CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

April 19, 2006

S. 1789
Personal Data Privacy and Security Act of 2005

As reported by the Senate Committee on the Judiciary on November 17, 2005

SUMMARY

S. 1789 would establish new federal crimes relating to the unauthorized access of sensitive personal information. The bill also would require most government agencies or business entities that collect, transmit, store, or use personal information to notify any individuals whose information has been unlawfully accessed. In addition, S. 1789 would require data brokers to allow individuals access to their electronic records and publish procedures for individuals to respond to inaccuracies.

Implementing S. 1789 could increase civil and criminal penalties and thus could affect federal revenues and direct spending, but CBO estimates that such effects would not be significant in any year. Complying with the bill's provisions would increase the administrative expenses of federal agencies. CBO estimates that those added costs would sum to $25 million over the 2007-2011 period and would generally come from agencies' salaries and expense budgets, which are subject to annual appropriation.

S. 1789 contains several intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA) including potentially costly notification requirements and explicit preemptions of the authority of State Attorneys General and state law. While the aggregate costs to state, local, and tribal governments of complying with these mandates is uncertain, CBO estimates that they would likely exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation) in at least one of the first five years after the mandates go into effect.

S. 1789 would impose several private-sector mandates as defined in UMRA. It would require certain entities to establish and maintain a data privacy and security program. It would also require all entities engaged in interstate commerce to notify individuals if a security breach occurs in which such individuals' sensitive personally identifiable information is compromised. Lastly, it would require data brokers to provide individuals with their personally identifiable information and to change the information if it is incorrect.

While CBO cannot estimate the direct cost of complying with each mandate, because millions of individuals are affected by security breaches annually, the data privacy and security program and notification requirements in S. 1789 could be costly. Based on information from government and industry sources, CBO estimates that the aggregate costs of all of the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation) in at least one of the first five years the mandates are in effect.

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of S. 1789 is shown in the following table. The costs of the legislation fall primarily in function 800 (general government).

	By Fiscal Year, In Millions of Dollars					
	2006	2007	2008	2009	2010	2011
CHANGES IN SPENDING SUBJECT TO APPROPRIATION[a]						
Estimated Authorization Level	0	3	5	7	7	7
Estimated Outlays	0	1	3	7	7	7

a. Enacting S.1789 also could affect direct spending and revenues, but CBO estimates that any such effects would not be significant.

BASIS OF ESTIMATE

For this estimate, CBO assumes the bill will be enacted during fiscal year 2006, that the necessary amounts will be provided each year, and that spending will follow historical patterns for similar programs.

Spending Subject to Appropriation

S. 1789 would require most government agencies or business entities that collect, transmit, store, or use personal information to notify any individuals whose information has been unlawfully accessed. CBO estimates that implementing S. 1789 would cost $25 million over the 2006-2011 period, assuming appropriation of the necessary amounts.

Security Breach Notification. The Federal Information Security Management Act of 2002 provides requirements for securing the federal government's information systems, including the protection of personal privacy. The National Institute of Standards and Technology develops information security standards and guidelines for other federal agencies, and the Office of Management and Budget (OMB) oversees information technology security policies and practices. OMB estimates that federal agencies spend around $5 billion a year to secure the government's information systems.

In the event of a security breach involving a significant risk of identity theft, government agencies would be required to notify an individual whose information may have been compromised. Notification would be in the form of individual notice (written notice to a home mailing address, via telephone, or via e-mail) as well as through the mass media.

The cost of such notification would depend on the number of security breaches that occur, the number of persons affected, and the cost per person of notification. CBO cannot estimate the number of security breaches that might occur within the federal government in any year. Nationwide, only the largest breaches are identified and reported. Limited anecdotal information over the last two years suggests that security breaches involving the federal government have occurred regularly usually involving the theft of computers containing personal information from specific agencies. Such thefts have affected the personal information of about 3 percent of the 4 million civilian and military federal employees (about 120,000). Based on that data and information from OMB and other agencies, CBO does not expect that there would be significant notification costs under the bill in any one year. Thus, CBO estimates that implementing the notification provision in S. 1789 would cost less than $500,000 annually.

Nonetheless, the federal government is also one of the largest providers, collectors, consumers, and disseminators of personnel information in the United States. The cost to notify individuals of a security breach to personnel information may cost up to $2 per notification. Although, CBO cannot anticipate the number of security breaches, a significant breach of security involving a major collector of personnel information, such as the Internal Revenue Service or the Social Security Administration could involve millions of individuals and would have a significant budgetary impact.

Federal Trade Commission. Title II would require companies that maintain databases containing individuals' personal information (known as data brokers) to provide individuals with their personal electronic records upon request. Title II also would require data brokers to provide individuals a means to correct mistakes in their records. Under the bill, the Federal Trade Commission would be directed to enforce provisions related to data brokers, including collecting civil penalties for violations of these requirements. CBO estimates that implementing title II would not have a significant effect on spending subject to appropriation.

