Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Will New Congress Pass A National Data Protection Law?

By **Joseph Facciponti and Maxwell Thompson** (January 4, 2019, 2:02 PM EST)

Joseph Facciponti

Maxwell Thompson

After years of false starts, there are signs that Congress might be ready to move forward on a national cybersecurity and data protection standard. With new mega-breaches reported with alarming regularity, significant legislative activity in this area among the states and abroad, and a heightened awareness of privacy risks by the American public, the 116th Congress faces an ideal opportunity to pass bipartisan legislation that could safeguard consumer data, provide clear and uniform rules for businesses, and preserve innovation. Yet any new legislation faces significant hurdles, as Congress must resolve a series of sensitive issues regarding the enforcement, scope, and potential preemptive effect of the new federal law.

Lawmakers have narrowed in on data privacy in recent years following a spate of data breach controversies, including the potential theft of the personal information of up to 500 million customers of Marriott,[1] questions about potential misuse of personal data by Facebook, including the purchase of millions of Facebook users' personal data by political consulting firm Cambridge Analytica Ltd.,[2] and the Equifax data breach that resulted in the exposure of over 140 million Americans' sensitive personal information.[3] It should come as no surprise that some surveys indicate that as many as 94 percent of Americans are now "generally concerned about their data" and 69 percent want legislation similar to the European Union's General Data Protection Regulation.[4] With such clear instruction from the American people, legislators certainly feel pressure to act.

However, up until now it has been state legislatures and regulators that have been leading the charge to adopt cybersecurity and data privacy rules. As of 2018, all 50 states plus the District of Columbia have consumer data breach notification laws. More recently, states have been aggressive in implementing data protection standards. For example, in 2017 New York's financial regulator, the New York State Department of Financial Services, introduced cybersecurity regulations for financial services companies, often referred to as "Part 500," setting a new standard for protections required by those entities covered by the regulation.[5] Building off that momentum, South Carolina became the first state to pass the Insurance Data Security Model Law drafted by the National Association of Insurance Commissioners, which was heavily modeled after Part 500.[6] In 2018, California introduced its Consumer Privacy Act, which mandates several GDPR-like requirements for a large swath of businesses operating in California or collecting the information of California residents.[7] Vermont has also stepped out on its own, enacting the nation's first data broker legislation, regulating those companies that buy and sell personal information.[8]

These are just a few examples of states taking the lead on data privacy and cybersecurity, and while we should applaud these states for moving quickly to address an issue that is of clear concern to many Americans, these developments nonetheless beg the question of whether a clear, national standard is the better path forward, rather than the developing patchwork of state data privacy regimes.

Some members of Congress are ahead of the curve, realizing the urgency in protecting such sensitive information and pressing ahead with legislative proposals. Indeed, Sen. Ron Wyden, D-Ore., recently proposed legislation[9] that would, among other things, impose GDPR-like fines on businesses and potential criminal liability on senior executives for failing to protect customer data.[10] The proposed legislation, titled the "Consumer Data Protection Act of 2018," would also empower the Federal Trade Commission to create a national "do not track" system for consumers, to establish minimum privacy and cybersecurity standards, and to give consumers more transparency and control over their data.[11] The law would also create a Bureau of Technology within the FTC and would provide that bureau with the ability to hire additional employees with expertise in "management, technology, digital design, user experience, product management, software engineering," and other related fields.[12]

Other bills are also being considered by Congress. For example, on April 10, 2018, Sen. Edward Markey, D-Mass., and Sen. Richard Blumenthal, D-Ct., introduced the Customer Online Notification for Stopping Edge-provider Network Transgressions Act, or the "CONSENT" Act.[13] Markey has referred to the bill as a "privacy bill of rights," declaring that "[t]he avalanche of privacy violations by Facebook and other online companies has reached a critical threshold, and we need legislation that makes consent the law of the land."[14] Among other things, the CONSENT Act directs the FTC to "establish privacy protections for customers of online edge providers" — a development that is likely welcomed by the FTC, given its own calls for clarity on the agency's authority with respect to regulating data security.[15] The bill specifies that those protections will require so-called "edge providers"[16] to notify customers about the collection and use of "sensitive customer proprietary information," which the act defines to include financial and health information, the content of communications, and web browsing and application usage history, among other things.[17] Customers must also be notified about the types of sensitive customer proprietary information that the edge provider collects,[18] how the information will be used and shared,[19] and the types of entities with which the edge provider will share the information.[20]

Similar to the GDPR, the CONSENT Act also includes an "opt-in" consent regime, requiring edge providers to obtain affirmative consent from customers in order to use their sensitive information.[21] This requirement differs from the current practice that is most widely used, under which customers may "opt out" of data collection but if they do not, then, by default, they agree to various uses of their data. The CONSENT Act also prohibits an edge provider from refusing to serve customers who do not consent to the use and sharing of their sensitive proprietary information for commercial purposes.[22]

Not long after the introduction of the CONSENT Act, Sen. Amy Klobuchar, D-Minn., and Sen. John Kennedy, R-La., introduced their own, bipartisan legislation, titled the Social Media Privacy Protection and Consumer Rights Act of 2018.[23] Kennedy has stated that the Social Media Privacy Act, among other things, requires terms of service agreements to be in plain language, ensures users have the ability to see what information about them has already been collected and shared, gives users the right to opt-out of data tracking and collection, and mandates that users be notified of a privacy violation within 72 hours.[24]

Even more recently, on Dec. 12, 2018, Sen. Brian Schatz, D-Hawaii — the top Democrat on the Senate

Communications, Technology, Innovation, and the Internet Subcommittee — led a group of 15 senators in introducing the Data Care Act, which "would require websites, apps, and other online providers to take responsible steps to safeguard personal information and stop the misuse of users' data."[25] Among other things, the Data Care Act creates "reasonable duties that will require providers to protect user data and will prohibit providers from using user data to their detriment," including duties of care, loyalty, confidentiality.[26] Like some of the other data privacy bills, the Data Care Act also provides additional rulemaking authority to the FTC.[27]

Yet as Congress continues to consider how best to move forward on national data privacy legislation, it must resolve significant questions regarding the scope and breadth of any new federal law in this area, particularly whether the law would preempt — that is, supersede — state law in this area as well as whether the law should apply to all businesses that collect and process personal data or merely to certain sectors or industries.

At a recent hearing of the Consumer Protection, Product Safety, Insurance and Data Security subcommittee of the Senate Commerce Committee, Rohit Chopra, one of the two FTC commissioners appointed by Democrats, stated that "clear rules of the road at the federal level" are required, but that "broad preemption [of state laws] would be a huge mistake."[28] In that same hearing, the subcommittee chairman Sen. Jerry Moran, R-Kan., expressed his belief that the CCPA and GDPR provide "a way to at least have negotiations about a national standard,"[29] suggesting that while Congress might not simply copy-and-paste the GDPR or the CCPA when crafting data privacy legislation for the United States, those laws may serve as guides and starting points.

If Congress is serious about enacting a national data protection law, it will need to make several significant decisions:

- Will the law apply to a specific industry or sector, such as social media companies, or more generally to all businesses that collect and process personal data?

- Will the law be addressed to data security, data privacy or both? In other words, will the law provide rules that require businesses to adopt safeguards and policies to protect personal data from theft, destruction, or tampering (data security) or will it also provide rules that protect individual privacy and prohibit misuse of personal data by businesses (data privacy).

- Will the law provide a national consumer data breach notification standard and will it require breach notification to any federal regulators, such as the FTC?

- Will the law preempt state lawmaking entirely, or will it merely establish a minimum national standard upon which states could impose additional requirements?

- Will the law provide prescriptive standards for businesses, such as requiring businesses to encrypt all personal data, or will it allow businesses to adopt their own risk-based standards, so long as those standards are reasonable and appropriate for the purpose of protecting the specific data they possess?

One thing that is clear is that the current regulatory regime, where a business operating in several states can fall somewhere between bare minimum state breach notification laws in one jurisdiction and heightened, prescriptive risk-based rules in another, is less than ideal. A national standard could provide

clear rules for all businesses operating in the United States while simultaneously providing a uniform level of data protection to all Americans across the country.

Joseph P. Facciponti is a shareholder at Murphy & McGonigle PC and a former federal prosecutor.

Maxwell T.S. Thompson is an associate at the firm and previously served at the New York State Department of Financial Services.

[1] https://www.wsj.com/articles/marriott-says-up-to-500-million-affected-by-starwood-breach-1543587121

[2] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

[3] https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html

[4] https://www.janrain.com/resources/industry-research/consumer-attitudes-toward-data-privacy-survey-2018

[5] https://www.dfs.ny.gov/about/press/pr1702161.htm

[6] https://www.insurancejournal.com/news/southeast/2018/05/31/490672.htm

[7] https://sd03.senate.ca.gov/news/20180628-governor-brown-signs-landmark-privacy-law

[8] https://bit.ly/2sfhtJT

[9] https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy

[10] SIL18B29 Section 4, Civil Penalty Authority

[11] SIL18B29 Section 6, “Do Not Track” Data Sharing Opt Out

[12] SIL18B29 Section 8, Bureau of Technology

[13] https://www.congress.gov/bill/115th-congress/senate-bill/2639/text

[14] https://www.markey.senate.gov/news/press-releases/as-facebook-ceo-zuckerberg-testifies-to-congress-senators-markey-and-blumenthal-introduce-privacy-bill-of-rights

[15] https://www.law360.com/cybersecurity-privacy/articles/1103398/ftc-calls-for-data-breach-law-to-clarify-its-authority?nl_pk=43f92aee-09a8-4480-90be-b6bc4cc15a0d&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy

[16] “Edge provider” is defined in the CONSENT Act as “a person that provides an edge service” which is further defined as “(a) a service that is provided over the Internet (i) for which the edge provider requires the customer to subscribe or establish an account in order to use the service; (ii) that the customer purchases from the edge provider without a subscription or account; (iii) through which a program searches for and identifies items in a database that correspond to keywords or characters specified by the customer; or (iv) through which a customer divulges sensitive customer proprietary information of the customer; and (b) includes any service that is provided (i) through a software program, including a mobile application; or (ii) over the Internet, directly or indirectly, through a connected device.

[17] S.2639 Section 2(a)(8)

[18] S.2639 Section 2(b)(i)(I)

[19] S.2639 Section 2(b)(i)(II)

[20] S.2639 Section 2(b)(i)(III)

[21] S.2639 Section 2(b)(iii)

[22] S.2639 Section 2(b)(vi)

[23] https://www.congress.gov/bill/115th-congress/senate-bill/2728/text

[24] https://www.kennedy.senate.gov/public/press-releases?ID=7430B6D4-FF7E-46B8-B631-48B56E9B71A7

[25] https://www.schatz.senate.gov/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online

[26] Id.

[27] Id.

[28] https://fcw.com/articles/2018/11/27/data-privacy-hearing-gunter.aspx

[29] Id.