Calendar No. 208

111TH CONGRESS, *1st Session* | SENATE | REPORT 111–110

PERSONAL DATA PRIVACY AND SECURITY ACT OF 2009

DECEMBER 17, 2009.—Ordered to be printed

Mr. LEAHY, from the Committee on the Judiciary, submitted the following

R E P O R T

[To accompany S. 1490]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to which was referred the bill (S. 1490), to prevent and mitigate identity theft, to ensure privacy, to provide security protections for personal data, 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, having considered the same, reports favorably thereon, with an amendment, and recommends that the bill, as amended, do pass.

CONTENTS

I. BACKGROUND AND PURPOSE OF THE PERSONAL DATA PRIVACY AND SECURITY ACT OF 2009

A. SUMMARY

Advanced technologies, combined with the realities of the post–9/11 digital era, have created strong incentives and opportunities

for collecting and selling personal information about ordinary Americans. Today, private sector and governmental entities alike routinely traffic in billions of electronic personal records about Americans. Americans rely on this data to facilitate financial transactions, provide services, prevent fraud, screen employees, investigate crimes, and find loved ones. The Government also relies upon this information to enhance national security and to combat crime.

The growing market for personal information has also become a treasure trove that is both valuable and vulnerable to identity thieves. As a result, the consequences of a data security breach can be quite serious. For Americans caught up in the endless cycle of watching their credit unravel, undoing the damage caused by security breaches and identity theft can become a time-consuming and lifelong endeavor. In addition, while identity theft is a major privacy concern for most Americans, the use and collection of personal data by Government agencies can have an even greater impact on Americans' privacy. The loss or theft of Government data can potentially expose ordinary citizens, Government employees, and members of the armed services alike to national security and personal security threats.

Despite these well-known dangers, the Nation's privacy laws lag far behind the capabilities of technology and the cunning of identity thieves. The Personal Data Privacy and Security Act of 2009 is a comprehensive, bipartisan privacy bill that seeks to close this privacy gap, by establishing meaningful national standards for providing notice of data security breaches, and addressing the underlying problem of lax data security, to make it less likely for data security breaches to occur in the first place.

B. THE GROWING PROBLEM OF DATA SECURITY BREACHES AND IDENTITY THEFT

According to the Privacy Rights Clearinghouse, more than 340 million records containing sensitive personal information have been involved in data security breaches since 2005.[1] Since the Personal Data Privacy and Security Act was first reported by the Judiciary Committee in November 2005, there have been at least 599 different data security breaches in the United States, affecting millions of American consumers.[2] For example, in January 2009, Heartland Payment Systems, one of the Nation's leading processors of credit and debit card transactions, announced that its processing system records containing more than 130 million credit card accounts had been breached by hackers. In January 2007, mega-retailer TJX disclosed that it suffered a data breach affecting at least 45.7 million credit and debit cards.[3] These data breaches follow many other commercial data breaches, collectively affecting millions of Americans, including data security breaches at ChoicePoint and LexisNexis.

Federal Government agencies have also suffered serious data security breaches. In February 2009, the Federal Aviation Adminis-

[1] See "Privacy Rights Clearinghouse Chronology of Data Breaches," available at *http://www.privacyrights.org/*.

[2] Id.

[3] "Breach of data at TJX is called the biggest ever, Stolen numbers put at 45 .7 million," Boston Globe, March 29, 2007.

tration revealed that computer hackers breached one of its servers and stole sensitive personal information concerning 45,000 current and former FAA employees.[4] In June 2008, Walter Reed Medical Center reported that the personal information of 1,000 Military Health System beneficiaries may have been improperly disclosed through the unauthorized sharing of data.[5] In May 2006, the Department of Veterans Affairs lost an unsecured laptop computer hard drive containing the health records and other sensitive personal information of approximately 26.5 million veterans and their spouses.[6] And, in May, 2007, the Transportation Security Administration (TSA) reported that the personal and financial records of 100,000 TSA employees were lost after a computer hard drive was reported missing from the Agency's headquarters, exposing the Department of Homeland Security to potential national security risks.[7]

The steady wave of data security breaches in recent years is a window into a broader, more challenging trend. Insecure databases are now low-hanging fruit for hackers looking to steal identities and commit fraud. Lax data security is also a threat to American businesses. The President's recent report on Cyberspace Policy Review noted that industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion.[8] Because data security breaches adversely affect many segments of the American community, a meaningful solution to this growing problem must carefully balance the interests and needs of consumers, business, and the Government.

C. THE PERSONAL DATA PRIVACY AND SECURITY ACT OF 2009

The Personal Data Privacy and Security Act of 2009 takes several meaningful and important steps to balance the interests and needs of consumers, business, and the Government in order to better protect Americans sensitive personal data. This legislation is supported by a wide range of consumer, business, and Government organizations, including, the United States Secret Service, the Federal Trade Commission, Microsoft, the Business Software Alliance, Consumer Federation of America, Consumers Union, the American Federation of Government Employees, Facebook, the Center for Democracy & Technology, and the ACLU.

1. Access and correction

First, to provide consumers with tools that enable them to guard against identity theft, the bill gives consumers the right to know what sensitive personal information commercial data brokers have about them. In addition, the bill extends the protections afforded under the Fair and Accurate Credit Transactions Act (FACTA) to this data, by allowing consumers to correct their personal information if it is inaccurate. Under circumstances where a business entity makes an adverse decision based on information provided to it

[4] "FAA Breach Heightens Cybersecurity Concerns," Federal Computer Week, February 23, 2009.

[5] "Walter Reed: Data Breach at Military Hospitals," The Associated Press, June 3, 2008.

[6] See Testimony of the Honorable James Nicholson, Secretary of Veterans Affairs, before the House Committee on Government Reform, June 8, 2006.

[7] See "TSA seeks hard drive, personal data for 100,000," USA Today, May 5, 2007; see also, the Federal Times, "Union Sues TSA over loss of data on employees," May 9, 2007.

[8] "President's Report on Cyberspace Policy Review," May 29, 2009, at page 2.

by a data broker, the bill also requires that the business entity notify the consumer of the adverse decision and provide the consumer with the information needed to contact the data broker and correct the information. There is an exemption to this requirement for fraud databases, to ensure that the Government can detect and combat fraud. The right of consumers to access and correct their own sensitive personal data is a simple matter of fairness. The principles of access and correction incorporated in the bill have precedent in the credit reporting industry context and these principles have been adapted to the data broker industry.

2. Data Security Program

Second, the bill recognizes that, in the Information Age, any company that wants to be trusted by the public must earn that trust by vigilantly protecting the information that it uses and collects. The bill takes important steps to accomplish this goal, by requiring that companies that have databases with sensitive personal information on more than 10,000 Americans establish and implement a data privacy and security program. There are exemptions to this requirement for companies already subject to data security requirements under the Gramm-Leach-Bliley (GLB) Act and the Health Information Portability and Accountability (HIPAA) Act.

3. Notice

Third, because American consumers should know when they are at risk of identity theft, or other harms because of a data security breach, the bill also requires that business entities and Federal agencies promptly notify affected individuals and law enforcement when a data security breach occurs. Armed with such knowledge, consumers can take steps to protect themselves, their families, and their personal and financial well-being. The trigger for notice to individuals is "significant risk of harm," and this trigger includes appropriate checks and balances to prevent over-notification and underreporting of data security breaches.

In this regard, the bill recognizes that there are harms other than identity theft that can result from a data security breach, including harm from other financial crimes, stalking, and other criminal activity. Consequently, the bill adopts a trigger of "significant risk of harm," rather than a weaker trigger of "significant risk of identity theft," for the notice requirement for individuals in the legislation.[9] There are exemptions to the notice requirements for individuals for national security and law enforcement reasons, as well as an exemption to this requirement for credit card companies that have effective fraud-prevention programs.[10] The bill con-

[9] A notice trigger based upon "significant risk of identity theft" would weaken the notice provisions in S. 1490 and such a standard would also fail to adequately protect consumers. First, the weaker "significant risk of identity theft" standard only requires notification of consumers when a business entity or Federal agency affirmatively finds that there is a significant risk of the specific crime of identity theft. In addition, as discussed above, there are other harms that could result from data security breaches, such as stalking, physical harm, or threats to national security, that are not addressed or covered under a notice standard based solely on the risk of identity theft.

[10] Some have incorrectly argued that S. 1490 will result in over-notification of consumers and in a lack of clarity for business. To the contrary, the bill contains meaningful checks and balances, including the risk assessment and financial fraud prevention provisions in Section 312, to prevent over-notification and the underreporting of data security breaches. The risk assessment provision in Section 312(b), furthermore, provides businesses with an opportunity to fully evaluate data security breaches when they occur, to determine whether notice should be pro-

templates that a reasonable delay of notice could include the time necessary for a victim company to conduct a risk assessment under Section 302(a)(3).

In addition, to strengthen the tools available to law enforcement to investigate data security breaches and to combat identity theft, the bill also requires that business entities and Federal agencies notify the Secret Service of a data security breach within 14 days of the occurrence of the breach. This notice will provide law enforcement with a valuable head start in pursuing the perpetrators of cyber intrusions and identity theft. The bill also empowers the Secret Service to obtain additional information about the data breach from business entities and Federal agencies to determine whether notice of the breach should be given to consumers and other law enforcement agencies. This mechanism gives businesses and agencies certainty as to their legal obligation to provide notice and prevents them from sending notices when they are unnecessary, which over time, could result in consumers ignoring such notices. The notice of breach provisions for electronic health records that Congress enacted in the American Reinvestment and Recovery Act (ARRA) apply to information that is accessed or disclosed from personal health records. The notice of breach provisions in this bill are not intended to preempt the notice requirements established by ARRA.

The bill also recognizes the benefits of separating the notice obligations of owners of personally identifiable information and third parties who use and manage personally identifiable information on the owner's behalf. The bill imposes an obligation on third parties that suffer a data security breach to notify the owners or licensees of the personally identifiable information, who would, in turn, notify consumers. If the owner or licensee of the data gives notice of the breach to the consumer, then the breached third party does not have to give notice. The bill also states that it does not abrogate any agreement between a breached entity and a data owner or licensee to provide the required notice in the event of a breach. Separating the notice obligations between data owners and licensees, and third parties, will encourage data owners and licensees to address the notice obligation in agreements with third parties and will help to ensure that consumers will receive timely notice from the entity with which they have a direct relationship and would recognize upon receiving such notice, in the event of a data security breach. However, this notice can only be effective if the entity which suffers the breach, and any other third parties, provide to the entity who will give the notice complete and timely information about the nature and scope of the breach and the identity of the entity breached.

---

vided to consumers. In addition, the bill complements and properly builds upon other Federal statutes governing data privacy and security to ensure clarity for business in this area. For example, to avoid conflicting obligations regarding the bill's data security program requirements, Section 301(c) specifically exempts financial institutions that are already subject to, and complying with, the data privacy and security requirements under GLB, as well as HIPAA-regulated entities. The bill also builds upon existing Federal laws and guidance, such as the data security protections established by the Office of the Comptroller of the Currency for financial institutions and the access and correction provisions in the Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act, to clarify the obligations of business.

4. Enforcement

Fourth, this legislation also establishes tough, but fair, enforcement provisions to punish those who fail to notify consumers of a data security breach, or to maintain a data security program. The bill makes it a crime for any individual, with knowledge of the obligation to provide notice of a security breach, to intentionally and willfully conceal the breach that subsequently causes economic harm to consumers. Violators of this provision are subject to a criminal fine under title 18, or imprisonment of up to five years, or both. This provision is no more onerous than criminal provisions for other types of fraudulent conduct which causes similar harm to individuals.

The bill also contains strong civil enforcement provisions. The bill authorizes the Federal Trade Commission (FTC) to bring a civil enforcement action for violations of the data security program requirements in the bill and to recover a civil penalty of not more than $5,000 per violation, per day and a maximum penalty of $500,000 per violation.[11] In addition, the bill authorizes State Attorneys General, or the U.S. Attorney General, to bring a civil enforcement action against violators of the notice requirements in the bill and to recover a civil penalty of not more than $1,000 per individual, per day and a maximum penalty of $1,000,000 per violation, unless the violation is willful or intentional. It is not uncommon for Congress to authorize both Federal and State regulators to enforce Federal consumer protection laws. In fact, Federal antitrust laws, the CAN–SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003), and the Communications Act of 1934 also authorize State Attorneys General to seek damages or to enjoin further Federal law violations. The State enforcement provisions in this bill are modeled after those laws.

The bill authorizes the Secret Service to investigate data security breaches and to provide guidance to companies that have been the victim of a data security breach on their notice obligations under the bill. Since 1984, Congress has provided statutory authority for the Secret Service to investigate a wide range of financial crimes, including offenses under 18 U.S.C. § 1028 (false identification fraud), § 1029 (access device fraud) and § 1030 (computer fraud). In the last two decades, the Secret Service has conducted more than 733,000 financial fraud and identity theft investigations involving these statutes, leading to the prosecution of more than 116,000 individuals.[12] Pursuant to the notice requirements in the bill, the Secret Service's Criminal Intelligence Section would analyze, coordinate and monitor all data breach investigations reported to it by victim companies.

When the Criminal Intelligence Section receives notification of a data breach, it would immediately analyze the information and refer the case to the appropriate field office and/or electronic/financial crimes task force, for investigation and prosecution. Throughout this process, the Criminal Intelligence Section would stand ready to support the victim company, investigating field office or task force, and prosecuting U.S. Attorney's Office as needed. The Criminal Intelligence Section would also coordinate with the Com-

[11] Double penalties may be recovered for intentional or willful violations of this provision.
[12] See Secret Service White Paper, "Data Broker Legislation—S. 1490," May 2007.

puter Crime and Intellectual Property Sections (CCIPS) of the Department of Justice to ensure proper and timely response through the Federal judicial system, regardless of where the data breach occurred. In addition, the Criminal Intelligence Section would have the responsibility of notifying Federal law enforcement and State Attorneys General as mandated by the legislation.

Section 316(b) of the bill expressly requires that the FBI must be notified of any data security breach that involves espionage, foreign counterintelligence, or national security matters. Under title 18, section 1030(d)(1), the Secret Service and FBI have concurrent jurisdiction to investigate Section 1030 violations relating to false identification fraud, access device fraud, and computer fraud. Section 1030 designates the FBI as the primary investigative agency for such offenses if they involve espionage, foreign counterintelligence, and other national security matters. Accordingly, the bill incorporates this requirement in the context of breach notice, so that the FBI is promptly notified of any data breach matters that involve espionage, foreign counterintelligence, or national security.

5. Preemption

The legislation also carefully balances the need for Federal uniformity in certain data privacy laws and the important role of States as leaders on privacy issues. Section 304 of the bill (relation to other laws) preempts State laws with respect to requirements for administrative, technical, and physical safeguards for the protection of sensitive personally identifying information. These requirements, which are referred to in this Section, are the same requirements set forth in Section 302 of the bill.

Section 319 of the bill (effect on Federal and State laws) also preempts State laws on breach notification. However, in recognition of the important role that the States have played in developing breach notification, the bill carves out an exception to preemption for State laws regarding providing consumers with information about victim protection assistance that is provided for by the State.

In addition, Section 319 of the bill provides that the notice requirements in S. 1490 supersede "any provision of law of any State relating to notification of a security breach, except as provided in Section 314(b) of the bill." The bill's subtitle on security breach notification applies to "any agency, or business entity engaged in interstate commerce," and the term "agency" is defined in the bill by referencing section 551 of title 5, United States Code, which pertains to Federal Governmental entities. As a result, the security breach notification requirements in the bill have no application to State and local governmental entities, and the Committee does not intend for this provision to preempt or displace State laws that address obligations of State and local governmental entities to provide notice of security breach.

6. Government Use

Finally, the bill establishes important new checks on the Government's use of personal data. In July 2009, the Government Accountability Office (GAO) released a new report on Government information security policies that found persistent weaknesses in

Federal agency data security policies and practices.[13] According to the report, all 24 of the major Federal agencies had weaknesses in their information security controls.[14] To address these concerns, the bill requires that Federal agencies consider whether data brokers can be trusted with Government contracts that involve sensitive information about Americans before awarding Government contracts. The bill also requires that Federal agencies audit and evaluate the information security practices of Government contractors and third parties that support the information technology systems of Government agencies. In addition, the bill requires that Federal agencies adopt regulations that specify the personnel allowed to access Government data bases containing personally identifiable information and adopt regulations that establish the standards for ensuring, among other things, the legitimate Government use of sensitive personal information.[15]

II. History of the Bill and Committee Consideration

A. Introduction of the Bill

Chairman Leahy introduced the Personal Data Privacy and Security Act of 2009 on July 22, 2009. This bipartisan, comprehensive privacy bill is cosponsored by Senators Specter, Hatch, Schumer, Durbin, Feingold, Cardin, and Brown.

This legislation is very similar to the Personal Data Privacy and Security Act of 2007, S. 495, which Senators Leahy and Specter introduced on July 6, 2007 and to the Personal Data Privacy and Security Act of 2005, S. 1789, which Senators Leahy and Specter introduced on September 29, 2005. The Judiciary Committee favorably reported S. 495 on May 3, 2007 by voice vote and S. 1789 on November 17, 2005, by a bipartisan vote of 13 to 5.

The Committee has held three hearings related to S. 1490. On April 13, 2005, the Judiciary Committee held a hearing titled, "Securing Electronic Personal Data: Striking a Balance between Privacy and Commercial and Governmental Use." This hearing examined the practices and weaknesses of the rapidly growing data broker industry and, in particular, how data brokers were handling

---

[13] See Report of the U.S. Government Accountability Office, "Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses," (July 2009).

[14] Id.

[15] In their accompanying views, the Minority makes several arguments in opposition to the bill that are without merit. First, the arguments that the bill's definitions for "sensitive personally identifiable information" and "security breach" are too broad are wholly unfounded. The Committee crafted the definition for sensitive personally identifiable information after careful consultation with the United States Secret Service, the FTC and several consumer organizations that have had significant experience with the kinds of information that is most vulnerable to identity theft and other cyber crimes. Moreover, the definition of security breach is fully consistent with other Federal computer fraud and privacy laws. See, e.g., §§ 18 U.S.C. 1030 (a)(2) and (3) (Computer Fraud and Abuse Act); 18 U.S.C. §§ 2510(4) (definition of "intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."). The Minority also incorrectly states that the bill does not exempt entities that are already regulated by other Federal laws governing data privacy and security. Section 201(b) of the bill clearly and expressly exempts FCRA, GLB and HIPPA-regulated entities from the transparency and accuracy provisions of the bill. Moreover, section 301(c) expressly exempts GLB and HIPPA-regulated entities from the data privacy and security program requirements in the bill. Lastly, the notion that the bill should exclude all law enforcement and counterterrorism programs from the privacy impact assessment requirements in the bill is simply without merit. The Minority cites no evidence to demonstrate that privacy impact assessments posed a unique concern for Federal agencies that are engaged in law enforcement or counterterrorism activities. To the contrary, many Federal agencies already conduct privacy impact assessments for these kinds of programs, to the benefit of all Americans.