Other Provisions. S. 1789 also would require additional reporting by agencies. The legislation would require agencies to conduct additional privacy impact assessments on commercially purchased private-sector data that contains personally identifiable information and a report by the Government Accountability Office on federal agencies' use of private-sector information. In addition, the General Services Administration (GSA) would have to provide additional security assessments for certain government contracts involving personally identifiable information. This would largely involve payroll processing, emergency response and recall, and medical data. Based on information from OMB and GSA, CBO estimates that the increased staffing levels and reporting requirements under the legislation would cost $7 million annually when fully implemented. (For this estimate, we assume the implementation process would take about three years.)

Direct Spending and Receipts

S. 1789 would establish new federal crimes relating to the unauthorized access of sensitive personal information. Enacting the bill could increase collections of civil and criminal fines for violations of the bill's provisions. CBO estimates that any additional collections would not be significant because of the relatively small number of additional cases likely to be affected. Civil fines are recorded as revenues. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and subsequently spent without further appropriation.

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 1789 contains several intergovernmental mandates as defined in UMRA. Specifically the bill would:

- Require that state and local governments—including public schools and universities —notify affected individuals, credit reporting agencies, and law enforcement agencies of any breach of security that could result in identity theft;

- Explicitly preempt state laws in at least 19 states regarding the treatment of personal information; and

- Place certain notification requirements and limitations on state attorneys general and state insurance authorities.

While the aggregate costs of complying with the mandates are uncertain, CBO estimates that the notification requirements would impose the most significant costs on state and local governments. The remainder of this analysis focuses on those requirements. CBO estimates that the total costs to state, local, and tribal governments of the mandates would likely exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation) in at least one of the first five years that the mandates go into effect.

In the event of a security breach meeting certain conditions, the bill would require state and local goverments to notify any individual whose information may have been disclosed, coordinate with consumer reporting and law enforcement agencies, and, to the extent possible, provide a toll-free number that affected individuals could use for further information. Costs to notify affected individuals would vary based on the circumstances of each security breach. Information from California suggest that a large university could expect to incur costs totaling between $100,000 and $200,000 to notify individuals whose personal information may have been compromised.

Entities that would be affected by these requirements include, but are not limited to, state departments of revenue and motor vehicles, public hospitals, courts at the state and local levels, agencies that oversee elections, K-12 schools, school districts, and post-secondary institutions. There are more than 190,000 such entities in the United States (75,000 municipal governments, about 3,600 counties, more than 100 public hospitals, about 100,000 schools, 14,000 school districts, and more than 1,500 public post-secondary institutions). Relatively few of these entities would have to experience a security breach in order for costs to be significant in any one year. For example, if the average cost to comply with the mandates was $50,000, less than one percent of intergovernmental entities that maintain databases would need to suffer a security breach in order for the threshold established in UMRA to be exceeded. According to data security experts, security breaches have been increasing substantially over time. While CBO cannot estimate the frequency or targets of such breaches, we expect that costs would be significant and would likely grow over time.

ESTIMATED IMPACT ON THE PRIVATE SECTOR

S. 1789 would impose three private-sector mandates as defined in UMRA. It would:

- Require certain entities to establish and maintain a data privacy and security program;

- Require all entities engaged in interstate commerce to notify individuals if a security breach occurs in which such individuals' sensitive personally identifiable information is compromised; and

- Require data brokers to provide individuals with their personally identifiable information and to change the information if it is incorrect.

While CBO cannot estimate the direct cost of complying with each mandate, because millions of individuals are affected by security breaches annually, the data privacy and security program and notification requirements in S. 1789 could be costly. Based on information from government and industry sources, CBO estimates that the aggregate costs of all of the mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation) in at least one of the first five years the mandates are in effect.

Data Privacy and Security Requirements

Subtitle A of title III would require certain business entities engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on more than 10,000 individuals to establish and maintain a data privacy and security program. Entities would be required to conduct risk assessments to identify possible security risks in establishing the program. They would also have to conduct periodic vulnerability testing on their programs. Additionally, entities would have to train their employees on the program.

If entities hire third-party contractors not subject to these provisions to maintain sensitive personally identifiable information on individuals, the entities must ensure that the contractors implement and maintain security measures in compliance with this act.

Some entities would be exempt from the requirements of subtitle A. These include entities that are subject to the Gramm-Leach-Bliley Act and entities that are subject to the Health Insurance Portability and Accountability Act.

