Published on *The National Law Review* https://natlawreview.com

The Battle of the Bills Begins: Proposed Federal Data Privacy Legislation Aims to End Patchwork Problem But Increases Enforcement

Article By:

Philip J. Bezanson

Brittney E. Justice

Claire E. Cahoon

After years of advocacy from both sides of the aisle and growing concerns about challenges created by state-based solutions, 2021 is poised to be a bellwether year for Congressional debate over federal data privacy regulation. On March 10th, Representative Suzan DelBene (D-WA), a former Microsoft executive, introduced the first of what will likely be many data privacy bills introduced in the 117th Congress. The Information Transparency and Personal Data Control Act ("ITPDCA") is intended to create one uniform standard for consumer data privacy regulation, suggesting a movement in Congress towards acknowledging industry's need for uniformity in what is otherwise an expanding patchwork of conflicting state privacy laws.

Congresswoman DelBene introduced a similar version of this legislation in 2019, but it ultimately did not gain traction. The updated ITPDCA largely mirrors its predecessor. The new bill requires opt-in consent prior to sharing consumers' personal information with a third party in a manner beyond any initially intended purpose. Companies must also honor consumers' requests to opt-out of "any collection, transmission, storage, processing, selling, sharing, or other use" of personal information.

Additionally, data controllers, processors, and third parties must publicly maintain a privacy and data use policy explaining, among other things, how data will be used, where data is stored, and how consumers' information is protected from unauthorized access. Privacy policies must be clear and written in "plain English." To ensure compliance with data privacy standards, companies using over 250,000 individuals' personal data per year must also obtain and publish the results of a privacy audit every two years.

The ITPDCA grants the Federal Trade Commission ("FTC") regulatory authority to promulgate rules and enforce the legislation. The bill also provides the FTC with $350,000,000 in additional funding and orders the Commission to hire 500 new full-time employees to facilitate enforcement under the Federal Trade Commission Act's existing unfair or deceptive acts or practices regime.[1] Unlike its 2019 predecessor, the ITPDCA contains a clause that prohibits companies from contracting out of

obligations imposed by the Act. Companies will not, however, bear legal responsibility if third-party contractors fail to provide opt-in or opt-out consent under new liability shield provisions.

Other additions to the ITPDCA include a recitation of principles styled as individuals' rights regarding their personal data. The current version of the bill includes immigration and citizen status, mental and physical health diagnoses, and gender identity or intersex status in the definition of protected "sensitive personal information." Information related to employment, de-identified information, and publicly available information are not "sensitive personal information" under the bill.

Two parts of the bill widely considered to be business-friendly, which could lead to bipartisan support, are (1) federal pre-emption of any similar state regulatory regime and (2) the lack of a private right of action by any individuals seeking to recover financially for violations of the ITPDCA. Largely thanks to these two provisions, trade organizations such as the National Retail Federation, the Main Street Privacy Coalition, and the U.S. Chamber of Commerce have already voiced support for the bill.

In a statement announcing the new ITPDCA, Rep. DelBene acknowledged that states were "understandably advancing their own legislation in the absence of federal policy." However, she agreed with many business leaders that any federal law must avoid "a patchwork of different privacy standards by preempting conflicting state laws." Currently, companies must navigate multiple state privacy laws to ensure compliance in all jurisdictions—a task that can create significant costs and disruptions as new laws, with potential inconsistencies, are enacted. The ITPDCA would eliminate all state laws regarding data privacy, excepting those which establish data breach notification requirements, laws regulating biometric data, wiretapping laws, and laws like the Public Records Act.

Unlike the EU's GDPR and California's CCPA, the ITPDCA does not provide a private right of action for consumers. Instead, enforcement is delegated to the FTC and State Attorneys General. State Attorneys General are only authorized to bring actions under the ITPDCA if the FTC does not bring an action within 60 days of discovering a violation. Further, State Attorneys General must give alleged violators 30 days to cure non-willful violations prior to commencing an enforcement action. Although ITPDCA appears to open the door to more federal and state investigations and potential enforcement actions, the ITPDCA's lack of a private right of action should be welcome news to companies concerned by the ever-increasing number of lawsuits filed under the CCPA – because the ITPDCA preempts all related state law, Californians' private right of action would disappear along with the rest of the CCPA.

Even if it is never signed into law, the ITPDCA's reintroduction is a foundational starting point for privacy policies to come. Several other lawmakers are reportedly planning to introduce their own data privacy bills. Sen. Ron Wyden (D-OR) plans to reintroduce his 2019 Mind Your Own Business Act, a less-business-friendly proposal which creates a national "do not track" system, allows the FTC to skip the consent decree process and assess large fines against first-time offenders, and includes criminal liability for making false statements to the FTC. Senators Kirsten Gillibrand (D-NY) and Sherrod Brown (D-OH) also appear to be planning to re-introduce their 2020 privacy proposals.

The introduction of the ITPDCA, and the debate that will surely follow, is likely to trigger a range of Congressional fact-finding and oversight. With this in mind, companies should consider whether their current data protection practices measure up to already-existing privacy laws, including the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley Act, and the Red Flags Rule. The FTC provides guidance on compliance with these acts and more on their website. Further, until federal law preempts the various state privacy laws, companies must continue to track, adjust and adapt their practices in order to comply with applicable state privacy laws. As of this writing,

lawmakers in several states, including New York, Florida and Washington, have announced that they are currently considering privacy legislation.

Regardless of whether or not federal privacy legislation passes in 2021, data protection and privacy laws are likely to continue shifting for years to come. Rep. DelBene has acknowledged that her legislation is only a starting point and that eventually, the U.S. will need to expand data privacy laws beyond the ITPDCA.

National Law Review, Volumess XI, Number 77