CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

December 2, 2009

S. 1490
Personal Data Privacy and Security Act of 2009

As ordered reported by the Senate Committee on the Judiciary on November 5, 2009

SUMMARY

S. 1490 would establish new federal crimes relating to the unauthorized access of sensitive personal information. The bill also would require most government agencies or businesses that collect, transmit, store, or use personal information to notify any individuals whose information has been unlawfully accessed. In addition, S. 1490 would require data brokers to allow individuals access to their electronic records and to publish procedures for individuals to respond to inaccuracies.

Assuming appropriation of the necessary amounts, CBO estimates that implementing S. 1490 would cost $25 million over the 2010-2014 period. Enacting S. 1490 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. Further, enacting S. 1490 could affect direct spending by agencies not funded through annual appropriations. CBO estimates, however, that any changes in net spending by those agencies would be negligible.

S. 1490 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 ($69 million in 2009, adjusted annually for inflation).

The new standards and requirements for data security in S. 1490 would constitute private-sector mandates as defined in UMRA. While much of the industry already complies in large part with the many of those requirements, a large number of entities in the private sector would face new security standards. CBO estimates that the aggregate direct cost of complying with those new standards would probably exceed the annual threshold established in UMRA for private-sector mandates ($139 million in 2009, 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. 1490 is shown in the following table. The costs of this legislation fall within budget functions 750 (administration of justice), 800 (general government), and any other budget functions that contain salaries and expenses.

	By Fiscal Year, in Millions of Dollars					
	2010	2011	2012	2013	2014	2010-2014
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Estimated Authorization Level	3	5	7	7	7	29
Estimated Outlays	1	3	7	7	7	25

BASIS OF ESTIMATE

For this estimate, CBO assumes that the bill will be enacted early in calendar year 2010, that the necessary amounts will be provided each year, and that spending will follow historical patterns for similar programs.

Most of the provisions of the bill would codify the current practices of the federal government regarding data security and procedures for notification of security breaches. While existing laws generally do not require agencies to notify affected individuals of data breaches, 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. Nonetheless, the federal government is one of the largest providers, collectors, consumers, and disseminators of personnel information in the United States. Although CBO cannot anticipate the number or extent 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 result in significant costs to notify individuals of such a breach.

S. 1490 also would require federal agencies to provide several reports to the Congress concerning data security issues. The legislation would require agencies to conduct additional privacy impact assessments on commercially purchased data that contains personally identifiable information, and the Government Accountability Office would be required to report to the Congress on federal agencies' use of commercial information. In addition, the General Services Administration (GSA) would provide additional security

assessments for certain government contracts involving personally identifiable information. Those assessments would include payroll processing, emergency response and recall, and medical data. Based on information from the Office of Management and Budget and GSA, CBO estimates that the additional staff needed to carry out those tasks and reporting requirements would cost $7 million annually when fully implemented. We expect that it would take about three years to fully implement the requirements.

The legislation also would require a business entity or agency—under certain circumstances—to notify the Secret Service that a security breach has occurred but would permit entities or agencies to apply to the Secret Service for exemption from notice requirements if the personal data was encrypted or similarly protected or if notification would threaten national security. Based on information from the Secret Service, CBO estimates that any additional investigative or administrative costs to that agency would likely be less than $500,000 annually, subject to the availability of appropriated funds.

Other provisions of the bill would require the Federal Trade Commission (FTC) to develop and enforce regulations that would require data brokers to allow individuals to access their personal information and to require companies to assess the vulnerability of their data systems. The FTC would be authorized to collect civil penalties for violations of those new regulations. CBO estimates that those provisions would have no significant effect on spending.

Direct Spending and Revenues

S. 1490 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 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.

ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 1490 contains intergovernmental mandates as defined in UMRA. The bill would preempt laws in 45 states regarding the treatment of personal information. It also would place procedural requirements and limitations on state attorneys general and state insurance authorities. The preemptions would impose no costs on states. CBO estimates that the costs to attorneys general and insurance authorities of complying with the procedural requirements would be small and would not exceed the threshold established in UMRA ($69 million in 2009, adjusted annually for inflation).

ESTIMATED IMPACT ON THE PRIVATE SECTOR

S. 1490 would impose several private-sector mandates as defined in UMRA, including requirements that:

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

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

- Data brokers provide individuals with their personally identifiable information and to change the information if it is incorrect; and

- Any entity taking an adverse action against an individual based on information obtained from a database maintained by a data broker notify the individual of that action.

The majority of businesses already comply with procedures for data security and breach notification that are 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. 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 ($139 million in 2009, 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 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 to assess possible security risks in establishing the program. Additionally, entities 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 entities would be exempt from the requirements of subtitle A. Those include certain financial institutions that are subject to the data security requirements under Gramm-Leach-Bliley Act and

entities that are subject to the data security requirements of the Health Insurance Portability and Accountability Act.

The cost per entity of the data privacy and security requirements would depend in part on the rules to be established by the FTC, the size of the entity, its current ability to secure, record, and monitor access to data, as well as the amount of sensitive, personally identifiable information maintained by the entity. The majority of states already have laws requiring businesses 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, business entities 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 personally identifiable information (PII). 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 of data containing PII would be a significant enhancement of data management hardware and software for the majority of business entities. The aggregate cost of implementing such changes could be substantial.

Security Breach Notification

Subtitle B of title III would require businesses 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' information is compromised. Entities would be able to notify individuals using written letters, the telephone, or email under certain circumstances. The bill also would require those entities to notify the owner or licensee of any such information that the entity does not own or license. 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, business entities 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. They would have to notify the U.S. Secret Service if the breach involves more than 10,000 individuals. The bill, however, would exempt business entities from the notification requirements under certain circumstances.

According to industry sources, millions of individuals' sensitive personally identifiable information is illegally accessed or otherwise breached every year. However, according to those sources, 45 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 the notification requirements would not impose significant additional costs on businesses.

Requirements for Data Brokers

The bill would impose new disclosure and data collection requirements on data brokers. The bill defines a data broker as a business entity which for monetary fees or dues regularly collects for 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.

Section 201 would require certain data brokers to disclose to individuals, upon their request, all personal electronic records relating to an individual that are kept primarily for third parties. 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 information. Upon investigation, data brokers could determine that some requests to change an individual's information are frivolous. However, the data broker would be required to notify any individual requesting a change of information if such an action is 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. However, the cost to data brokers of having to change individuals' information and notifying the individuals could be large. According to information from industry sources, however, some data brokers already correct information based on requests from individuals.

The average cost to large data brokers that currently provide this service is about $8.50 each time a record is disclosed and information is disputed by an individual, according to some industry experts. However, the cost per record may be higher for data brokers who do not currently have systems in place to handle such disputes. Some evidence exists that many individuals' personally identifiable information housed at 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. Because of uncertainty about the number of individuals who would request information under the bill and as a result of

those requests, the amount of information that would need to be changed, CBO cannot estimate the cost of this mandate.

Adverse Actions Using Information from Data Brokers

Section 201 also would require any entity taking an adverse action with respect to an individual based on information contained in a personal electronic record maintained, updated, owned, or possessed by a data broker to notify the individual of the adverse action. The notification can be written or electronic and must include certain information about the data broker. While the per-individual cost of notification would be small, the cost of complying with the mandate would depend on the number of adverse actions that would be taken against individuals by entities. Because data about the incidence of such actions are unavailable, CBO has no basis to determine the direct cost of complying with this mandate.

ESTIMATE PREPARED BY:

Federal Costs: Federal Agencies—Matthew Pickford
U.S. Secret Service—Mark Grabowicz

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