CORPORATE COUNSEL
An ALM Website
corpcounsel.com | February 4, 2019

A Survey of Proposed Federal Privacy Legislation and the Year Ahead

This article surveys the current legislative proposals and, based on this review, provides in-house counsel with an outline of the most likely contours for any eventual data privacy and cyber security legislation affecting businesses.

By Jeffrey Atteberry

The social, economic, and political forces pushing for a comprehensive overhaul of the nation's privacy regime are numerous, and many see 2019 as presenting the best opportunity yet for passage of federal data privacy legislation.

Revelations about how social media platforms use and share consumers' personal data have raised public concerns about relatively unregulated data markets, while a series of high-profile data breaches have highlighted the complexities and vulnerabilities facing companies that handle large-scale collection and storage of personal data. Meanwhile, lawmakers and other federal officials are taking notice, and data privacy and cyber security issues are moving up everyone's list of priorities.

At the same time, the details of any potential federal privacy regime remain less clear. As in-house legal departments prepare for a year likely to contain sweeping changes in privacy policy, the best indicator of what lies ahead may be found in the various bills and proposals that have surfaced over the past year. These proposals, while unlikely to be adopted in their current form, offer an overview of the current debate and can help corporate counsel anticipate the changes that will arise from the eventual enactment of federal data privacy legislation.

This article surveys the current legislative proposals and, based on this review, provides in-house counsel with an outline of the most likely contours for any eventual data privacy and cyber security legislation affecting businesses.

Current Congressional Proposals

A number of proposals have circulated in the U.S. Senate over the past year. The action began in April when a pair of overlapping and competing bills were introduced. Senate Democrats Ed Markey (D-Mass.) and Richard Blumenthal (D-Conn.) first introduced the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act. The Act would authorize the Federal Trade Commission (FTC) to promulgate rules consistent with the Act's basic requirements. Adopting the framework of "edge providers," the CONSENT Act would broadly apply to any internet or mobile service that is either purchased or offered through the creation of a customer account. The core of the CONSENT Act would be the creation of an opt-in regime requiring edge providers to obtain affirmative consent from customers before collecting their "sensitive information." As defined in the Act, sensitive information includes geolocation data, web browsing history, and call detail information. To shore up this opt-in regime, the Act prohibits edge providers from refusing service to users who do not provide consent. Under the bill, the FTC is directed to promulgate rules requiring user notification in the event of a data breach from which "harm is reasonably likely to occur." The CONSENT Act would be enforced by the FTC, other federal agencies which have statutory authority over specific activities, and state attorneys general.

Also in April, Senators Amy Klobuchar (D-Minn.) and John Kennedy (R-La.) introduced S.2728, entitled the Social Media Privacy Protection and Consumer Rights Act of 2018. The bill applies to "online platforms," which are defined (more broadly, perhaps, than the bill's title suggests) as any public facing websites or apps that collect personal data during the consumers' use of the platform. In contrast to the CONSENT Act, however, the bill adopts an opt-out regime. Covered platforms would be required to disclose what data is collected, and the consumer has the right to opt-out of data collection and tracking. Furthermore, the bill allows providers to deny service to customers if opting-out of data collection "creates inoperability in the online platform." Consumer notification of a data breach is required within 72 hours after the provider becomes aware that user's personal data has been transmitted in manner inconsistent with the user's expressed preferences or the platform's disclosed uses. Enforcement is left to the FTC and state attorneys general.

Another flurry of activity in the Senate came at the end of the year. Of all the proposed pieces of legislation that have been recently introduced, the draft bill circulated by Ron Wyden (D-Ore.) in November has grabbed the most headlines. Given its stringent penalties, Wyden's bill is generally viewed as the strictest of all the current proposals. Entitled the Consumer Data Protection Act, Wyden's draft legislation applies generally to entities subject to Section 5 of the FTC Act. However, the Act excludes from its requirements entities with annual gross revenue of less than $50 million and which have collected information from less than 1 million customers and devices. Adopting an expansive opt-out framework, Sen. Wyden's bill would require the FTC to create a centralized "Do Not Track" List, enabling consumers to opt-out of data sharing from all covered entities. Before collecting any user data, covered entities would be required to consult the Do Not Track List. Covered entities would be permitted to deny service to consumers who chose to opt-out, so long as the consumers are offered a paid version of the service instead. Furthermore, much like the GDPR and the CCPA, the bill gives consumers the right to request, review, and challenge any information collected on them. Covered entities must establish and implement cyber security and data privacy policies, practices, and procedures. Covered entities are further required to submit annual reports detailing their compliance with the bill's various regulations. Such reports are to be certified by the entity's Chief Privacy Officer and imposes a penalty of up to $5 million or 20 years' imprisonment for intentionally falsified certifications. Finally, the bill would be enforced by the FTC, whose power to impose fines is increased up to 4 percent of annual gross revenue. In order to bolster this newly expanded enforcement authority, a Bureau of Technology with 125 new employees would be cre-

ated within the FTC. Interestingly, the bill also directly confronts the standing issue that has plagued much privacy litigation by defining "substantial injury" as including "noneconomic impacts."

In the broadest display of support for data privacy and cyber security legislation, Senator Brian Schatz (D-Hawaii), along with 14 other Democratic senators, introduced in December the Data Care Act of 2018. Taking a different approach than the other pieces of proposed legislation, the Data Care Act would impose fiduciary duties on "online service providers" that collect individually identifying data about users. Under a duty of care, online service providers would be required to "reasonably secure" personally identifiable information. In the event of a breach of sensitive information (including biometric, health or financial data), users must be "promptly" notified. A duty of loyalty prohibits providers from using end user's PII in any manner that would benefit the provider to the detriment of the user. However, the Act limits such detriment or injury to "material physical or financial harm." Finally, a duty of confidentiality prohibits providers from disclosing or sharing users PII with third parties, except as may be consistent with the duties of care and loyalty. Once again, enforcement will rest primarily with the FTC, which is also granted the authority to promulgate rules and regulations to operationalize the broad and general requirements of the Act. The Act also authorizes enforcement by state attorneys general and state consumer protection officers.

While the Senate has been more active, the House of Representatives also has seen some recent legislative proposals. Congressman Hank Johnson (D-Ga.) has introduced two bills, one that focuses on data privacy on mobile devices and another that provides users with rights to opt-out of data collection by "data brokers." Under the mobile app proposal, app developers would be required to obtain consumer consent before collected data. Conversely, pursuant to his proposed data broker legislation, data brokers are to provide consumers with a means of opting-out of the use, sharing, or selling of their personal information. Consumers are also afforded the right to review and correct the personal information that the data broker collects, assembles, or maintains.

Finally, Congresswoman Suzan DelBene (D-Wash.), a former executive at Microsoft, has co-sponsored a bill with Congressman Hakeem Jeffries (D-N.Y.), entitled the Information Transparency and Personal Data Control Act. The Act would apply to any "operator" of a website or other online service that collects or maintains personal information of users for commercial purposes. The draft bill does contain a carve-out for operators with 500 or fewer employees. The heart of the bill is the establishment of an opt-in regime for data collection. Operators would be required to provide a conspicuous privacy and data use policy that specifically requests the user's express affirmative consent before the collection, storage, processing, sale, or sharing of any sensitive personal information. The bill mandates specific disclosures, including the identity of the entity collecting the information, what information is collected, the purpose for such collection or use, the identity of any third parties receiving the information, and how long the information is stored. Evidencing a concern with overly complicated terms of use and privacy policies, the bill further requires that such disclosures be "concise and intelligible" and written in "clear and plain language." Users must also be provided with clear instruction as to how they can view the sensitive personal information they have provided to the operator. After obtaining opt-in consent, the operators must provide users with the ability to opt-out at any time. Finally, covered operators must conduct annual privacy audits detailing the adequacy and effectiveness of their privacy and cyber security measures. Once again, the FTC and the state attorneys general would enforce the provisions of the bill.

Key Takeaways

The proposed pieces of legislations appear to have the most agreement on issues of enforcement.

First and foremost, enforcement for any data legislation is likely to rest with the FTC, a consensus which is not all surprising given the Commission's historic role in enforcing data privacy and cyber security. Second, none of the current proposals provide a private

right of action. By excluding private rights of action, the current proposals are consistent with the preferences expressed by the tech industry and the U.S. Chamber of Commerce. On the other hand, consumer advocacy groups, including the Electronic Privacy Information Center and the Center for Digital Democracy, have advocated for a private right of action and will likely continue to do so. Nevertheless, based on the current proposals, it appears as if an unexpressed agreement may have been reached among lawmakers that enforcement will be limited to the FTC and state attorneys general. The real issues regarding enforcement are likely to be whether or not the FTC receives any expanded authority to directly impose fines or promulgate rules, and whether the ranks of the FTC will be expanded to accommodate any increase in its authority.

There is more uncertainty regarding the central question of what consent framework is likely to structure any federal data privacy legislation. While a handful of proposals have adopted an opt-in framework, most of the current drafts and bills have opt-out regimes of varying kinds and strengths. Again, the emerging consensus in favor of an opt-out regime is in line with expressed preferences of the tech industry, as well as the current frameworks employed by most online platforms. Nevertheless, while the current momentum here appears to be in favor of an opt-out framework, there is likely to be considerable debate around this issue. One nuance to look for in any future legislation is opt-out frameworks that prohibit data collectors from discriminating against user's who choose to opt out or that require platforms to provide a reasonably priced paid service for those users who do.

The largest unresolved issue, which is conspicuously avoided by the current proposals, remains whether any federal legislation will preempt state laws. Looming large in the background of this debate is, of course, the CCPA. Indeed, passage of the CCPA (along implementation of Europe's GDPR) is largely responsible for the sudden interest, especially within the tech industry, in promoting uniform federal legislation. The tensions surrounding the preemption issue were front and center during a series of Congressional hearings held in the fall. Representatives from tech all stated that they were in favor of preemption and expressed concern that federal legislation would only add to the regulatory thicket if preemption was not part of the legislation. However, a number of senators, including Senators Schatz and Blumenthal, expressed the view that, in order for preemption to be part of any legislation, the federal protections must be "meaningful" and at least as strong as the CCPA. In the end, the preemption issues is likely to remain hotly contested issue that is deeply intertwined with the detailed requirements of any possible legislation.

The coming year promises to be an eventful one for federal privacy legislation. Of course, Congress being what it is, any number of completely unrelated issues could sideline the push for comprehensive federal data privacy and cyber security legislation. Nevertheless, the momentum at present is strong; and, with the CCPA currently scheduled to go into effect on Jan. 1, 2020, the underlying forces pressuring for federal legislation are unlikely to abate. In-house counsel responsible for data privacy and cyber security should keep a close-year on the developments and be prepared for an eventful year ahead.

Dr. ***Jeffrey Atteberry****, CIPP/US, is a partner in Jenner & Block's Los Angeles office who has extensive experience litigating complex matters in federal and state courts. His practice focuses on commercial litigation, including disputes involving misappropriation of trade secrets, unfair competition, breach of contract, class action defense and securities regulation. A Certified Information Privacy Professional/United States (CIPP-US), Dr. Atteberry also has significant experience advising and representing companies on a variety of privacy issues.*