Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

House Data Privacy Bill Makes Strides, But Still Faces Fight

By **Allison Grande**

Law360, New York (March 13, 2015, 9:25 PM ET) -- A draft of a data security and breach notification law floated by House lawmakers Thursday makes strides toward bridging partisan disagreements, but provisions shifting federal oversight of telecoms and excluding only certain health companies could doom the bill to the scrapheap with its predecessors.

The introduction of the draft Data Security and Breach Notification Act comes amid mounting pressure from the White House, businesses and consumer groups for Congress to deliver legislation that would strengthen the framework that protects consumers' data from increasingly prevalent cyberattacks.

While **previous legislative proposals** to require companies to institute reasonable data security requirements and eliminate the patchwork of 47 state breach notification laws have fallen flat, attorneys see promise in the newest bipartisan measure, which was drafted by House Commerce and Energy Committee Vice Chair Marsha Blackburn, R-Tenn., and Rep. Peter Welch, D-Vt.

"The proposal seems to have a good chance of passing in some form, as the recent high profile data breaches have created bipartisanship in Congress," Kaufman Dolowich & Voluck LLP technology services practice vice chair Hsiao "Mark" Mao said. "The current House draft also echoes much of the sentiments proposed by the Obama administration **back in January**, and thus should have the president's backing as well."

In previous congressional sessions, the passage of data privacy legislation was in large part stymied by disputes over whether more stringent state laws should be preempted, where the trigger for notification should be set, and how much power the FTC should be given over data security.

But Thursday's discussion draft takes steps to overcome these hurdles, attorneys say.

"This is a useful step forward on this issue," Wiley Rein LLP privacy practice chair Kirk Nahra said. "It contains a good preemption provision, which would be a deal breaker for industry if not included."

While state enforcers and privacy advocates are still likely to object to the displacement of more stringent state requirements, their objections may be softened by the bill's proposal to

allow state attorneys general to enforce the bill, its preservation of more stringent state common law requirements, and relatively strong reporting requirements that come close to matching what is generally required by existing state laws.

"The bill doesn't strike me as fundamentally different from existing state rules," Colin Zick, co-chair of the privacy and data security practice at Foley Hoag LLP, said. "So that would mean that the reporting requirements at the federal level stay essentially the same, but companies won't have to report to as many places."

Instead of setting the lowest bar possible, the draft federal bill takes a more aggressive higher ground that leaves out few of the most stringent state law requirements, attorneys noted.

Specifically, the legislation sets a national standard that requires companies to maintain "reasonable security measures" that many businesses already have in place for consumer data, and defines personal information as data tied to identity theft or payment fraud, such as Social Security numbers, financial account credentials, biometrics, driver's license numbers and mother's maiden names, although it leaves out log-in credentials that are covered by reporting laws in California and Florida.

"I still think more likely than not we will see Congress pass a federal data breach notification law this year," Shook Hardy & Bacon LLP data security and data privacy practice co-chair Al Saikali said. "Business advocates see the benefit of predictability in a single standard and a more unified method of enforcement, [while] consumer advocates see a higher floor of protection for consumers than in many jurisdictions where the standards are currently lower or nonexistent."

The bill also adopts the suggestion put forth in both the White House proposal to notify consumers of a breach within 30 days, which is also the most stringent time frame required by a state law, although it does make the novel proposal that the reporting clock begin only after the covered entity has taken the necessary measures to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system, rather than at the moment the intrusion is discovered.

"It's a good compromise because it imposes a time limit while allowing entities sufficient time to investigate, which is critical, because having to do an investigation and notify within 30 days is a big challenge," Hunton & Williams LLP global privacy and data security practice head Lisa Sotto said.

But despite the bill's apparent success at finding a middle ground to ease many existing disputes, more unique provisions put forth in the bill are likely to throw up additional hurdles to passage, attorneys say.

For one, in what the authors described as an attempt to achieve "consistency," the bill would give the Federal Trade Commission the authority to regulate not only nonprofits that currently fall outside of its jurisdiction, but also telecommunications, cable and satellite providers.

In order to bestow the latter authority on the FTC, the bill would strip the Federal Communications Commission of its authority under the Communications Act to regulate telecommunications service providers' data security practices.

The debate over which agency should be in charge of enforcing data security for telecoms

heated up last week, when the FCC's enforcement chief revealed that the agency is planning to step up its privacy and security activities while the FTC expressed concerns over new net neutrality rules that would place broadband service providers outside its enforcement net.

"The bill is trying to create the same set of requirements for all entities that are collecting the same type of information," Mayer Brown LLP partner Howard Waltzman said.

Debate is also likely to be sparked over the way the federal bill interacts with the Health Insurance Portability and Accountability Act. While the proposed measure exempts HIPAA-covered entities from the new regulatory regime, it includes no such carve out for their business associates, which are also bound by the requirements of the federal health privacy law.

"I'm very uncomfortable with the exclusion of HIPAA business associates from the exemptions under the proposal, as that will cause considerable confusion and complexity for the health care industry," Nahra said.

Even if the disagreements are ironed out and the bill — which is slated to be considered by the House Commerce Committee Wednesday — achieves what its predecessors could not and finds its way through Congress, attorneys were quick to note that data security and breach notification were only a piece of the equation for improving the nation's cybersecurity posture, which also requires the passage of equally difficult-to-enact measures related to cyberthreat information-sharing and enhancing criminal hacking penalties.

"The bill doesn't for the most part address the larger objective of preventing the occurrence of breaches themselves," Zick said. "So while the measure might make people feel good, it doesn't address the fundamental problem that there are too many breaches."

--Editing by John Quinn and Kelly Duncan.