the most sensitive personal information about Americans. The hearing also explored how Congress could establish a sound legal framework for future data privacy legislation that would ensure that privacy, security, and civil liberties will not be pushed aside in the new Digital Age. The following witnesses testified at this hearing: Deborah Platt Majoras, Chairman of the Federal Trade Commission; Chris Swecker, Assistant Director for the Criminal Investigative Division at the Federal Bureau of Investigation; Larry D. Johnson, Special Agent in Charge of the Criminal Investigative Division of the U.S. Secret Service; William H. Sorrell, President of the National Association of Attorneys General; Douglas C. Curling, President, Chief Operating Officer, and Director of ChoicePoint, Inc.; Kurt P. Sanford, President & CEO of the U.S. Corporate & Federal Markets LexisNexis Group; Jennifer T. Barrett, Chief Privacy Officer of Acxiom Corp.; James X. Dempsey, Executive Director of the Center for Democracy & Technology; and Robert Douglas, CEO of PrivacyToday.com.

On March 21, 2007, the Judiciary Committee's Subcommittee on Terrorism, Technology and Homeland Security held a hearing titled, "Identity Theft: Innovative Solutions for an Evolving Problem." This hearing examined the problem of identity theft and legislative solutions to this problem, and discussed the need for Federal legislation on data breach notification. The following witnesses testified at this hearing: Ronald Tenpas, Associate Deputy Attorney General, United States Department of Justice; Lydia Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission; James Davis, Chief Information Officer and Vice Chancellor for Information Technology, University of California, Los Angeles; Joanne McNabb, Chief, California Office of Privacy Protection; and Chris Jay Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic, School of Law (Boalt Hall), University of California, Berkeley.

On January 27, 2009, the Committee held a hearing titled, "Health IT: Protecting Americans' Privacy in the Digital Age." This hearing examined best practices for protecting electronic health records and for protecting Americans' health privacy. The following witnesses appeared at that hearing: Adrienne Hahn, Senior Attorney and Program Manager for Health Policy, Consumers Union; James Hester, Jr. Ph.D., Director, Health Care Reform Commission, Vermont State Legislature; Deven McGraw, Director, Health Privacy Project, Center for Democracy and Technology; Michael Stokes, Principal Lead Program Manager, HealthVault, Microsoft Corporation; John Houston, Vice President of Information Security and Privacy, University of Pittsburgh Medical Center; and David Merritt, Project Director, Center for Health Transformation and the Gingrich Group.

B. COMMITTEE CONSIDERATION

On October 23, 2009, S. 1490 was placed on the Judiciary Committee's agenda. The Committee considered this legislation on November 5, 2009.

During the Committee's consideration of S. 1490, three amendments to the bill were offered and one amendment was unanimously adopted by the Committee:

First, the Committee adopted, without objection, a manager's amendment to S. 1490 which Chairman Leahy offered on behalf of himself and Senator Specter. The manager's amendment clarifies enforcement provisions in the bill, including: (1) adding a fraud data base exemption to the provisions allowing consumers to access and correct their personal data; (2) clarifying that the FTC has the authority to enforce the civil enforcement provisions in the bill with respect to business entities; (3) harmonizing the notice of breach provisions in the bill; (4) striking the provision establishing an Office of Federal Identity Protection within the FTC; (5) clarifying the definition of encryption and the standards for the data privacy and security program safe harbor; and (6) amending the definition of security breach to clarify that fraud is a harm that the bill seeks to prevent and address.

The Committee rejected by a vote of 6 to 13 an amendment offered by Senator Sessions (GRA09859) which would limit the information included in the definition of "security breach."

The Committee rejected by a vote of 7 to 12 an amendment offered by Senator Kyl (GRA09884) which would create an exception to the requirement that that Federal agencies appoint a Chief Privacy Officer and conduct privacy impact assessments for law enforcement and national security matters.

The Committee then voted to report the Personal Data Privacy and Security Act of 2009, as amended, favorably to the Senate. The Committee proceeded by roll call vote as follows:

Tally: 14 Yeas, 5 Nays

Yeas (14): Cardin (D–MD), Durbin (D–IL), Feingold (D–WI), Feinstein (D–CA), Franken (D–MN), Grassley (R–IA), Hatch (R–UT), Kaufman (D–DE), Klobuchar (D–MN), Kohl (D–WI), Leahy (D–VT), Schumer (D–NY), Specter (D–PA), Whitehouse (D–RI).

Nays (5): Coburn (R–OK), Cornyn (R–TX), Graham (R–SC), Kyl (R–AZ), Sessions (R–AL).

III. Section-by-Section Summary of the Bill

Section 1. Short title

This section provides that the legislation may be cited as the "Personal Data Privacy and Security Act of 2009."

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

Section 101. Organized criminal activity in connection with unauthorized access to personally identifiable information

Section 101 amends 18 U.S.C. 1961(1) to add intentionally accessing a computer without authorization to the definition of racketeering activity.

Section 102. Concealment of security breaches involving personally identifiable information

Section 102 makes it a crime for a person who knows of a security breach requiring notice to individuals under title III of this Act, and of the obligation to provide such notice, to intentionally and willfully conceal the fact of, or information related to, that se-

curity breach. Punishment is either a fine under title 18, or imprisonment of up to 5 years, or both.

Section 103. Review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information

Section 103 requires the U.S. Sentencing Commission to review and, if appropriate, amend the Federal sentencing guidelines for persons convicted of using fraud to access, or to misuse, digitized or electronic personally identifiable information, including sentencing guidelines for the offense of identity theft or any offense under 18 U.S.C. §§ 1028, 1028A, 1030, 1030A, 2511, and 2701.

Section 104. Effects of identity theft on bankruptcy proceedings

Section 104 amends 11 U.S.C. §§ 101 and 707(b) to exempt debtors from section 707(b)(2) means testing under the Bankruptcy Abuse Prevention and Consumer Protection Act, if the debtor's financial problems were caused by identity theft. This section requires that, to be eligible for this exemption, the identity theft must result in at least $20,000 in debt in one year, 50 percent of the debtor's bankruptcy claims, or 25 percent of the debtor's gross income for a 12–month period. The purpose of this provision is to ensure that victims who incur debts due to identity theft have all available protections under the bankruptcy code.

TITLE II—DATA BROKERS

Title II addresses the data brokering industry that has come of age, prompted by technology developments and changes in marketplace incentives. Data brokers collect and sell billions of private and public records about individuals, including personal, financial, insurance, medical and "lifestyle" data, as well as other sensitive information, such as details on neighbors and relatives, or even digital photographs of individuals. Companies like ChoicePoint, LexisNexis, and Acxiom, which are generally regarded as leaders in this industry, use this information to provide a variety of products and services, including fraud prevention, identity verification, background screening, risk assessments, individual digital dossiers, and tools for analyzing data.

Although some of the products and services offered by data brokers are subject to existing privacy and security protections aimed at credit reporting agencies and the financial industry under the Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley (GLB), many are not subject to such protections. In addition, there has been insufficient oversight of the industry's practices, including the accuracy and handling of sensitive data. These concerns have been highlighted by numerous reports of harm caused by inaccurate data records. This title draws from the principles in FCRA and GLB to close these loopholes.

Section 201. Transparency and accuracy of data collection

Section 201 applies disclosure and accuracy requirements to data brokers that engage in interstate commerce and offer any product or service to third parties that allows access to, or use, compilation, distribution, processing, analyzing or evaluating of personally identifiable information. Section 201 requirements are not applicable to

products and services already subject to similar disclosure and accuracy provisions under FCRA and GLB, and implementing regulations.

Section 201 requires data brokers to disclose to individuals, upon their request and for a reasonable fee, all personal electronic records pertaining to that individual that the data broker maintains for disclosure to third parties. Section 201 also requires data brokers to establish a fair process for individuals to dispute, flag or correct inaccuracies in any information that was not obtained from a licensor or public record. Modeled after section 611 of FCRA, section 201 requires data brokers to: (1) investigate disputed information within 30 days; (2) notify any data furnishers who provided disputed information and identify such data furnishers to the individual disputing the information; (3) provide notice to individuals on dispute resolution procedures and the status of dispute investigations, including whether the dispute was determined to be frivolous or irrelevant, whether the disputed information was confirmed to be accurate, or whether the disputed information was deleted as inaccurate; and (4) allow individuals to include a statement of dispute in the electronic records containing the disputed personal information. If the information was obtained from a licensor or public record, the data broker must provide the individual with contact information for the source of the data.

Section 201 also provides that, under circumstances where a person or business takes an adverse action regarding a consumer, which is based in whole or in part on data maintained by a data broker, the person or business must notify the consumer in writing of the adverse action and provide contact information for the data broker that furnished the information, a copy of the information at no cost and the procedures for correcting such information. There is an exemption for fraud databases.

Section 202. Enforcement

A data broker that violates the access and correction provisions of section 201 is subject to penalties of $1,000 per violation per day with a maximum penalty of $250,000 per violation. A data broker that intentionally or willfully violates these provisions is subject to additional penalties of $1,000 per violation per day, with a maximum of an additional penalty of $250,000 per violation.

The Federal Trade Commission (FTC) will enforce section 202 and may bring an enforcement action to recover penalties under this provision. States have the right to bring civil actions under this section on behalf of their residents in U.S. district courts, and this section requires that States provide advance notice of such court proceedings to the FTC, where practicable. The FTC also has the right to stay any State action brought under this section and to intervene in a State action.

Section 203—Relation to State Laws

Section 203 preempts State laws with respect to the access and correction of personal electronic records held by data brokers.

Section 204—Effective Date

Section 204 provides that title II will take effect 180 days after the date of the enactment of the Personal Data Privacy and Security Act.

TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

SUBTITLE A—A DATA PRIVACY AND SECURITY PROGRAM

Section 301. Purpose and Applicability of Data Privacy and Security Program

Section 301 addresses the data privacy and security requirements of section 302 for business entities that compile, access, use, process, license, distribute, analyze or evaluate personally identifiable information in electronic or digital form on 10,000 or more U.S. persons. Section 301 exempts from the data privacy and security requirements of section 302 businesses already subject to, and complying with, similar data privacy and security requirements under GLB and implementing regulations, as well as examination for compliance by Federal functional regulators as defined in GLB, and HIPAA regulated entities.

Section 302. Requirements for a Data Privacy and Security Program

Section 302 requires covered business entities to create a data privacy and security program to protect and secure sensitive data. The requirements for the data security program are modeled after those established by the Office of the Comptroller of the Currency for financial institutions in its Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. § 30.6 Appendix B (2005).

A data privacy and security program must be designed to ensure security and confidentiality of personal records, protect against anticipated threats and hazards to the security and integrity of personal electronic records, protect against unauthorized access and use of personal records, and ensure proper back-up storage and disposal of personally identifiable information. In addition, section 302 requires a covered business entity to: (1) regularly assess, manage and control risks to improve its data privacy and security program; (2) provide employee training to implement its data privacy and security program; (3) conduct tests to identify system vulnerabilities; (4) ensure that overseas service providers retained to handle personally identifiable information, but which are not covered by the provisions of this Act, take reasonable steps to secure that data; and (5) periodically assess its data privacy and security program to ensure that the program addresses current threats. Section 302 also requires that the data security program include measures that allow the data broker to: (1) track who has access to sensitive personally identifiable information maintained by the data broker; and (2) ensure that third parties or customers who are authorized to access this information have a valid legal reason for accessing or acquiring the information.

Section 303. Enforcement

Section 303 gives the FTC the right to bring an enforcement action for violations of sections 301 and 302 in subtitle A. Business entities that violate sections 301 and 302 are subject to a civil penalty of not more than $5,000 per violation, per day and a maximum penalty of $500,000 per violation. Intentional and willful violations of these sections are subject to an additional civil penalty of $5,000 per violation, per day and an additional maximum penalty of $500,000 per violation. This section also grants States the right to bring civil actions on behalf of their residents in U.S. district courts, and requires States to give advance notice of such court proceedings to the FTC, where practicable. There is no private right of action under this subtitle.

