions (AL); requires any entity that owns or licenses sensitive personal information to implement and maintain "reasonable" security and notification procedures and practices appropriate to the nature of the information; preempts any state laws which relate "in any way to electronic information security standards or notification."

S. 1332, Personal Data Privacy and Security Act of 2005—Introduced 6/29/2005 by Sen. Arlen Specter (PA) and Sen. Patrick Leahy (VT); deals with different issues relating to identity theft and security breaches, specifically providing security measures that require "business entities" that have information on more than 10,000 United States persons to adopt measures, commensurate with the sensitivity of the data and the size and complexity of the entities activities.

S. 1336, Consumer Identity Protection and Security Act—Introduced 6/29/2005 by Sen. Mark Pryor (AR); establishes procedures for the protection of consumers from misuse of, and unauthorized access to, sensitive personal information contained in private information files maintained by commercial entities engaged in, or affecting, interstate commerce.

S. 1408, Identity Theft Protection Act—Introduced 7/14/2005 by Sen. Gordon Smith (OR) and Sen. Bill Nelson (FL); strengthens data protection and safeguards, requires data breach notification, and further prevents identity theft.

Challenges for Passage of Such Bills

There are some common threads running through these privacy protection bills:


Require prompt notification when a security breach occurs or is discovered

Grant more regulatory power to the U.S. federal government

Establish minimum standards for information security


Although there are a staggering number of bills that have been submitted to Congress, few have continued on to become full-fledged laws, illustrating the many challenges for passage of these bills. Lobbyists from large organizations that must comply with the laws have huge influence and strong voices in blocking these bills; they have historically lobbied to not make businesses responsible for security breaches. Privacy advocates also have huge influence and equally strong voices in blocking these bills; they have historically lobbied to make weak bills stronger and to prevent the passage of what they view would be watered-down laws with so many loopholes that any such law would be basically meaningless.

However, with the escalation in the number of reported personal information security breaches, as well as the sometimes hugely varying requirements of state-level breach notification laws that make it extremely challenging for businesses to find common compliance ground, lobbyists, privacy advocates, and already heavily regulated industries alike are now supporting the passage of uniform federal privacy laws.

 From the Prepared Testimony and Statement for the Record of Marc Rotenberg, President, EPIC; Hearing on “Identity Theft and Data Broker Services” Before the Committee on Commerce, Science and Transportation, United States Senate; May 10, 2005: “Congress can continue to deal with these challenges in piecemeal fashion, but it seems that the time has come to establish a formal government commission charged with the development of long-term solutions to the threats associated with the loss of privacy. Such a commission should be established with the clear goal of making specific proposals. It should include a wide range of experts and advocates. And it should not merely be tasked with trying to develop privacy safeguards to counter many of the government new surveillance proposals. Instead, it should focus squarely on the problem of safeguarding privacy. Congress needs to establish a comprehensive framework to ensure the right of privacy in the twenty-first century.”

PDPSA Passage Likely

Pundits largely believe the PDPSA will meet with successful passage by congress. What makes this bill appealing to lawmakers is that it is one of the few, perhaps only, of the bills that establish criminal activities for entities that do not provide proper safeguards for personal information and that do not respond appropriately to personal information breach incidents.

 If the PDPSA is passed into law, there can be criminal penalties including as many as 5 years in prison for those who intentionally conceal information related to a security breach and as many as 10 years for breaking into systems maintained by data broker companies in the business of selling personal information.

The PDPSA would also restrict the sale and publication of Social Security numbers. This restriction appeals to the many members of Congress who have submitted bills specific to the protection of Social Security numbers. It also would limit the authority of states to write their own state-specific legislation of personal data protection—something that Congress believes will help in creating a more consistent level of privacy protection throughout the states.

The other proposed bills largely include only civil penalties and would place most of the enforcement and regulatory powers with the Federal Trade Commission (FTC). Most of them also explicitly preempt state and local laws involving the same issues, and detail a wide range of monetary penalties on entities that don't provide notification according to what many consider as ambiguous terms, such as "without unreasonable delay." The guidelines for breach notification also are different from bill to bill.

Benefits and Detriments of Such Bills

The PDPSA would likely result in the FTC creating a new standard for minimally acceptable and reasonable security practices in addition to creating regulations requiring covered entities to

Develop, implement, and maintain an effective information security program that contains administrative, technical, and physical safeguards for sensitive personal information, taking into account the use of technological safeguards, including encryption, truncation, and other safeguards available or being developed for such purposes

Implement procedures for verifying the credentials of any third party seeking to obtain the sensitive personal information of another person

Implement disposal procedures for not only disposal of sensitive personal information but also secure transfer of sensitive personal information to third parties for disposal

As it is now written, it would not require federal preemption of any similar state law except if the state law were inconsistent with the PDPSA.

As information security and privacy professionals who have been struggling to keep up with regulations know, there are a variety of benefits as well as detriments to these assorted and sundry bills. Table 1 explores these benefits and detriments.

Benefits	Detriments
Increased awareness of information security and privacy issues by business leaders who, under the bills, become ultimately responsible for having adequate safeguards in place.	Overly broad notification requirements may result in so many breach notifications being sent that consumers—for typically “normal” security incidents such as virus outbreaks—start disregarding them. This oversight may lead to customer complaints, and result in weakened business leader support.
Subsequently increased budgets and resources for addressing information security and privacy issues in order to be in compliance.	Resources may be pulled from other vital information security and privacy projects because they are not explicitly cited in regulatory text, so they lose their funding. This situation could leave important risks unaddressed. Organizations have already been dealing with this situation with regard to Sarbanes-Oxley compliance activities.
Increased leverage for information security and privacy professionals implementing security controls and practices.	A large increase in “snake oil” compliance-related vendor product solutions will be pushed upon organizations. Many of these products will likely be relabeled applications from existing “compliance” products. Using these will likely lead to gaps in compliance and a false sense of achieving compliance.

Table 1: Benefits and detriments of privacy bills.

PDPSA Considerations

The specific requirements for the PDPSA will certainly help to beef up corporate information security and privacy programs, but will also create challenges for information security and privacy leaders:


Covered entities (CEs) would need to report each data breach of “personally identifiable information” to the U.S. Secret Service, credit reporting agencies, and consumers.

CEs would need to “implement a comprehensive personal data privacy and security program.”

CEs would be required to conduct risk assessments to identify all vulnerabilities that could potentially allow a data breach.

CEs would need to evaluate the sufficiency of policies, procedures, and security controls. For example, the PDPSA would require CEs to make appropriate provisions for facility access, employee training programs, and the destruction of media or storage devices.

What is personally identifiable information? Within the PDPSA “the term ‘personally identifiable information’ means any information, or compilation of information, in electronic or digital form serving as a means of identification, as defined by section 1028(d)(7) of title 18, United State Code.”

 Section 1028(d)(7) of title 18 United State Code:

“(7) the term “means of identification” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any -


(A) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or


(D) telecommunication identifying information or access device (as defined in section 1029(e))”

The PDPSA would require that data brokers (defined by the bill as “a business entity which for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of collecting, transmitting, or otherwise providing personally identifiable information on a nationwide basis on more than 5000 individuals who are not the customers or employees of the business entity or affiliate”) and companies possessing databases with the personally identifiable information of 10,000 or more U.S. citizens would be covered entities (subject to the law). Civil and criminal penalties for violating the PDPSA are wide-ranging depending on the type of breach that has occurred and the number of personal records compromised. Businesses could potentially be fined as much as \$35,000 a day for each day the enterprise is in violation of PDPSA requirements.

 Unlike most of the state breach notification laws, the PDPSA does NOT include a provision to exempt encrypted data from the breach notification requirement; it applies to both encrypted and unencrypted data.

Get Ready to Meet Compliance

Just before the Thanksgiving recess in November 2005, the Senate Judiciary Committee approved the PDPSA in a bipartisan vote. With the broad base of support from not only corporations but also from privacy groups, several legislative analysts expect the PDPSA to pass into law sometime during the last half of 2006 with little to no opposition. Organizations will then have one more regulation with which to comply. However, it is likely that with everything else on their compliance plates, most will take a wait-and-see attitude (much like most did with HIPAA and GLBA) before getting fired up to take compliance actions. Such lackadaisical attitude is risky and could be costly.

 According to the January 10, 2006 issue of the McLean Report “As with most new legislation, companies generally don’t begin compliance initiatives until 60 or 90 days before a legal deadline...each \$1 spent on compliance efforts pre-deadline will end up costing \$10 for the same activity if addressed post-deadline.”

Even without the passage of PDPSA, the U.S. government has already been finding businesses accountable for safeguarding personal information. Businesses will be impacted, with or without passage of the PDPSA, if an incident involving the breach of personal information occurs. It is wise to prepare now to respond to what seems to be the inevitable personal information breach. Think now about addressing the following issues:

Establish an area or position with accountability and responsibility for information security and privacy activities.

Define the personally identifiable information within your organization.

Identify where all the personally identifiable information is located.

Perform a privacy impact assessment (PIA).

Create a breach incident identification and response plan.

Create or review and update as necessary information security and privacy policies and procedures.

Implement an ongoing information security and privacy training and awareness program.