Insight

Understanding the ADD Act

WILL RINEHART | JANUARY 17, 2019

Senator Marco Rubio introduced the American Data Dissemination Act of 2019 (or the ADD Act) on January 16, kicking off the 116th Congress's debate over federal privacy legislation. The core of the bill tasks the Federal Trade Commission (FTC) with writing a new set of regulations for the information age based on the principles in the Privacy Act of 1974, only updated to apply to Internet businesses. The bill will likely face opposition from Democrats and advocates, since it would create an expansive privacy regime, supersede state laws, and grant the FTC wide latitude in creating new privacy rules.

Unlike Senator Schatz's Data Care Act of 2018 or Senator Wyden's Consumer Data Protection Act of 2018, the ADD Act is unique in that it charges the FTC with submitting to Congress a set of regulations that are substantially similar to the Privacy Act of 1974. While the Privacy Act applies to federal agencies, the ADD Act would be applied to "covered providers" (more on that later). Of note, the Act would give Congress two years to respond to the FTC's proposal; if Congress fails to take any action, then the FTC is given the power to "promulgate final regulations that impose such privacy requirements," which would supersede any state effort. In other words, the Act gives the FTC wide latitude to write the rules of the road for the information age.

The ADD Act does give the FTC some guidance. For one, the regulations must exempt small, newly formed businesses. As Senator Rubio explained in a statement, "It is critical that we do not create a regulatory environment that entrenches big tech corporations." The European Union's General Data Protection Regulation provides part of the subtext to this provision. In the months since becoming enforceable, small businesses have struggled to comply with the law and have seen significant dips in income, while large companies such as Google and Facebook have been able to bear the costs.

A small business exemption is also needed because the ADD Act would apply to nearly every business. While the legislation is focused on big tech corporations, the bill defines "covered

providers" as an entity that "provides a service that uses the internet" and "collects records." There is hardly a business in America that wouldn't be included with that kind of expansive definition.

The ADD Act also directs the FTC to create regulations that would:

- Restrict the disclosure of records;
- Give individuals access to those records;
- Grant individuals the right to amend records; and
- Establish a code of "fair information practices."

In total, every business in the United States would be subject to an onerous privacy regime. And because the ADD Act is based on the Privacy Act of 1974, it too will commit the same errors by focusing on data collection and disclosure. But collecting and disclosing data isn't especially problematic. What is worrying is how a company might use information in a way that could be *harmful* to consumers. Since the Privacy Act allows for exemptions, the actual form of the privacy regulations coming from the ADD Act will depend on how the FTC interprets these exceptions for Internet businesses.

The ADD Act also faces an uphill battle in Congress. Privacy-regulation advocates and Democratic leadership have fought federal preemption, as a federal law would supersede more restrictive state efforts such as the recently passed California Consumer Privacy Act. Furthermore, since data privacy is one of the few issues where there is some bipartisan agreement, it is difficult to imagine that congressional leaders would choose to hand over their authority to a federal agency. The ADD Act of 2019 might be the first of its kind out of the gate, but it likely won't be the final form of a federal privacy law.