Section 304. Relation to other laws

Section 304 preempts State laws relating to administrative, technical, and physical safeguards for the protection of sensitive personally identifying information. The requirements referred to in this section are the same requirements set forth in section 302.

SUBTITLE B—SECURITY BREACH NOTIFICATION

Section 311. Notice to individuals

Section 311 requires that a business entity or Federal agency give notice to an individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, compromised, following the discovery of a data security breach. The notice required under section 311 must be made without unreasonable delay. Section 311(b) requires that a business entity or Federal agency that does not own or license the information compromised as a result of a data security breach notify the owner or licensee of the data. The owner or licensee of the data would then provide the notice to individuals as required under this section. However, agreements between owners, licensees and third parties regarding the obligation to provide notice under section 311 are preserved.

Section 312. Exemptions

Section 312 allows a business entity or Federal agency to delay notification by providing a written certification to the U.S. Secret Service that providing such notice would impede a criminal investigation, or damage national security. This provision further requires that the Secret Service must review all certifications from business entities (and may review certifications from agencies) seeking an exemption from the notice requirements based upon national security or law enforcement, to determine if the exemption sought has merit. The Secret Service has 10 business days to conduct this review, which can be extended by the Secret Service if additional information is needed. Upon completion of the review, the Secret Service must provide written notice of its determination to the agency or business entity that provided the certification. If the Secret Service determines that the exemption is without merit, the exemption will not apply. Section 312 also prohibits Federal agencies from providing a written certification to delay notice, to conceal violations of law, prevent embarrassment or restrain competition.

Section 312(b) exempts a business entity or agency that conducts a risk assessment after a data breach occurs, and finds no significant risk of harm to the individuals whose sensitive personally identifiable information has been compromised, from the notice requirements of section 311, provided that: (1) the business entity or Federal agency notifies the Secret Service of the results of the risk assessment within 45 days of the security breach; and (2) the Secret Service does not determine within 10 business days of receipt the notification that a significant risk of harm does in fact exist and that notice of the breach should be given. Under section 312(b) a rebuttable presumption exists that the use of encryption technology, or other technologies that render the sensitive personally identifiable information indecipherable, and thus, that there is no significant risk of harm.

Section 312(c) also provides a financial fraud prevention exemption from the notice requirement, if a business entity has a program to block the fraudulent use of information—such as credit card numbers—to avoid fraudulent transactions. Debit cards and other financial instruments are not covered by this exemption.

Section 313. Methods of notice

Section 313 provides that notice to individuals may be given in writing to the individuals last known address, by telephone or via email notice, if the individual has consented to email notice. Media notice is also required if the number of residents in a particular State whose information was, or is reasonably believed to have been, compromised exceeds 5,000 individuals.

Section 314. Content of notification

Section 314 requires that the notice detail the nature of the personally identifiable information that has been compromised by the data security beach, a toll free number to contact the business entity or Federal agency that suffered the breach, and the toll free numbers and addresses of major credit reporting agencies. Section 314 also preserves the right of States to require that additional information about victim protection assistance be included in the notice.

Section 315. Coordination of notification with credit reporting agencies

Section 315 requires that, for situations where notice of a data security breach is required for 5,000 or more individuals, a business entity or Federal agency must also provide advance notice of the breach to consumer reporting agencies.

Section 316. Notice to law enforcement

Section 316 requires that business entities and Federal agencies notify the Secret Service of the fact that a security breach occurred within 14 days of the breach, if the data security breach involves: (1) more than 10,000 individuals; (2) a database that contains information about more than one million individuals; (3) a Federal Government database; or (4) individuals known to be Government employees or contractors involved in national security or law enforcement. The Secret Service is responsible for notifying other Federal law enforcement agencies, including the FBI, and the rel-

evant State Attorneys General within 14 days of receiving notice of a data security breach.

Section 317. Enforcement

Section 317 allows the Attorney General to bring a civil action to recover penalties for violations of the notification requirements in subtitle B. Violators are subject to a civil penalty of up to $1,000 per day, per individual and a maximum penalty of $1 million per violation, unless the violation is willful or intentional.

Section 318. Enforcement by State Attorneys General

Section 318 allows State Attorneys General to bring a civil action in U.S. district court to enforce subtitle B. The Attorney General may stay, or intervene in, any State action brought under this subtitle.

Section 319. Effect on Federal and State law

Section 319 preempts State laws on breach notification, with the exception of State laws regarding providing consumers with information about victim protection assistance that is available to consumers in a particular State. Because the breach notification requirements in the bill do not apply to State and local Government entities, this provision does not preempt State or local laws regarding the obligations of State and local government entities to provide notice of a data security breach.

Section 320. Authorization of appropriations

Section 320 authorizes funds for the Secret Service as may be necessary to carry out investigations and risk assessments of security breaches under the requirements of subtitle B.

Section 321. Reporting on risk assessment exemptions

Section 321 requires that the Secret Service report to Congress on the number and nature of data security breach notices invoking the risk assessment exemption and the number and nature of data security breaches subject to the national security and law enforcement exemptions.

Section 322. Effective date

Subtitle B takes effect 90 days after the date of enactment of the Personal Data Privacy and Security Act.

TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

Section 401. General Services Administration review of government contracts

Section 401 requires the General Services Administration (GSA), when issuing contracts for more than $500,000, to review and consider Government contractors' programs for securing the privacy and security of personally identifiable information, contractors' compliance with such programs, and any data security breaches of contractors' systems and the responses to those breaches.

In addition, GSA is required to include penalties in contracts involving personally identifiable information for (1) failure to comply

with subtitle A (Data Privacy and Security Programs) and subtitle B (Security Breach Notification) of title III of this Act; and (2) knowingly providing inaccurate information. Section 401 also requires that GSA include a contract requirement that Government contractors exercise due diligence in selecting service providers that handle personally identifiable information and that Government contractors take reasonable steps to select service providers that maintain appropriate data privacy and security safeguards.

Section 402. Requirement to audit information security practices of contractors and third party business entities

Section 402 amends 44 § U.S.C. 3544 to require that Federal agencies audit and evaluate the information security practices of Government contractors and third parties that support the information technology systems of Government agencies.

Section 403. Privacy impact assessment of Government use of commercial information services containing personally identifiable information

Section 403(a) updates the E-Government Act of 2002 to require Federal departments and agencies that purchase or subscribe to personally identifiable information from a commercial entity, to conduct privacy impact assessments on the use of those services. In addition, section 403(b) requires Federal departments and agencies that use such services to publish a description of the database, the name of the provider and the contract amount.

Section 403 also requires that Federal departments and agencies adopt regulations that specify the personnel allowed to access Government databases containing personally identifiable information and the standards for ensuring, among other things, the legitimate Government use of such information, the retention and disclosure of such information, and the accuracy, relevance, completeness and timeliness of such information. Section 403 further provides that Federal departments and agencies must include in contracts for more than $500,000 and agreements with commercial data services, penalty provisions for circumstances where a data broker delivers personally identifiable information that it knows to be inaccurate, or has been informed is inaccurate and is in fact inaccurate. Section 403(c) also requires that data brokers that engage service providers, who are not subject to the data security program requirements of the bill, exercise due diligence in retaining these service providers to ensure that adequate safeguards for personally identifiable information are in place.

Section 403(d) directs the Government Accountability Office to conduct a follow-up study and report to Congress on Federal agency use of commercial databases, including the impact of such use on privacy and security, sufficiency of privacy and security protections, and the extent to which commercial data providers are penalized for privacy and security failures.

Section 404. Implementation of Chief Privacy Officer requirements

Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 requires each agency to create a Chief Privacy Officer. Section 404 facilitates the efficient and effective implementation of this requirement

by directing the Department of Justice to implement this provision by designating a Department-wide Chief Privacy Officer, whose primary role is to fulfill the duties and responsibilities of Chief Privacy Officer. In addition, the DOJ Chief Privacy Officer will report directly to the Deputy Attorney General.

Section 404 also stipulates responsibilities for the DOJ Chief Privacy Officer that are tailored to the mission of the Department and the requirements of this Act. Specifically, this section directs the Chief Privacy Officer to: (1) oversee DOJ's implementation of the privacy impact assessment requirement under section 402; (2) promote the use of law enforcement technologies that sustain, rather than erode, privacy protections and ensure that technologies relating to the use, collection and disclosure of personally identifiable information preserve privacy and security; and (3) coordinate implementation with the Privacy and Civil Liberties Oversight Board, established in the Intelligence Reform and Terrorism Prevention Act of 2004.

IV. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

The Committee sets forth, with respect to the bill, S. 1490, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

DECEMBER 2, 2009.

Hon. PATRICK J. LEAHY,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 1490, the Personal Data Privacy and Security Act of 2009.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

S. 1490—Personal Data Privacy and Security Act of 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 Serv-

ices 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 individ-

uals' 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.

V. Regulatory Impact Evaluation

In compliance with Rule XXVI of the Standing Rules of the Senate, the Committee finds that no significant regulatory impact will result from the enactment of S. 1490.

VI. Conclusion

The Personal Data Privacy and Security Act of 2009, S. 1490, provides greatly needed privacy protections to American consumers

and businesses, to ensure that all Americans have the tools necessary to protect themselves from identity theft and other data security risks. This legislation will also ensure that the most effective mechanisms and technologies for dealing with the underlying problem of lax data security are implemented by the Nation's businesses to help prevent data breaches from occurring in the first place. The passage and enactment of this important privacy legislation is long overdue.

VII. MINORITY VIEWS FROM SENATORS SESSIONS AND KYL

This legislation deals with two issues about which there is bipartisan agreement on the need for congressional action: data security and identity theft. We fully support the goals behind the provisions on this legislation dealing with notice to law enforcement and to consumers in the event of a data breach. Such notice provides law enforcement with valuable information on how to fight data and identity theft crimes which have exploded in recent years, and which are now increasingly committed by sophisticated criminal enterprises with global reach. Timely notice of genuine threats to individuals' identity information also gives consumers the ability to protect themselves. We believe, however, that notice to consumers must occur after an intelligent assessment of the risk a breach poses to consumers. Requiring notice for trivial security breaches will cause consumers to be inundated by inconsequential warnings, and if consumers find themselves overwhelmed by trivial notices, they will be more likely to ignore warnings that matter—when their identity information is genuinely at risk. Such a notice regime would not help consumers, but will affirmatively harm them.

While we commend the Chairman's efforts in this area, we unfortunately cannot support S. 1490 because we believe that it will be counterproductive to our shared goal of consumer protection, and because we fear that it strays far afield from the core objective of protecting consumers whose information has been compromised. S. 1490 seeks to impose new regulations not only on "Data Brokers"—a class of businesses defined so broadly as to ensnare companies not engaged in the data broker business—but also on any entity or person that merely uses information obtained from commercial data sources. The regulations proposed in this bill will confuse consumers and businesses alike, and eventually harm the economy at large.

BACKGROUND

Identity theft is a major concern for consumers and for businesses, and the threat from increasingly sophisticated criminal enterprises is both serious and growing. Both business and government have spent a great deal of time and effort to understand and combat this crime. Law enforcement at the federal, state and local levels have increased their cooperation, and businesses have adopted more rigorous internal controls to protect their customers' information. During the last Administration, the President's Identity Theft Task Force issued a report in April 2007 after 10 months of study, showing that the business community had spent billions of dollars enhancing data security, building better ways to detect and stop fraud and identity theft before it occurs, and working with victims.

State governments have also become very active in this area. Already 45 states and the District of Columbia have enacted laws to combat identity theft and to require businesses who are victimized by a data breach to contact consumers and inform them of the risk to their sensitive personal identity information. There are significant differences across the various state laws, however, and so a Federal response—to provide consistency and predictability which will promote interstate commerce—is clearly necessary.

Our first priority must be to ensure that consumers have the tools to protect themselves in the event of a data breach. Americans need to be notified when information pertaining to them is compromised in a way that may jeopardize their identities. For such notices to be effective, however, they must be issued only when there are reasonable grounds to do so. We know from the experience of the Gramm-Leach-Bliley Act (GLBA) that over-notification leads to consumer apathy, with the result that consumers are exposed to greater risks.

SPECIFIC CONCERNS WITH S. 1490, THE PERSONAL DATA PRIVACY AND SECURITY ACT

Though we support many of the stated goals of this legislation, we have several specific concerns with S. 1490 as reported by the Committee.

1. The Notice provisions will likely result in over-notification to consumers of data breaches

The bill sets a default rule that consumers must be notified of any breach "following the discovery" of a breach. It then provides a "safe harbor" that excuses companies from that obligation if the company conducts a risk assessment and concludes that the breach does not bear a reasonable risk of "harm" to the consumer. The term "harm" is potentially very broad, and the bill does not define it. Although supporters of the bill have been repeatedly asked what "harm" would cover, they have never provided a clear answer. In the face of such ambiguity, and in the face of the severe consequences for failure to issue notices when required, businesses are likely to minimize their legal risk by simply notifying consumers even of minor non-threatening breaches. Such defensive behavior, however rational from the perspective of the business victimized by a data breach, will almost certainly dull consumers' sensitivity to breach notices and leave them at greater risk than they face in the absence of federal legislation.

2. The scope of protected information is over-broad, and will contribute to over-notification

The bill also defines the protected class of information—"sensitive personally identifiable information"—to include widely available information that is not sufficient to pose a risk of identity theft. But the bill's notice and "safe harbor" provisions would be triggered even where the data breach only revealed such relatively innocuous information.

3. The definition of Security Breach is over-broad

The bill defines a breach as including unauthorized "access" or "acquisition" of sensitive personally identifiable information. While "access" to such information is a common term used in the criminal code, its use alongside "acquisition" implies that "access" refers only to instances where the personal data is not "acquired"—i.e. where the data is not in some way recorded, collected, or taken for future, potentially harmful, use. Thus, the current definition of a "breach" would appear to cover instances where information is viewed in passing, or possibly where a person obtains unauthorized access to a computer system that contains personal information, even if the invader never views or downloads the information. Such activity, however, does not threaten individuals whose data was "accessed" with any harm.

The problems posed by this definition may be reduced in part by the new proviso added to the definition of a "security breach" in committee, which limits the definition of a breach to incidents "which present a significant risk of harm or fraud to any individual." That language, however, leads to different problems.

One of the most valuable aspects of S. 1490 is the requirement for companies who suffer data breaches to report those incidents to law enforcement. That reporting requirement will assist our law enforcement agencies to better analyze and defend against the methods of increasingly sophisticated and global criminal enterprises that commonly engage in data theft. In order to avoid desensitizing the public through over-notification of such breaches, however, any legislation in this area should include a clear risk-based standard for requiring companies to take the additional step of notifying individual consumers who might have been affected by the breach.

Inserting the "significant risk of harm or fraud" test in the definition of a "security breach," however, places the threshold too early in the process. This language also places the determination of whether there is a "substantial risk," and thus, the applicability of the entire breach notice regime, largely within the discretion of the business that experienced the data breach. While S. 1490 imposes severe penalties on companies who refuse to provide appropriate notice to consumers, the inclusion of a "significant risk" test in the definition of a "breach" dramatically increases the risk that a company might incorrectly conclude that the attack it suffered did not meet the statutory definition of a "security breach" and thus fail to notify or seek the views of law enforcement.

4. The legislation should specifically and completely exempt entities regulated by other federal laws from the provisions of this Act

Consumer reporting agencies (CRAs) are already fully regulated under requirements under the Fair Credit Reporting Act (FCRA), and financial institutions are regulated under the Gramm-Leach-Bliley Act. Companies that are already regulated under the FCRA and Gramm-Leach-Bliley (GLB) should be specifically exempt from this Act, and from the definition of "data broker" because they are already subject to rigorous data safeguard requirements under these statutes.

The Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) is a time-tested statute that has received frequent and thoughtful review by Congress, and was most recently updated in 2003, with extensive changes implemented by the FACT Act (Pub. L. 108–159).[1]

The requirements laid out in this legislation would create a host of conflicting, inconsistent, unworkable and potentially negative impacts on FCRA-regulated entities, and could have significant negative effects on consumers.

Further, assuming that it was the Committee's intent to exempt FCRA and GLB covered entities from the scope of some provisions of this Act, the exemption crafted by the Committee is incomplete, and would in many cases subject FCRA regulated entities to duplicative and conflicting standards. Rather than having the Judiciary Committee attempt to craft those exemptions, we should defer to the Banking Committee, which has the expertise to determine that the exemptions are as complete as intended.

5. Other issues

In addition to these flaws, S. 1490 also contains unnecessary provisions that might be politically attractive to their advocates but which do not ultimately serve the interests of the consumers we are pledged to protect.

The data broker regulations in Title II of S. 1490 are the best example of the "bloat" that afflicts this bill. Notwithstanding the exemptions incorporated into this title, the bill's definition of "data broker" is far too broad and runs the risk of covering a range of entities—including on-line payment or banking service providers—that are not engaged in a business that fits the common understanding of what constitutes a "data broker."

Title II also attempts to treat data broker services as analogous to credit reporting services, while overlooking the fact that the uses of these databases—e.g., for authenticating identity and fraud prevention, as well as for things such as locating deadbeat parents—is very different from the predominant use of credit report data as a financial transactions tool. For example, Title II contains a vague and potentially wide-ranging notice obligation by any person or entity who takes "adverse action" against an individual based in whole or in part on information obtained from a data broker. Yet "adverse action" is never defined, and the potential reach of this obligation is enormous. In addition, Title II creates a reach-through right for any consumer to contest information held by a data broker by being referred to the source of the information, including any commercial business with which the individual has a transaction history. Such a requirement would impose enormous costs on the U.S. economy, in exchange for little protection gained for the individual consumer.

Title IV of S. 1490 is also problematic, since it would require federal agencies that use data broker services to publish privacy impact notices in the Federal Register. Not only does this take an obligation that attaches to records in government's own control and attach it to privately held data which the government reviews

[1] That Act contained a number of significant provisions designed to protect consumers and combat identity theft, and I again complement Senator Shelby for his work on that legislation as the then—Chairman of the Senate Banking Committee.

under contract, but the privacy impact analysis language in the bill contains no exception for law enforcement or counterterrorism uses of the data broker's services. According to a 2005 GAO audit, 91% of government use of data broker services was for these two types of activities, and publication of details about the government's data use (e.g. for security investigations or other sensitive activities) could hamper these critical functions.

CONCLUSION

For these reasons, we dissent from the views and policy represented by S.1490, and we would urge our colleagues to revisit many of the policy and drafting problems created by this bill.

JEFF SESSIONS.
JON KYL.

VIII. CHANGES TO EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of Rule XXVI of the Standing Rules of the Senate, the Committee finds that it is necessary to dispense with the requirement of paragraph 12 to expedite the business of the Senate.