National Data Breach Law Rears Its Ugly Head Again

June 3, 2011 - You may think that it's odd for a consumer organization concerned with privacy and identity theft to be against a national data breach notification law. But there has been a lot about the proposals floating around Washington over the past several years to dislike. The newest iteration, straight from the White House, is no exception. While there are a few things about the proposal that are very good - specifically, the definition of "personally identifiable information" - this particular proposal has loopholes so large that you could drive a fleet Mac trucks through them with your eyes closed. And like every other proposal we've reviewed, this one too would prevent any of the states from enforcing tougher laws that they already have on the books.

The new proposal for a national data breach law is coming straight out of the Obama administration's cyber security proposal which was recently submitted to Congress. We might as well get to the good part of the law first. That's the definition of what constitutes personally identifiable information. It reads, " The term â€˜sensitive personally identifiable informationâ€™ means any information or compilation of information, in electronic or digital form that includesâ€”(1) an individualâ€™s first and last name or first initial and last name in combination with any two of the following data elements: (A) Home address or telephone number; (B) Motherâ€™s maiden name; (C) Month, day, and year of birth; (2) A non-truncated social security number, driverâ€™s license number, passport number, or alien registration number or other government-issued unique identification number; (3) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation; (4) A unique account identifier, including a financial account number or credit card or debit card number, electronic identification number, user name, or routing code; or (5) Any combination of the following data elements: (1) An individualâ€™s first and last name or first initial and last name; (B) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; or (C) Any security code, access code, or password, or source code that could be used to generate such codes or passwords."

While this definition is much more comprehensive than virtually all other state laws, even it has a weakness. Its definition specifically covers only data that is stored electronically. That might not be so bad if the states were allowed to enforce their existing data breach laws for non-electronically stored data, but it doesn't appear that they will be allowed. The law specifically prevents the states from enforcing their own data breach laws. Based on that, if you run a business and throw out a bunch of printed forms that contain names, addresses and SSN's, you won't face any legal ramifications at all. No need to notify anyone of a breach of this type.

The proposed legislation also would exempt many businesses. Any business that stores records containing personally identifiable information on less than 10,000 people in a 12 month period would be exempt. Ironically though, for any business that has more than 10,000 people in their database, a breach of just 5,000 records would trigger a requirement for media notification. It's a schizophrenic approach to data breaches.

For several years business organizations have been pushing for a national law. Businesses don't like the fact that 46 states and the District of Columbia have different laws and different notification requirements. And the truth is that there probably should be some standardization to make it easier for businesses to comply. Certainly, they could coordinate their definition of "personally identifiable information" as well as what needs to be contained in notices sent to consumers once a breach has occurred.

Unfortunately, this particular proposal will significantly reduce the protections that consumers in most states now enjoy. Few if any of the data breach laws on the books right now provide exemptions based on the size of the business. And millions of consumers who live in states that require notification when a breach is in something other than electronic form would see those protections vanish.

The White House proposal for data breaches deserves the same fate as every other similar proposal that has come before it. It needs to go away.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter: