Worst Data Breach Law Ever Continues to Advance in Congress

December 10, 2015 â€“ For several years now, Congress has been working on a national standard for data breach notification. And for that same period of time we have been telling our readers that Congress doesnâ€™t know what it is doing. In fact, you have some members of Congress who are open about the fact that they donâ€™t know how to use a computer also writing legislation that will set standards for protecting computer-stored data. More importantly that legislation would usurp stronger state laws in 47 states. What could possibly go wrong?

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

As proof that bad ideas can actually get worse, the House Financial Services Committee has passed the Data Security Act of 2015 on a 46 to 9 vote. This is just the latest, and perhaps the worst, attempt by members of Congress to establish a national standard for data breach notification. The bill is packed full of little gems that demonstrate the technical incompetence and lack of industry knowledge of its authors. Here are just few of them.

The bill usurps all state data breach notification laws. Many states have significantly stronger laws. One of the primary weaknesses in the federal approach is that companies that experience a data breach will now be able to make a determination of whether or not the breach is likely to lead to identity theft. If they come to the conclusion that ID theft isnâ€™t likely, they donâ€™t have to notify consumers. Many of the state laws being replaced do not have this exception.

The bill specifically exempts companies that are regulated by HIPAA. California recently defined healthcare related data as one of the forms of personally identifiable data that triggers the states data breach notification law. When healthcare related data is accidentally released, residents of the state must be notified under the current law. But the federal bill would end this.

The bill codifies certain security protocols that companies must use with stored data. This is a huge mistake. By requiring companies to use certain encryption standards and certain types of access control for data, hackers will be free to develop more advanced methods to access data. But the companies storing that data may not be able to implement new more advanced methods of data protection because doing so would violate the law. Congress isnâ€™t qualified to make technical decisions for data storage.

The bill strips consumers of any meaningful redress in the event of a data breach. In fact, a letter sent to Congress by the Center for Democracy & Technology and 16 other organizations says, â€œwould also eliminate virtually all avenues of redress for consumers. For example, the law in some states currently provides consumers with a private right of action, and enables state attorneys general to seek restitution on behalf of consumers harmed by data breaches. But if this bill

were to pass, state attorneys general would be limited to seeking civil penalties and injunctive relief, even in cases where consumers suffer extensive harm as a result of a breach of highly sensitive information. This would provide harmed consumers with no relief.â€•

The Senate has already passed a similar bill. If the House and the Senate work out a compromise and the bill is passed by both houses of Congress, the President has already said he will sign the bill. If you agree that this legislation would be bad for consumers everywhere, write or call your congressman and your senators. At this point, that may be the only way to stop this legislation from becoming law.
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:

Follow ACCESS