Top Privacy Law Issues in 2022 as Congress Debates a Federal Law

Published in Bloomberg Law (December 28, 2021) by Kirk Nahra –

WilmerHale cybersecurity and privacy attorney Kirk J. Nahra discusses several issues for 2022 that will shape any national privacy law. He recommends watching action at the state level, bias and discrimination issues involving the use of big data and algorithms, and the FTC's enforcement role.

Will 2022 be the year for a national privacy law? We are seeing new federal proposals, ongoing negotiations about key issues such as a private right of action and state pre-emption, and new activity at the state level. There is still a long way to go, and 2022 isn't likely to be the year—but watch for 2023.

Here are five key issues to watch next year as this debate evolves.

Identifying Pressure Points From State Law

It is clear that one of the key pressure points for Congress is the activity in states concerning "general" or "comprehensive" privacy laws.

With the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), and new laws going into effect in 2023 in Colorado and Virginia, both Congress and (more importantly) various constituency groups are paying attention to the states. With each passing state law, the baseline for any eventual privacy law rises (meaning the price for pre-emption grows).

At the same time, while there clearly are similarities between these laws, there also are critical differences—meaning that no obvious state model is emerging.

A new Massachusetts proposal—which seems to be getting some traction—could be, in the words of Woody Hartzog, professor of law and computer science at Northeastern University, "the most revolutionary data-privacy legislation in the United States."

My view remains that, if three to six major states pass a law along the lines of the CCPA—in any reasonable analogy (especially if this includes an aggressive Massachusetts law)—then corporate America will need to go to Congress and request a national privacy law.

Is There a Realistic Alternative to Notice and Choice?

There is increasing criticism from a broad range of constituencies about the role of the traditional "notice and choice" regime for privacy law. The concern is that proceeding down a "notice and choice" path puts too much burden on the consumer without placing appropriate restrictions on the companies collecting and using personal data.

As of yet, however, other than in some prominent academic circles and other advocacy, no meaningful alternative approach has emerged in these state laws. The CCPA, for example, places very few direct restrictions on covered companies, while providing significant additional “notice and choice” options for consumers.

The Virginia law provides that no processing of sensitive data can emerge without consumer consent, without explaining how that consent will be obtained or what realistic alternative there will be for consumers when presented with, presumably, an “all or nothing” approach.

I have written about the possibilities of a context based option, but these concepts have not for the most part yet emerged in proposed legislation.

Addressing the FTC’s Role

The Federal Trade Commission, under new leadership, is engaged in a widespread set of actions to broaden its overall reach, on data privacy, security, and wide range of other consumer protection areas. This may include an extended rulemaking proceeding to develop unfairness privacy principles related to its authority under Section 5 of the FTC Act.

Congress may also give the FTC authority for penalties under Section 5 in the first instance (rather than only being able to pursue penalties after violations of previous orders).

At the same time, several current bills in Congress give primary regulatory authority under a national privacy law to a new agency rather than the FTC. So, anyone interested in the debate over a national privacy law should be watching what the FTC is doing, both on its own and as part of the aggregate pressure on Congress.

Will Congress Tackle Algorithmic Discrimination?

The Biden administration also has embarked on its own initial efforts to develop some specific privacy principles. In December, the National Telecommunications and Information Administration held three “listening sessions,” designed to “provide the data for a report on the ways in which commercial data flows of personal information can lead to disparate impact and outcomes for marginalized or disadvantaged communities.”

This raises the key question of whether Congress will try to address these bias and discrimination issues involving the use of big data and algorithms in a national privacy law. Traditionally, we have addressed these concerns as civil rights issues or in the context of other subject specific laws (e.g, insurance or health care), rather than through privacy law.

Will Congress tackle this enormously complicated issue in a national privacy law as well as all the other elements it needs to address?

Will the Law Impact the EU Data Transfer Issue?

As a last key issue, how will Congress try to address the increasing concern in the EU and other countries about the transfer of personal data to the U.S.? The key element in the current concern—emanating from the Schrems 2 decision—is how the U.S. government can access data that is transferred to the U.S.

Few—if any—of the major privacy bills that have been introduced address this issue in any meaningful way. Business will be watching closely to see whether Congress can help navigate a solution with the EU authorities to this increasingly challenging issue.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Write for Us: Author Guidelines

Author Information

Kirk J. Nahra is a partner with WilmerHale in Washington, D.C., where he is the co-chair of the firm's global Cybersecurity and Privacy Practice. He teaches privacy issues at several law schools, serves as a fellow with the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis, and as a fellow with the Institute for Critical Infrastructure Technology.