CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

October 27, 2011

S. 1151
Personal Data Privacy and Security Act of 2011

As reported by the Senate Committee on the Judiciary on September 22, 2011

SUMMARY

S. 1151 would establish new federal crimes relating to unauthorized access to sensitive personal information. The bill also would require most federal agencies and businesses that collect, transmit, store, or use such personal information to establish a data privacy and security program and to notify any individuals whose information has been unlawfully accessed.

Assuming appropriation of the necessary amounts, CBO estimates that implementing S. 1151 would cost $14 million over the 2012-2016 period. Enacting S. 1151 could increase civil and criminal penalties and could affect direct spending by agencies not funded through annual appropriations; therefore, pay-as-you-go procedures apply. CBO estimates, however, that any changes to revenues and net direct spending would be negligible.

S. 1151 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the cost of complying with the requirements would be small and would not exceed the threshold established in UMRA ($71 million in 2011, adjusted annually for inflation).

S. 1151 also would impose several private-sector mandates. Much of the private sector already complies with many of the bill's requirements. However, a large number of entities in the private sector would need to implement new or enhanced security standards if the bill is enacted. Consequently, CBO estimates that the aggregate direct cost of the mandates in the bill would probably exceed the annual threshold established in UMRA for private-sector mandates ($142 million in 2011, 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. 1151 is shown in the following table. The costs of this legislation fall within budget functions 050 (national defense), 370 (commerce and housing credit), 750 (administration of justice), 800 (general government), and other budget functions that contain salaries and expenses.

	By Fiscal Year, in Millions of Dollars					
	2012	2013	2014	2015	2016	2012-2016
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Estimated Authorization Level	3	3	3	3	3	15
Estimated Outlays	2	3	3	3	3	14

BASIS OF ESTIMATE

For this estimate, CBO assumes that the bill will be enacted early in 2012, that the necessary amounts will be provided each year, and that spending will follow historical patterns for similar programs.

Spending Subject to Appropriation

Most of the provisions of the bill would codify the current practices of the federal government regarding data security and procedures for notifying individuals whose personal information may have been disclosed. In general, a data breach occurs when sensitive, protected, or confidential information is copied, transmitted, viewed, or stolen by someone not authorized to do so. The federal government is one of the largest providers, collectors, consumers, and disseminators of personal information in the United States. Although CBO cannot anticipate the number or extent of breaches, a significant breach of security involving a major collector of personal information, such as the Internal Revenue Service or the Social Security Administration, could involve millions of individuals and result in significant costs to notify those individuals of such a breach. Existing laws generally do not require federal agencies to notify affected individuals of such security breaches; however, agencies that have experienced security breaches have generally provided such notification. Therefore, CBO expects that codifying this practice would probably not lead to a significant increase in spending.

The legislation also would require a business entity or federal agency—under certain circumstances—to notify the Department of Homeland Security that a security breach has

occurred but would permit entities or agencies to apply to the federal government for a delay or exemption from the requirements if the personal data were encrypted or similarly protected or if notification would threaten national security. Other provisions of the bill would require the Federal Trade Commission (FTC) to develop and enforce regulations to implement the bill's new requirements for data security programs and policies. Finally, S. 1151 would require federal agencies to provide several reports to the Congress, which would include the number and type of data breaches.

Based on information from the Department of Homeland Security, the Federal Bureau of Investigation, the FTC, and other agencies with a significant information technology presence, CBO estimates that additional investigative and administrative work under the bill would cost about $3 million annually, subject to the availability of appropriated funds.

Direct Spending and Revenues

S. 1151 would establish new federal crimes relating to unauthorized access to 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 result. Civil fines are recorded as revenues. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and subsequently spent without further appropriation.

PAY-AS-YOU-GO CONSIDERATIONS

The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. CBO estimates that enacting S. 1151 would have a negligible effect on direct spending and revenues.

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 1151 contains intergovernmental mandates as defined in UMRA because it would explicitly preempt laws in at least 46 states regarding the treatment of personal information and impose notification requirements and limitations on state Attorneys General. Because the limits on state authority would impose no duties with costs and because the notification requirements would result in minimal additional spending, CBO estimates that the costs of the mandates would be small and would not exceed the threshold established in UMRA for intergovernmental mandates ($71 million in 2011, adjusted annually for inflation).

ESTIMATED IMPACT ON THE PRIVATE SECTOR

S. 1151 would impose several private-sector mandates as defined in UMRA by:

- Requiring certain business entities that handle personally identifiable information for 10,000 or more individuals to establish and maintain a data privacy and security program;

- Requiring any business entity engaged in interstate commerce to notify individuals if a security breach occurs in which such individuals' sensitive personally identifiable information is compromised;

- Requiring providers of electronic communication services to inform any user that initiated transmission of data on their network if they become aware of a data breach; and

- Limiting existing rights to seek damages against a person if the only basis for the suit is the violation of a contractual obligations involving the use of computers or access to personal information.

The majority of businesses already comply with data security standards and breach notification procedures similar to many of the bill's requirements. However, some of the requirements in the bill would impose new standards for data maintenance and security on a large number of entities in the private sector. Consequently, CBO estimates that the aggregate direct cost of all the mandates in the bill would probably exceed the annual threshold established in UMRA for private-sector mandates ($142 million in 2011, 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 II would require businesses engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more individuals to establish and maintain a program for data privacy and security. The program would be designed to protect against both unauthorized access and any anticipated vulnerabilities. Business entities would be required to conduct periodic risk assessments to identify such vulnerabilities and assess possible security risks in establishing the program. Additionally, businesses would have to train their employees in implementing the data security program.

The bill would direct the FTC to develop rules that identify privacy and security requirements for the business entities covered under subtitle A. Some businesses would be exempt from the requirements of subtitle A. Those include certain financial institutions that are subject to the data security requirements under the Gramm-Leach-Bliley Act, entities that are subject to the data security requirements of the Health Insurance Portability and Accountability Act, and providers of electronic communications services to the extent that they are exclusively engaged in the temporary storage, transmission, or routing of data.

The cost per entity of the data privacy and security requirements would depend on the rules to be established by the FTC, the size of the entity, and its current ability to secure, record, and monitor access to data, as well as on the amount of sensitive, personally identifiable information maintained by the entity. The majority of states already have laws requiring business entities to utilize data security programs, and it is the current practice of many businesses to use security measures to protect sensitive data. However, some of the new standards for data security in the bill could impose additional costs on a large number of private-sector entities.

For example, under the bill, businesses covered under subtitle A would be required to enhance their security standards to include the ability to trace access and transmission of all records containing sensitive personally identifiable information. The current industry standard on data security has not reached that level. According to industry experts, information on a particular individual can be collected from several places and, for large companies, can be accessed by thousands of people from several different locations. The ability to trace each transaction involving data containing personally identifiable information would require a significant enhancement of data management hardware and software for the majority of businesses. Further, the bill's definition of sensitive personally identifiable information is broader than the current industry standard.

This definition would significantly increase the number of entities that would be required to implement new or enhanced data security standards. The aggregate cost of implementing such changes could be substantial.

Notification of Security Breaches

Subtitle B of title II would require 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, the telephone, or email. If a business does not own or license the information, it would have to notify the owner or licensee of the information following a breach. A notice in major media outlets serving a state or jurisdiction also would have to be provided for any breach of more than 5,000 residents' records within a particular state. In addition, businesses would be required to notify other entities and

agencies in the event of a large security breach. Entities that experience the breach of such data would have to notify the affected victims and consumer reporting agencies if the breach involves more than 5,000 individuals. The bill, however, would exempt business entities from the notification requirements under certain circumstances.

According to industry sources, the sensitive personally identifiable information of millions of individuals is illegally accessed or otherwise breached every year. However, according to those sources, 46 states already have laws requiring notification in the event of a security breach. In addition, it is the standard practice of most business entities to notify individuals if a security breach occurs. Therefore, CBO estimates that the notification requirements would not impose significant additional costs on businesses.

The subtitle also contains a provision requiring providers of electronic communication services (such as Internet service providers) to inform the entity that began a transmission of information using their systems if they become aware that a breach of sensitive personally identifiable information has occurred. This would constitute a mandate on those service providers. The cost to inform business entities of a breach would probably be small.

Elimination of Existing Rights of Action

Title I would eliminate certain existing rights of action against individuals for violating contractual agreements involving the use of computers or access to personal information. Currently, a lawsuit may be filed against an individual for exceeding authorized access (obtaining or altering information without the proper authorization) and computer fraud if that individual violates the terms of a related contractual agreement. The bill would eliminate any right of action alleging someone has exceeded authorized access or committed computer fraud when the only basis for the suit is the violation of a related agreement. Because there are few such cases, CBO estimates that the cost of the mandate would be minimal.

ESTIMATE PREPARED BY:

Federal Costs: Department of Homeland Security—Jason Wheelock
Federal Trade Commission—Susan Willie
U.S. Secret Service—Mark Grabowicz
Other Federal Agencies—Matthew Pickford

Impact on State, Local, and Tribal Governments: Elizabeth Cove Delisle

Impact on the Private Sector: Marin Randall

ESTIMATE APPROVED BY:

Theresa Gullo
Deputy Assistant Director for Budget Analysis