

THE
NEW ENGLAND
COUNCIL

NEW ENGLAND COUNCIL DATA SECURITY BREACH PRINCIPLES
APRIL 2006

There is a growing concern among consumers, businesses, policymakers and privacy advocates about the theft of personal information and the loss of sensitive data files containing confidential information. A CBS News/New York Times Poll in September 2005 reported that nearly nine in 10 Americans are concerned about identity theft, with more than half saying they are “very concerned.”

The New England Council, the nation’s oldest regional business organization, believes it is now time that Congress adopt legislation that provides a uniform national data breach standard. Currently, only three of New England’s six states have adopted data breach laws and a national framework is needed to protect all New England consumers and to provide guidance for organizations that use personal information. This legislation must preempt the patchwork of state laws that have developed over the last few years. These state laws have required entities to undertake complex and potentially inconsistent activities in various states in the event of a data breach and have delayed notice to the consumer in the event of a breach.

In crafting this law, Congress should recognize that a data breach law will affect a range of industries in various business sectors as well as the non-profit world. The law must adequately protect the consumer but also must ensure that organizations are not required to take unnecessary or counter-productive steps to comply with its requirements.

In the winter of 2001, the New England Council issued a Statement of Principles on Internet, Health and Financial Privacy. The Principles noted that inconsistent state laws on data privacy are more detrimental in New England where six states share a small geographic area and business activities are more likely to cross state borders. These Principles also noted that privacy laws directly impact three core industries in New England – health care, technology and financial services. As in 2001, these industries continue to form the backbone of the region’s economy and New England is dependent on them for its continued economic growth.

These principles have been developed based on input from New England Council members representing a variety of different industries that would be affected by a federal data security breach law, including the health care, technology, financial services, legal and educational sectors.

I. Federal Data Security Breach Legislation Should Preempt State and Local Law.

With the rise of electronic communications, it has become considerably easier, cheaper and quicker to send information across state borders. Information is exchanged on a daily basis by millions through a single keystroke and state borders play almost no role in these exchanges. In short, there is a strong public policy rationale for a federal data breach standard that creates a "ceiling" where states cannot impose additional requirements.

At least 21 states including Connecticut, Maine and Rhode Island and one municipality -- New York City -- have adopted data breach security laws. These various and sometimes conflicting local laws can cause significant harm. First, the proliferation of local laws results in delay in notice to the consumer in the event of a breach as organizations determine the requirements of the laws in the various states and municipalities that may have been implicated. It is undisputed that prompt notification to consumers is crucial and the various local laws are hampering this prompt notification.

The varying state laws may also lead to over-notification. Organizations that operate on a nationwide basis cannot efficiently develop data breach notification compliance plans in different states. Such organizations develop a compliance plan that complies with the most onerous state laws even if it results in sending more notices than required in the majority of other states. Accordingly, the state legislators passing the most onerous state laws are dictating the law for the rest of country.

Furthermore, the overabundance of state laws could also interfere with law enforcement investigations. If state laws do not contain notice delay provisions for law enforcement purposes, organizations may be required to provide notice even if it is in the best interest of law enforcement that notification is delayed.

Finally, these varying state laws have the potential to stifle e-commerce. Small businesses and non-profit organization are forced to spend needlessly to understand and comply with the various local laws in the event of a breach or to be prepared in case of a breach. These various local laws are creating a high barrier of entry into the e-commerce arena for small organizations.

Because of these harms, the Council urges Congress to act quickly to pass legislation that results in a uniform national data breach standard that preempts state and local laws.

II. The Breach Standard Should Not Require Over-Notification and the Form of Notification Should be Consistent with Customer Expectations.

It is important that Congress adopt a breach standard that does not require over-notification of consumers. California's law, which became a model for much of the state laws across the nation, has led to over-notification. According to the National Business Coalition on E-Commerce and Privacy, the California Office of Privacy Protection (OPP)

tracked 45 breaches of that state's data breach law that required notification to consumers. Of those 45 breaches, OPP was able to link only one of those breaches to an instance of identity theft.

A breach standard that encourages over-notification will lead consumers to ignore notices and therefore it is important that notification is tied to an actual, actionable threat. The Council urges Congress to adopt a notice standard that requires organizations to notify consumers when there is a significant risk that they might become victims of identity theft. This would protect against over-notification that results from laws that do not properly take into account whether any harm would actually result from a data breach. Moreover, Congress should specify that where the information is protected by encryption or other verified information security practices, no significant risk of harm exists.

In addition, the Council recommends that organizations be provided time to conduct an investigation of potential data breaches and that legislation should provide a safe harbor for organizations if the investigation finds that no actual breach has occurred. Furthermore, legislation should provide less onerous notification requirements if the cost to notify exceeds an extraordinary amount. This provision would protect non-profits and small businesses in New England that could be overwhelmed by notice requirements in the event of a breach.

Similar to the Interagency Guidance interpreting the Gramm-Leach Bliley Act, data breach legislation should provide entities with discretion to provide notice in any manner that a customer can reasonably be expected to receive it. Moreover, legislation should require that the Federal Trade Commission and the functional regulators develop a model notification to give organizations clear direction as to the form of notification.

III. Federal Functional Regulators Should be Given Sole Authority to Promulgate Regulations and No Private Right of Action Should Exist.

The federal functional regulators of the affected industries, including the Federal Trade Commission for those businesses not currently subject to functional regulation, are best suited to promulgate regulations under the law. These regulators can best evaluate the law's relation to the wide range of organizations that have custody over sensitive personal information.

Allowing a private right of action will lead to over-notification and harm New England's small businesses and non-profit organizations. If the law allows for a private right of action, organizations will be forced to notify consumers even if no threat of identity theft exists in order to avoid litigation. Accordingly, the Council urges Congress to specifically prohibit individual rights of action under the law.

IV. The Legislation Should not Supersede Any of the Existing Federal Privacy Laws.

Congress has already enacted several pieces of legislation on data privacy that affect various industries and organizations such as the Gramm-Leach Bliley Act (GLB), the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act and the Family Educational Rights and Privacy Act. Businesses and organizations have spent considerable time and energy undertaking efforts to understand these complex laws and to develop procedures to comply with these laws. Accordingly, while the Council supports a federal security breach law, any new law should not supersede the detailed requirements that have been created by these existing laws. For example, financial services companies are already required to adopt measures to protect data under GLB; compliance with those provisions of GLB should be deemed to satisfy any similar provisions of a data security bill.