Industry sources estimate that thousands of business entities would be required to implement a data privacy and security program. The per-entity cost of the data privacy and security requirements, though, would depend greatly on the size of the entity, the number of establishments for the entity, and the amount of sensitive personally identifiable information that pertains to the entity. While CBO cannot estimate the direct costs to entities of establishing the data privacy and security program, it estimates that the aggregate cost to the private sector could be large in at least one of the first five years the mandate is in effect.

Security Breach Notification

Subtitle B of title III would require certain business entities engaged in interstate commerce that use, access, transmit, store, dispose of, or collect sensitive personally identifiable information to notify individuals in the event of a security breach if the individuals' sensitive personally identifiable information is compromised. Entities would be able to notify individuals using written letters, telephone, or by email under certain circumstances.

Additionally, such business entities would be required to notify other entities and agencies in the event of a large security breach. The additional notification requirements are:

- If more than 1,000 individuals are affected by a security breach, the entities would be required to notify appropriate consumer reporting agencies that compile and maintain files on consumers on a nationwide basis;

- If more than 5,000 individuals are affected by a security breach in a state, the entity would be required to notify major media outlets serving that state or jurisdiction; and

- Entities would be required to notify the Secret Service if:

    (1) More than 10,000 individuals are affected by a security breach,

    (2) A security breach involves a database that contains sensitive personally identifiable information on more than 1 million people,

    (3) A security breach involves databases owned by the federal government, or

    (4) A security breach involves sensitive personally identifiable information of employees or contractors of the federal government involved in national security or law enforcement.

The cost of the mandates in subtitles A and B depends on the amount of firms that would be required to implement data privacy and security programs under this bill and the number of security breaches that continue to occur. If a large number of firms implement data privacy and security programs, the number of security breaches would likely decline over time. Conversely, if a large number of individuals are affected by ongoing security breaches despite the new data privacy and security requirements, business entities would be required to notify a large number of individuals on an annual basis. According to industry sources, millions of individuals' sensitive personally identifiable information is illegally accessed every year.

The mandates in subtitles A and B would extend to thousands of business entities that use or maintain sensitive personally identifiable information. CBO estimates that although the per-entity costs of implementing a data privacy and security program and notifying individuals in the event of a security breach may be low relative to the threshold, the aggregate costs of these provisions for all private-sector entities would exceed the annual threshold established by UMRA for private-sector mandates in at least one of the first five years the mandates are in effect.

Requirements for Data Brokers

Section 201 would require certain data brokers to disclose all personal electronic records relating to an individual that are kept primarily for third parties if requested by the individual. The bill defines data broker as a business entity which for monetary fees or dues regularly engages in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to nonaffiliated third parties on an interstate basis.

Additionally, if an individual disputes the accuracy of the information that is contained in the data brokers' records, the data brokers would be required to change the information or provide the individual with contact information for the source from which they obtained the individual's information. Data brokers could determine that some requests to change an individual's information are frivolous. However, the data brokers would be required to notify any individual requesting a change of information of the action taken.

The cost of providing records upon request depends on the costs of gathering and distributing the information to individuals and the number of individuals requesting their information. Under the bill, data brokers would be allowed to charge a reasonable fee for this service. Data brokers would likely be able to cover their costs of providing individuals with their personal information with the fee they could charge. The cost to data brokers of having to change individuals' information and notifying the individuals, however, could be large. Some evidence exists that many individuals' personally identifiable information housed at large data brokerage firms is in part incorrect. If a large number of individuals request data changes, CBO estimates that the time and notification costs to data brokers could be high.

PREVIOUS CBO ESTIMATES

CBO has provided cost estimates for four pieces of legislation that deal with identity theft or the safeguarding of personal information. Each has different provisions, and would require private companies and the government to take certain precautions to safeguard personal information. The cost estimates reflect those differences.

- On April 6, 2006, CBO transmitted a cost estimate for H.R. 4127, the Data Accountability and Trust Act, as ordered reported by the House Committee on Energy and Commerce on March 29, 2006, with a subsequent amendment provided by the committee on April 4, 2006.

- On March 30, 2006, CBO transmitted a cost estimate for H.R. 3997, the Financial Data Protection Act, as ordered reported by the House Committee on Financial Services on March 16, 2006.

- On March 10, 2006, CBO transmitted a cost estimate for S. 1326, the Notification of Risk to Personal Data Act, as ordered reported by the Senate Committee on the Judiciary on October 20, 2005.

- On November 3, 2005, CBO transmitted a cost estimate for S. 1408, the Identity Theft Protection Act, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 28, 2005.

ESTIMATE PREPARED BY:

Federal Costs: Federal Agencies—Matthew Pickford
Federal Trade Commission—Melissa Petersen

Impact on State, Local, and Tribal Governments: Sarah Puro

Impact on the Private Sector: Tyler Kruzich

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis