BRACEWELL

INSIGHTS

Federal Privacy Legislation – Is it Finally Happening?

July 26, 2022

By: ***Lucy Porter***

Proposed federal privacy legislation is not a new thing. But the latest iteration – ***the American Data Privacy and Protection Act*** – has many wondering if this will be the legislation that finally goes the distance. This is the first federal privacy legislation to advance out of committee, and despite the obstacles, momentum is on the upswing for a federal privacy law. Read on to find out more about the legislation and why the support may finally be there to enact a comprehensive federal privacy law.

Setting the Stage

The American Data Privacy and Protection Act (the "Act") is not the first privacy legislation introduced in the 117th Congress, in fact protections for consumer privacy, health privacy, financial privacy, cybersecurity, children's privacy, and other protections have been introduced. But there are two elements that make this Act unique. First, it is the "bipartisan and bicameral effort to produce a comprehensive data privacy framework" as noted in the joint press release by the authors of the Act U.S. Senator Roger Wicker (R-MS) of the Senate Committee on Commerce, Science, and Transportation and U.S. Representatives Frank Pallone (D-NJ) and Cathy McMorris (R-WA), both members of the House Committee on Energy and Commerce. Indeed, the theme of compromise featured prominently during the July 20 House Committee on Energy and Commerce markup of the bill, the members focused repeatedly on the compromise nature of the bill as they discussed proposed amendments. The framework proposed by the Act builds on legislation that has come before, but in doing so reflects a thoughtful approach to development and a potential path to building broad support.

Second, the timing of the Act. We now have five states – California, Connecticut, Colorado, Utah, and Virginia – that have enacted a comprehensive privacy law. There is mounting concern from key stakeholders of the impact that this "patchwork" of laws will have on consumers and businesses. At the same time, without a federal privacy law the United States is being left out of the conversation at a global level as Europe and China seek to lead the world in defining the privacy protection framework.

Key Elements of the Act

The framework for the Act, H.R. 8152, steers away from the consent framework while still including consumer rights, imposing duties on covered entities including privacy by design and corporate accountability. Other features of note:

- Covered data does not include employee data.

- Data minimization is required
    - "a covered entity may not collect, process or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to" achieve a purpose specified in the Act.

    - The FTC, who ultimately would be granted enforcement authority, shall issue guidance regarding what is reasonably necessary and proportionate.

While these elements may be of significant concern to those subject to the Act, the provisions likely to get the most discussion are the provisions related to preemption and private right of action.

The proposed private right of action limits awards to compensatory damages, injunctive relief, and attorney's fees. What complicates, or perhaps overly complicates, the private right of action is a requirement to notify the FTC and the respective State Attorney General of the intent to file the suit prior to doing so. The FTC and State Attorney General then have 60 days to determine "whether they will independently seek to intervene in such action." Committee markups changed the effective date of the right begin two years from when the Act takes effect compared to the initial four, but to this point the right has been maintained.

Regarding preemption, the story is different. The Act preempts state comprehensive data privacy laws, such as CPRA, but does not preempt the Illinois Biometric Information Privacy Act. Other examples of state laws that are not preempted include (i) breach notification requirements, including the personal information breach requirements under the CPRA; (ii) criminal laws for fraud, identity theft, or cyberstalking; (iii) financial and bank records; or (iv) health information. The Act does not preempt COPPA. An amendment to exempt the California Consumer Privacy Act and the California Privacy Rights Act failed, but it is likely this issue will be raised again.

Where do we go from here?

The next stop is the House floor. As we saw in the Committee, the issue of preemption from the California delegation may continue to be a significant obstacle. Additionally, no Senate Democrat has yet signed on to the Act and until they do it is unclear whether the Act truly has the support required to achieve passage in this election year. For certain Senators, the private right of action and preemption may not go far enough to protect the rights of consumers and thus without changes they may be unwilling to support the text in its current form. On the other hand, some industry and privacy professionals are speaking out in support of the Act arguing the Act has stronger protections for Americans' online presence than any current state law. One thing is certain, without federal legislation, the patchwork of state data privacy laws is only going to grow.