

Law Office of
RICHARD P. GOLDBERG

Attorney at Law
Washington, D.C.

202-656-5774
www.GoldbergLawDC.com

Briefing: Senate Considers the Personal Data Privacy and Security Act of 2009

September 3, 2009

By Richard P. Goldberg

On July 22, 2009, Senator Patrick Leahy (D-VT) introduced Senate Bill 1490, the Personal Data Privacy and Security Act of 2009 (the “Act”). The stated purpose of the Act is “[t]o prevent and mitigate identity theft, to ensure privacy, 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.”¹

Although Senator Leahy has introduced similar legislation twice in the past without success, recent large-scale security breaches may speed passage of the bill this time. If signed into law, the Act could have implications for companies that hold sensitive personally identifiable information and for security professionals charged with protecting that data or auditing how such data is protected. The Act would also impose new requirements on government contractors, who could face audits of their procedures for protecting personally identifiable information.

This briefing summarizes the key sections of the Act that may apply to your business. It is not legal advice and is not a substitute for legal advice.

I. Overview

In general, the Act would do the following: (1) require entities that maintain personal data to establish internal policies to protect that data and to give notice both to individuals and to law enforcement when they experience a security breach involving sensitive data; (2) give individuals the right to examine and correct personal information held by so-called “data brokers”; (3) impose civil penalties on data brokers who violate the provisions of the Act; (4) make it a federal crime to intentionally or willfully conceal the fact of a security breach that involves personal data; and (5) impose requirements that government agencies audit their information security controls regarding personally identifiable information, perform privacy impact assessments on the impact of potential data breaches, and require that their private contractors adhere to the objectives and requirements of the Act.

¹ S. 1490, 111th Cong. (2009), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s1490is.txt.pdf.

RICHARD P. GOLDBERG

Attorney at Law

II. Who and What the Act Covers

A. Covered Entities, Data Brokers, and Government Contractors

The provisions of the Act would principally apply to three types of business entities: (1) “covered entities,” which would include any business that engages in interstate commerce that involves “collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form” of 10,000 or more people; (2) data brokers, who, in exchange for fees, collect, transmit, or provide access to sensitive personally identifiable information of more than 5,000 individuals *who are not customers*; and (3) government contractors. A business may fall into more than one of these classifications. However, the Act does not apply to businesses already covered by the Gramm-Leach-Bliley Act,² such as banks, or those already covered by HIPAA,³ such as doctors and hospitals, nor do many of its protections apply to the government.⁴

B. Sensitive Personally Identifiable Information

The Act defines “sensitive personally identifiable information” broadly, such that it encompasses any electronically stored information that includes an individual’s last and first name *or* an individual’s last name and first *initial* plus *any* of the following: (1) a financial account, credit, or debit card number in combination with any security code, access code, or password required to access funds; (2) a non-truncated social security number, driver’s license number, passport number, or alien registration number; (3) any two of (i) a home address or telephone number, (ii) a mother’s maiden name (identified as such), or (iii) a full birth date; (4) unique biometric data such as a fingerprint, “voice print,” retina or iris image, or any other unique physical representation; or (5) a unique account identifier, electronic identification number, user name, or routing code, in combination with an associated security code, access code, or password required to obtain any thing of value. It should be clear that the extent of data collection can be seemingly minimal and still be covered by the Act.

C. Security Breaches

The Act also defines a “security breach” broadly to include not only evidence of an actual breach, but merely the existence of a “reasonable basis to conclude [a compromise of security] has resulted in, acquisition of or access to sensitive personally identifiable information that is unauthorized or in excess of authorization.”⁵ This expansive definition could mean that a successful attempt to breach a system’s security that only left hackers with *access* to sensitive personally identifiable information, even if only some evidence exists of that access, would be

² 15 U.S.C. § 6801-6809 (1999).

³ The Health Insurance Portability and Accountability Act, 42 USC § 201 *et seq.* (1996).

⁴ S. 1490 at § 3.

⁵ *Id.* at § 3(11)(A).

RICHARD P. GOLDBERG

Attorney at Law

considered, for the purposes of the Act, a “security breach,” which would bring to bear the Act’s notification and civil and criminal penalties.

III. Preventative Measures, Penalties, and Notice Requirements for Covered Entities and Data Brokers

A. Requirements for Covered Entities

Every covered entity would be required to create a “data privacy and security program” that would include “administrative, technical, and physical safeguards appropriate to the size and complexity” of the business.⁶ This program would need to protect against both unauthorized access and anticipated vulnerabilities.⁷ Businesses would also be required to perform risk assessments to identify such vulnerabilities and assess the likelihood of potential damage from security breaches, as well as to continue to review policies to assess the success of their programs. They would also be required to perform periodic vulnerability testing.⁸

As a preventative measure, businesses would be required to adopt measures to detect both actual and attempted fraudulent, illegal, or unauthorized access. They would also be required to use encryption, redaction, access controls, and proper disposal of information. Use of access logs would be required to trace access to records to ensure that such access was authorized. Finally, businesses would be required to perform sufficient due diligence to ensure that any third-party customer that would acquire or have access to their information would only use the information for a “valid legal purpose.”⁹ The Act does not impose penalties to the originators of data if third parties subsequently use that data improperly.

B. Additional Requirements for Data Brokers

The Act would additionally require 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 “specifically for disclosure to third parties.” It would also require data brokers to create processes for individuals to dispute and correct inaccuracies in their *own* records.¹⁰

Notably, the Act would not require procedures to correct information that incorrectly identifies an individual as a part of another individual’s record. For instance, if a record sufficiently identified “George Washington” (*e.g.*, with a first and last name), and then identified

⁶ *Id.* at § 302.

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.* at § 201.

RICHARD P. GOLDBERG

Attorney at Law

his wife “M. Washington,” but did not sufficiently identify her further with the details required by the Act, any incorrect information about M. Washington, for instance that she was a convicted violent felon and known gambler, could only be corrected by George. Under the Act as written, Martha would have no rights to correct it. This would still apparently be true if Martha’s record identified George as her husband. Moreover, without examining George’s record, Martha might never know that this incorrect information existed and was being spread throughout the commercial data-broker system, resulting in credit problems and potentially problems with prospective landlords and employers. If George and Martha were divorced or separated and not on speaking terms, Martha might have no ability at all to correct the information or even learn about it.

C. Penalties for Data Brokers

A data broker that violates these provisions is subject to a penalty of \$1,000 per violation per day, to a maximum of \$250,000. A data broker that intentionally or willfully violates these provisions is subject to an additional penalty of \$1,000 per violation per day, to a maximum of an additional \$250,000. Thus, the theoretical maximum statutory fine—for intentional violations that last 36 weeks—would be \$500,000.¹¹

From the text of the Act, it is not clear whether this maximum is to be calculated per incident or per person. It is likely, however, that the limit is intended to be calculated per incident. If it were calculated per person, the maximum fine could begin (assuming a minimum of 5,000 records) at \$2.5 billion. For large data brokers that generate millions in fees, a single data breach, resulting from unintentional acts, would result in a mere \$250,000 fine. If the cost of adequate security to prevent such breaches were even to approach that cost, the statutory fines for periodic security breaches could be considered the cost of doing business, resulting in little privacy protection for individuals.

Additionally, the Act explicitly provides that nothing in the section on data brokers creates a private right of action that would allow an individual to sue. Enforcement would be left to federal and state authorities.¹²

D. Requirements for Notice to Individuals

A covered entity that experiences a data breach would be required to notify all individuals affected by the breach after only a “reasonable delay,” which would allow the company first to investigate the scope of the breach, prevent further disclosures, and to “restore the reasonable integrity of the data system and, when required, to provide notice to law enforcement.”¹³ The Act would also require that *any person or company*—not just a data broker—who takes an adverse action based upon data received from a data broker provide notice

¹¹ *Id.* at § 202.

¹² *Id.* at § 303(d).

¹³ *Id.* at § 311.

RICHARD P. GOLDBERG

Attorney at Law

to the person affected by the adverse action, as well as contact information for the data broker, the content of the information received, and information regarding correcting inaccuracies in the information.

The Act also provides exceptions to the notice requirements in the event disclosure would hinder law enforcement or cause damage to national security.¹⁴ And unlike other recent government requirements,¹⁵ this provision would not require that the company notify the public.

E. Criminal Penalties for Failure to Report a Breach

The Act makes it a federal crime for a person who knows of a security breach, and knows of the obligation to provide notice to individuals, to intentionally and willfully conceal the security breach. Violation of the criminal portion of the act could result in a fine and up to five years imprisonment.¹⁶ Unlike the civil penalties, it is clear that the criminal penalties would not be measured per individual but per breach that affects one or more individuals.

IV. Audit and Security Requirements for Government Agencies, Contractors, and Subcontractors

A. Requirements for Agencies Regarding Government Contractors and Subcontractors

The Act would amend the law that currently requires federal agencies to audit their information security controls to add a requirement for personally identifiable information. The current law¹⁷ provides a framework for ensuring the federal government maintains effective information security controls. The Act would require new procedures for evaluating and auditing the security practices of government contractors and third-party business entities (for contracts of over \$500,000) that “support[] the information systems or operations of the agency involving personally identifiable information” and would require remedial action to address significant deficiencies.¹⁸

The Act would also require any federal agency that intends to contract with a commercial data broker to perform a “privacy impact assessment.”¹⁹ The Act also provides standards for such an assessment to ensure the information is collected and retained only for a “legitimate

¹⁴ *Id.* at § 312(a).

¹⁵ *See e.g.*, American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5.

¹⁶ *Id.* at § 102.

¹⁷ 44 U.S.C. 3544.

¹⁸ *Id.* at § 402.

¹⁹ 44 U.S.C. § 3501 (the E-Government Act of 2002).

RICHARD P. GOLDBERG

Attorney at Law

purpose,” to limit retention and re-disclosure of the information, and to ensure the data is accurate, relevant, complete, and not out of date. Each assessment would also be required to include standards for auditing the data to prevent “unauthorized access, analysis, use, or modification” of the data and procedures for individuals to “secure timely redress for any adverse consequences wrongly incurred due to such a breach.”²⁰

The Act incorporates into each government contract worth \$500,000 or more a requirement that contracts with subcontractors and data brokers contain provisions that require such subcontractors implement and maintain measures designed to meet the “objectives and requirements” of the Act. The Act also incorporates its penalties into each government contract for entities that know or have reason to know that personally identifiable information being provided to the federal government is inaccurate.²¹

These audit and security requirements could create an additional cost-of-doing-business for government contractors and subcontractors. It could also create a new niche for security professionals capable of conducting the audits required to assure contractors are in compliance or to bring them into compliance.

B. Designation of Chief Privacy Officers

The Act would require that each government agency designate a Chief Privacy Officer to oversee implementation of the Act. It would also require that the Department of Justice to designate a department-wide Chief Privacy Officer to oversee implementation of the Act. The DOJ Chief Privacy Officer, who would report directly to the Deputy Attorney General, would additionally be responsible for overseeing conduct of privacy impact assessments of use by the DOJ of commercial data containing personally identifiable information.

V. Conclusion

With large-scale data breaches on the rise, and electronic medical records becoming a reality, the time for this legislation may have come. As currently written, the Act could have implications for companies that hold personally identifiable information, for security professionals charged with protecting that information or auditing how it is maintained, and for government contractors, who may face audits.

If you would like to discuss how the Personal Data Privacy and Security Act could affect your business, whether through increased security precautions or increased auditing, or if you would like to discuss any other issues in information security and data privacy, please do not hesitate to contact me.

Attorney Advertising: These materials have been prepared for general informational purposes only and are not intended as legal advice.

²⁰ S. 1490 at § 403.

²¹ *Id.*