BROOKINGS

TechTank

How the 2020 elections will shape the federal privacy debate

Cameron F. Kerry and Caitlin Chin Monday, October 26, 2020

The 116th Congress opened with great energy and promise for federal privacy legislation across both houses and parties. The main action took place in the Senate Committee on Commerce, Science, and Transportation, where Chairman Roger Wicker (R-MS) once called for a federal privacy law "on the books by the end of 2019" and senior members engaged in bipartisan negotiations. That was far from the only activity, though—the House Energy and Commerce Committee, Senate Judiciary Committee, and Senate Banking Committee also held hearings and explored legislation. In all, more than 30 bills have been filed since the 2018 election.

By the end of 2019, though, Wicker and Ranking Member Maria Cantwell (D-WA) each released separate proposals, respectively the draft United States Consumer Data Privacy Act (USCDPA) and the Consumer Online Privacy Rights Act (COPRA). Despite sharp differences when it came to federal preemption of state privacy laws and individual rights to sue, these bills showed promising agreement on significant issues, including data minimization, individual privacy rights, transparency, and discriminatory uses of personal data. In June 2020, we released detailed analysis of these bills with a proposed approach to bridge the differences between the two.

In the end, these efforts fell short. The pandemic took up most of the legislative energy and made it more difficult to overcome partisan polarization. This polarity was underscored by the introduction of two bills in May 2020, one from either side of the aisle, to promote privacy protections for COVID-19 contact tracing. Some may have expected that the urgency of the pandemic would prompt bipartisan support for trustworthy contact tracing—and in turn, that consensus on this narrow issue could provide an

example for broader legislation. Yet, even these contact tracing bills reflected the same divisions on preemption and the private right of action as did USCDPA and COPRA. Both bills—plus a third from Senator Cantwell which left out a private right of action—ultimately fizzled out by the end of the summer.

Senators put in a bookmark for the next Congress

As Congress came back into session in September, the Senate Commerce Committee held a full committee hearing titled "Revisiting the Need for Privacy Legislation"—an appropriate reminder that privacy legislation is unfinished business. During the hearing, Wicker reflected on early privacy hearings at the beginning of the 116th Congress, the committee's work on developing data privacy legislation since then, and the current opportunity to pass a privacy law "with real consensus among members of both parties."

In advance of the hearing, Chairman Wicker introduced a new bill, the SAFE DATA Act, co-sponsored by John Thune (R-SD), Deb Fischer (R-NE), and Marsha Blackburn (R-TN). This bill incorporates much of Senator Wicker's USCDPA, bundled with elements from Thune's Filter Bubble Transparency Act, Fischer's DETOUR Act, and Blackburn's BROWSER Act.

The SAFE DATA Act consolidates existing bills into a more unified Republican position—but does nothing to advance negotiations across the aisle. Like its predecessor USCDPA, the SAFE DATA Act broadly preempts state privacy laws and makes no mention of any kind of private right of action for individuals to sue. These provisions alone are likely to preclude Democratic support on the bill. In addition, the SAFE DATA Act includes several modifications to USCDPA that could each, in their own respect, stiffen Democratic opposition to the bill. COPRA, USCDPA, and the SAFE DATA Act all feature the rights for individuals to access, correct, delete, and request portability of personal information—but small differences in language can significantly affect implementation. Both COPRA and USCDPA give individuals the right to access the names of third parties to whom personal data has been transferred—but the SAFE DATA Act only provides for access to "categories of third parties and service providers." USCDPA and COPRA both allow covered entities 45 days to fulfill access, correction, deletion, and portability requests; the SAFE DATA Act extends this to 90 days.

Furthermore, the SAFE DATA Act adds new exceptions to the individual rights provision that afford covered entities greater flexibility to decline a person's request to exercise a privacy right. For example, the SAFE DATA Act permits covered entities to decline requests that would "require disproportionate effort" or "result in the release of trade secrets, or other proprietary or confidential data or business practices." It also gives them the option to delete covered data (except for sensitive data) rather than fulfill access and correction requests. Finally, while the SAFE DATA Act, USCDPA, and COPRA all specify that individuals cannot waive their privacy rights, only the SAFE DATA Act allows covered entities to offer different prices and functionalities for products or services based on an individual's exercise of their privacy rights. These changes could give more leeway to businesses that collect, process, and transfer personal data.

Looking ahead to the 117th Congress

On the surface, some provisions of the SAFE DATA Act seem to marginally widen the gap between COPRA and USCDPA. But taken together, neither Republicans nor Democrats have significantly changed their approach to privacy legislation in 2020—COPRA and USCDPA had already achieved near agreement on many significant issues, but with the fundamental issues of preemption and the private right of action far apart.

Senator Cantwell's remarks during the September 23 hearing, as well as the committee's invitation to California Attorney General Xavier Becerra to testify, underscored her position that a federal privacy law must include a private right to sue and allow states to adopt privacy legislation with stronger protections. Meanwhile, the introduction of the SAFE DATA Act shows the parties coalescing around two leading privacy bills—the Republicans behind the SAFE DATA Act and the Democrats behind COPRA—each with three co-sponsors on the Senate Commerce Committee.

As for whether USCDPA or COPRA will emerge as the main vehicle for privacy legislation in 2021, that will depend on who chairs the Senate Commerce Committee come January. If Republicans hang on to the Senate next year, the SAFE DATA Act will serve as a focal point for negotiations with Senate and House Democrats—and potentially with the White House. But if Democrats take the Senate, COPRA will be the focal point.

Whoever sits in the White House will also play into the prospects for privacy legislation. Democratic nominee Joe Biden is on the record supporting comprehensive privacy legislation. Thus, a Biden administration would likely play a role in privacy regardless of which party holds the Senate. If elected, it is possible Biden might have to deal with a Republican Senate—but this is nothing new for Biden, who has experience operating with numerous Republican-controlled Congresses. And, if the table turns, a clean sweep would give Democrats significant control over the direction of privacy legislation, depending on what becomes of the filibuster, Senate rules, and overall level of partisanship in Congress.

The Trump administration, on the other hand, has been a bystander on federal privacy legislation. There is little reason to expect that to change if he remains in office—except that a Trump administration could be expected to veto much legislation passed by two Democrat-controlled houses, if he somehow survives a Senate wave.

Thus, the outcome of the 2020 elections, and especially the party in control of the Senate Commerce Committee, will shape the negotiations of these two positions. The process will also be influenced by the result of California's Proposition 24 ballot initiative, which could harden preemption positions by expanding the California Consumer Privacy Act, and by what could be a federal legislative agenda packed with initiatives to address economic recovery, pandemic management, and other crisis responses. While the need for privacy legislation will remain fundamentally the same in 2021, the political situation could look vastly different.