

Data Protection, the Next Big Thing from the Feds?

Over the past several years, greater attention has been paid to issues related to protection of sensitive consumer data collected by businesses, government and other organizations as more consumers utilize the Internet for a host of personal and business transactions. High profile news reports of theft of millions of credit card numbers, social security numbers or other personal data are not uncommon. In fact, fear of identity theft has led to the emergence of data protection companies like Lifelock, which claim to protect consumers from identify theft.

State and federal government agencies and legislatures are increasingly debating the value of regulating how such personal data (referred to as Personally Identifiable Information or PII) is collected and handled, and what consumer notices are required in the event of a data breach. Generally, not all data is protected under such regulations.

Typically, PII is defined as:

- A person's name when used in conjunction with:
 - Social security numbers.
 - Driver's license numbers or state identification card numbers.
 - Account numbers such as credit or debit card numbers (where such numbers can be used without additional identifying information, access of pass codes).
 - Account passwords, other personal identification numbers or access codes.

California was one of the first states to take action to protect consumer data. In 2003, the state passed Senate Bill 1386, which requires that anyone doing business with California residents must disclose any security breach of unencrypted, personally identifiable information that was, or is reasonably believed to have been, viewed or acquired by an unauthorized person. However, the law is extremely limited in its application and only applies to a person's first and last name when combined with a social security number, a driver's license number or a password and financial account. Though several organizations, including major public universities, have had to notify consumers or employees, to date, there have been no cases tested in court.

Massachusetts is the most recent state to pass a consumer data privacy law. In Massachusetts, companies must limit the amount of data they collect and maintain a written security policy, in addition to maintaining a detailed inventory of data that has been collected and how it is stored. The Massachusetts Law also requires that businesses that handle sensitive personal data, as defined by the act, encrypt the data when it is transmitted over the Internet or stored on a mobile storage device such as a laptop, thumb drive or external hard drive.

In all, [46 States](#) have passed some form of data protection laws. While the requirements of these laws vary, in most cases, such laws require notification of consumers of data security breaches that involve their PII.

Federal Legislation/Regulations

In 2009, two bills were introduced in Congress related to the protection of consumer data—[House Bill 2221](#) (H.R.2221) and [Senate Bill 1490](#) (S.1490). Both bills would preempt state law on consumer data, thus establishing uniform requirements nationwide. Both bills were introduced in 2009 and H.R.2221 was [heard](#) in the House Energy and Commerce Committee and passed the House. It was sent to the Senate in April of 2009. Senate Bill 1490 was reported out of its Senate Committee and sent to the Senate floor, but there is no record of a vote. Both bills were opposed by affected industries and their trade organizations.

Both H.R.2221 and S.1490 would create a regulatory regime to regulate the collection and storage of consumer PII. Both would empower the Federal Trade Commission to regulate such data. As H.R.2221 was referred to the Senate, and is similar to S.1490, the outline of the bill's requirements will focus on the S. 1490.

Senate Bill 1490

Bill Status

Senate Bill 1490 is titled the Personal Data Privacy and Security Act of 2009. It was introduced in the 111th Congress by Senator Leahy (CT) and referred to the Senate Judiciary Committee. Other than additional comments filed by Senator Leahy, the bill has not been the subject of Senate action.

Summary of Bill Requirements

The Personal Data Privacy and Security Act of 2009 addresses issues of data privacy in three substantive areas. First, it creates a set of federal crimes and penalties for violation of the regulations adopted by the act. Second, it creates a nationwide set of regulations for Data Brokers¹. Third, it would create a set of federal regulations to govern the collection of and protection of consumer PII and it would also create a set of regulations governing notification of consumers for security breaches involving PII.

¹ Data Brokers are defined as entities primarily engaged in the collection of personal data of more than 5,000 individuals for a fee and transmission of that data through interstate commerce to third parties.

Privacy & Security of Personally Identifiable Information

As noted, Title III of [S.1490](#) would create laws and regulations to govern the collection of PII and set requirements for protection of such data.

The act would apply to business entities that are engaged in interstate commerce and collect personal identifiable information in electronic or digital form for 10,000 or more persons in the United States. Companies that fall under this definition (save for exempt financial institutions and entities covered by HIPPA) must comply with the data protection provisions of the act.

The bill would require that the entity enact a comprehensive personal data privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the business entity and the nature of its activities.

Such security programs would be designed to ensure the privacy, security and confidentiality of PII data (as defined in the legislation), protect against any anticipated vulnerabilities and protect against unauthorized access to such information.

The business entity must also identify reasonably foreseeable internal and external vulnerabilities that could result in unauthorized access of PII, assess the likelihood of damage or alteration of that data, assess the effectiveness of the entities internal controls and assess the vulnerability of the data when it is scheduled to be destroyed.

The act would also require covered entities to design personal data privacy and security programs to control risks to such data, adopt measures commensurate with the sensitivity of the data as well as the size of the entity and its activities. Such measures need to take into account protections for the entire lifecycle of the covered data, and need to include provisions addressing access to systems, means to detect attempted infiltration/ unauthorized access to such data and, finally, to protect such data. The data protections must include policies to address the use, transmission and storage of such data. It must also protect sensitive personally identifiable information during use, transmission, storage, and disposal by encryption, redaction or access controls that are widely accepted as an effective industry practice or industry standard, or other reasonable means— including policies and procedures as directed for disposal of records under section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w) and the implementing regulations of such Act as set forth in section 682 of title 16, Code of Federal Regulations.

Entities must ensure employees are trained in the policies adopted to comply with this act and must undertake regular testing of its protection measures.

These requirements would become effective one year from passage of the bill.

Regulatory Commonalities and Looking Ahead

Current federal legislative proposals appear to be focused on creating a federal regulatory regime to standardize protection of PII, which is presently governed by a mish-mash of 46 state or local laws. As noted, both S.1490 and H.R.2221 have not seen significant action in Congress since late 2009 when they were originally introduced. At present, they do not appear to possess enough political momentum for passage in the near term.

Additionally, there is talk at the Senate staff level of a third approach to regulating PII. While no official bill has been introduced, a Senate discussion draft has emerged which would impose a lower set of requirements and focus its data protection efforts on data collected by websites and other electronic interfaces. What this says is that consensus has yet to emerge on this issue and, as such, it would be unusual if any bill would pass in the near term on this topic.

That said, by looking at the current discussion drafts, some predictions can be made as to what type of regulatory regime will emerge as these different approaches are harmonized by looking at areas of conceptual agreement between the existing and discussed approaches. Additionally, protections required by the pending, but long delayed, FTC Red Flags Rule provides further hints as to areas of government concern. Together, these future regulations would likely include:

- 1) Empowering the FTC to regulate and enforce any federal regulations and laws on PII.
- 2) Establishing a threshold of collecting 10,000 or more records before a business entity would be required to comply with PII regulations.
- 3) A requirement that entities develop policies and programs to protect PII data, educate employees, assess potential risks, and protect PII data throughout its lifecycle that *may* include encryption, redaction or access controls.

Conclusions

Regulation of consumer PII continues to evolve. At present, the regulatory environment is characterized by a wide array of state-based regulations with a handful of federal requirements. Pending regulations such as the FTC Red Flags Rule and introduced legislation demonstrate that this regulatory trend is moving increasingly to the federal level. Much of the current requirements involve companies adopting written policies and plans for the collection and protection of the PII data along with employee education and system testing. While the variable approach by states makes it likely that federal regulations will emerge to standardize such protections, it is difficult to say when such action will occur.

Based on recent actions in 2009, it is possible that enactment of currently pending bills or new legislation could happen within the year. However, looking at the implementation of

state laws and the pending FTC Red Flags Rule, such regulation, especially as a matter of first impression, make action by the end of 2010 possible, but unlikely. A more probable outcome is the adoption of federal data protection requirements in 2011 or beyond. In the long term, the need for uniformity in data protection laws makes adoption of some type of federal regime extremely likely. The situation at present remains fluid but is worth watching by CAI and its members.