CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

May 17, 2007

S. 495
Personal Data Privacy and Security Act of 2007

As ordered reported by the Senate Committee on Judiciary on May 3, 2007

SUMMARY

S. 495 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. 495 would require data brokers to allow individuals access to their electronic records and publish procedures for individuals to respond to inaccuracies. Finally, the bill would establish the Office of Federal Identity Protection (OFIP) within the Federal Trade Commission (FTC) to assist victims of identity theft to restore the accuracy of their personal information.

Assuming appropriation of the necessary amounts, CBO estimates that implementing the provisions of S. 495 would cost $30 million in 2008 and $335 million over the 2008-2012 period. Enacting S. 495 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. 495 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. 495 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 ($66 million in 2007, adjusted annually for inflation).

S. 495 would impose several private-sector mandates as defined in UMRA. The bill would impose data security standards and procedures, and notification requirements on certain private-sector entities. In addition, it would require data brokers to provide individuals with their personally identifiable information if requested, and to change the information if it is incorrect. Finally, the bill would require any entity taking an adverse action against an individual based on information maintained by a data broker to notify the individual of that action. Because of uncertainty about the number of entities that are already in compliance

with the data security and notification mandates, CBO cannot estimate the incremental cost of complying with those mandates. Further, the number of requests for information and the incidence of adverse actions that would occur under the bill are uncertain. Consequently, CBO cannot determine whether the aggregate direct cost of mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of S. 495 is shown in the following table. The costs of this legislation fall within budget functions 370 (commerce and housing credit), 750 (administration of justice), and 800 (general government).

	By Fiscal Year, in Millions of Dollars				
	2008	2009	2010	2011	2012
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
FTC Office of Federal Identity Protection					
Estimated Authorization Level	33	66	69	73	76
Estimated Outlays	30	63	69	72	76
Other Provisions					
Estimated Authorization Level	3	5	7	7	7
Estimated Outlays	1	3	7	7	7
Total Changes					
Estimated Authorization Level	36	71	76	80	83
Estimated Outlays	31	66	76	79	83

BASIS OF ESTIMATE

For this estimate, CBO assumes that the bill will be enacted during fiscal year 2007, that the necessary amounts will be provided each year, and that spending will follow historical patterns for similar programs.

Spending Subject to Appropriation

S. 495 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. The bill also would establish the Office of Federal Identity Protection within the FTC to help victims of identity theft correct their personal records. CBO estimates that implementing the provisions of S. 495 would cost $335 million over the 2008-2012 period, assuming appropriation of the necessary amounts.

Security Breach Notification. In the event of a security breach of government information likely to involve personal information, S. 495 would require government agencies to notify an individual whose information may have been compromised. The legislation defines personal information as a combination of a person's name or financial information with any additional unique identifier. Notification would be in the form of individual notice (written notice to a home mailing address or via e-mail) as well as through the mass media and credit-reporting agencies if the security breach affects more than 5,000 individuals. The legislation also would require the agency to provide affected individuals with a description of the accessed information, a toll-free number to contact the agency, the names and toll-free telephone numbers of the major credit-reporting agencies, and information regarding state victim assistance protections.

The Federal Information Security Management Act of 2002 sets 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 $5.5 billion a year to secure the government's information systems.

S. 495 would codify the current practices of the federal government regarding data security and security breach notification procedures. 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 also one of the largest providers, collectors, consumers, and disseminators of personnel information in the United States. 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 there would be significant costs to notify individuals of such a security breach.

S. 495 also would require a business entity or agency—under certain circumstances—to notify the Secret Service that a security breach has occurred. The bill also would permit entities or agencies to apply to the Secret Service for exemption from the bill's 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.

Federal Trade Commission. The bill would establish the Office of Federal Identity Protection (OFIP) within the FTC. The OFIP would be responsible for providing individuals with information and assistance when their personal information has been stolen or compromised. Individuals would be able to request assistance that would include accessing remedies available under federal law, restoring the accuracy of personal information, and retrieving stolen information. FTC would be required to develop regulations to enable the OFIP to help restore stolen or otherwise compromised information.

Under current law, the FTC provides general assistance to individuals who call a toll-free number with questions about identity theft or who believe they are the victim of identity theft. Counselors are trained to provide information regarding steps consumers must take to restore the accuracy of their personal information; FTC has entered into a contract with an independent call center to provide assistance and be reimbursed based on the time of each call. This toll-free system received approximately 200,000 complaints in 2006, as well as about 90,000 calls for general information.

By requiring the FTC to develop customer-service teams to provide a higher level of assistance than is offered under current law, CBO expects that the amount of time counselors spend with each individual would increase significantly. Under the bill, counselors, rather than the individual, would be expected to take the necessary steps to restore the accuracy of an individual's personal information and any records containing that information that were stolen or compromised. To accomplish this, counselors would spend more time on the phone with individuals collecting relevant information and make additional calls to creditors and credit-reporting agencies to alert them to the compromised information in their records. Currently, counselors spend an average of eight minutes per call answering questions and suggesting follow-up actions the individual must take to correct his or her personal information. The FTC has estimated that S. 495 would increase the amount of time counselors spend on the phone from eight minutes to more than two hours (including calls to an individual and calls to creditors and credit-reporting agencies). CBO expects that call volume also would increase as individuals become aware of the additional assistance available. Assuming appropriation of the necessary amounts, CBO estimates that the additional time counselors spend on the phone with individuals, creditors, and credit-

reporting agencies would cost about $30 million in 2008 and $310 million over the 2008-2012 period.

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

Other Provisions. S. 495 also would require several reports to the Congress by federal agencies concerning data security issues. The legislation would require agencies to conduct additional privacy impact assessments on commercially purchased private-sector data that contains personally identifiable information. Under the bill, the Government Accountability Office would report to the Congress on federal agencies' use of private-sector information. In addition, the General Services Administration (GSA) would 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 additional staff to fulfill those tasks and reporting requirements under the legislation would cost $7 million annually when fully implemented. For this estimate, we assume that the implementation process would take about three years.

Direct Spending and Revenues

S. 495 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. 495 contains intergovernmental mandates as defined in UMRA. Specifically, S. 495 would:

- Preempt state laws in 35 states regarding the treatment of personal information;

- Place certain procedural requirements and limitations on state attorneys general and state insurance authorities; and

- Preempt state or local law by requiring state and local jurisdictions to accept a certification by the Office of Federal Identity Protection to grant individuals access to business records used in fraudulent transactions.

The preemptions would impose no costs on states. CBO estimates that the costs to attorneys general of complying with the procedural requirements would be small and would not exceed the threshold established in UMRA ($66 million in 2007, adjusted annually for inflation).

ESTIMATED IMPACT ON THE PRIVATE SECTOR

S. 495 would impose several private-sector mandates as defined in UMRA. The bill would:

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

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

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

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

Because of uncertainty about the number of entities that are already in compliance with the data security and notification mandates, CBO cannot estimate the incremental cost of complying with those mandates. Further, the number of requests for information and the incidence of adverse actions that would occur under the bill are uncertain. Consequently, CBO cannot determine whether the aggregate direct cost of mandates in the bill would exceed the annual threshold established by UMRA for private-sector mandates ($131million in 2007, adjusted annually for inflation).

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. The bill would direct the FTC to develop rules that identify privacy and security requirements for business entities. Business entities would be required to conduct risk assessments to identify possible security risks in establishing the program. They also would have to conduct periodic vulnerability testing on their programs. Additionally, entities would have to train their employees.

Some entities would be exempt from the requirements of subtitle A. These 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 per-entity cost of the data privacy and security requirements would depend on the rules to be established by the FTC, the size of the entity, and the amount of sensitive, personally identifiable information maintained by the entity. According to industry and government sources, many states already have laws requiring business entities to utilize data security programs, and moreover, it is the current practice of many businesses to use security measures to protect sensitive data. However, because of uncertainty about the number of entities that are already in compliance with the data security mandates, CBO cannot estimate the incremental cost of complying with those mandates.

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, 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. The bill, however, would exempt business entities from the notification requirements under certain circumstances.

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 5,000 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.

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

  - More than 10,000 individuals are affected by a security breach.

  - A security breach involves a database that contains sensitive, personally identifiable information on more than one million people.

  - A security breach involves databases owned by the federal government.

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

According to industry and government sources, millions of individuals' sensitive personally identifiable information is illegally accessed every year. However, according to those sources, 38 states already have laws requiring notification in the event of a security breach. In addition, it is the current practice of many business entities to notify individuals in the event of a security breach. Because of uncertainty about the number of entities that are already in compliance with the notification mandates, CBO cannot estimate the incremental cost of complying with the notification requirement under the bill.

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 a 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 could be large. According to information from industry sources, however, some data brokers already correct information based on the individual requests. 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 changed, CBO cannot estimate the cost of this mandate.

Adverse Actions Using Information From Data Brokers

The section 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. CBO does not have enough information about the incidence of such actions to determine the direct cost of complying with the mandate.

ESTIMATE PREPARED BY:

Federal Costs: Federal Agencies—Matthew Pickford
Federal Trade Commission—Susan Willie
U.S. Secret Service—Mark Grabowicz

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

Impact on the Private Sector: Paige Piper/Bach

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis