State influence on the path to a federal US privacy law

As California and Virginia adopt privacy laws, many other states propose similar legislation to protect their consumers. By **Lindsey Tonsager** and **Tian Kisch** of Covington & Burling LLP.

Support for a comprehensive data privacy law in the United States has grown over the last three years. However, the legislative agenda in the US Congress is crowded, and prospects for passage of federal privacy legislation remain uncertain. Congress is focused on pandemic-related recovery efforts, proposals to update the nation's infrastructure, and several other significant matters unrelated to data privacy. Multiple privacy measures have been introduced in Congress that overlap in many respects, but diverge on a few important details. And, in the meantime, numerous states have proposed their own privacy measures, but few have succeeded in enacting privacy legislation. As a result, and as explored more below, whether Congress succeeds in enacting federal privacy legislation might be influenced in large part on what does or does not happen in the states over the next 18 months.

Federal privacy proposals under consideration

Multiple comprehensive privacy bills have been introduced so far in the 117th Congress, including the Information Transparency & Personal Data Control Act (H.R. 1816), the Social Media Privacy Protection and Consumer Rights Act (S. 1667), and the Data Care Act (S. 919). These proposals share many common elements, including requirements to provide consumers notice and control over how personal information is processed. However, certain key differences remain, as summarized below.

H.R. 1816: Information Transparency & Personal Data Control Act[1]: This bill, which Rep. Suzan DelBene (D-WA) introduced, would require affirmative, express consent for the collection, sale, or sharing of sensitive personal information with third parties if the third party will use the data for a purpose distinct from those outlined in the privacy notice provided to consumers. Sensitive personal information is defined under the proposal to include, for example, identifiable financial and health information, children's information, Social Security numbers, geolocation information, immigration status, religious beliefs, and web browsing history. Consumers also would be able to opt out of having personal information – that is not sensitive – collected or shared. Privacy policies must clearly state how users can exercise these choices and publish the contact information of entities collecting sensitive personal information. Businesses that collect sensitive personal information also must submit to biannual privacy audits.

The bill would preempt conflicting state laws with certain exceptions, such as state data breach notification laws and state laws regarding biometric information.

The bill does not provide a private right of action. Instead, it allocates $350 million to the Federal Trade Commission (FTC) and authorizes the hiring of 500 new FTC employees.

S. 1667: Social Media Privacy Protection and Consumer Rights Act of 2021[2]: Reintroduced by Sen. Amy Klobuchar (D-MN), the scope of this bill is broader than its title implies. The bill would regulate certain "online platforms" that collect personal data "during the online behavior of a user of the online platform." "Online platform" is a defined term that includes "a social network, an ad network, a mobile operating system, a search engine, an email service, or an Internet access service."

The bill would require affirmative express consent in certain circumstances, including overriding a consumer's privacy preferences. It also would require covered online platforms to establish and maintain privacy or security programs and to notify users if personal data is transmitted in violation of these programs within 72 hours.

Unlike the Information Transparency & Personal Data Control Act, Sen. Klobuchar's bill does not include a preemption clause. There is, however, no provision for private right of action. The Act would be enforced by the FTC and state attorneys general (AG).

S. 919: Data Care Act of 2021[3]: Sen. Brian Schatz (D-HI) reintroduced the Data Care Act, which would establish certain duties for online service providers that handle sensitive personal data. These duties include a duty of care, duty of loyalty, and duty of confidentiality. The bill sets out requirements for meeting these duties, including reasonably securing personal data and ensuring that any third party an online service provider shares personal data with fulfills the same duties.

The bill does not include a preemption provision, nor does it include a provision for a private right of action. The bill grants enforcement and rulemaking authority to the FTC to implement the Act. States may also bring civil enforcement actions under this bill.

More action in the states

The first half of 2021 has proven to be an action-packed six months for US state privacy legislation. In March, Virginia passed the Consumer Data Protection Act, becoming the second state after California to pass comprehensive data privacy legislation governing the online and offline collection, handling, and processing of personal data. Many other states (including, for example, Florida, Colorado, Oklahoma, New York, and Washington) actively considered privacy legislation. Some of these states' legislative sessions ended with no passage of the privacy proposals, and other states' sessions are soon coming to a close. However, these proposals remain relevant because some of them are likely to be re-introduced in the next legislative session or influence what is happening in other states. Importantly, these state proposals

differ from each other in significant ways, including whether they provide for a private right of action, the type of consent required, whether they obligate businesses to conduct and disclose privacy risk assessments, and whether they impose fiduciary duties on businesses processing personal information.

Private right of action

One of the most notable differences between the state privacy proposals considered so far is whether they include a private right of action. The California Consumer Privacy Act (CCPA), passed in 2018 and in effect as of 1 January 2020, provides for a private right of action in limited circumstances.[4] Specifically, consumers can sue for damages only if a subset of personal information is accessed and exfiltrated, stolen, or disclosed without authorization, and both:

(1) the data was neither encrypted nor redacted, and
(2) the breach was the result of the business failing to implement and maintain reasonable security procedures or practices appropriate to the nature of the information.

The California Privacy Rights Act (CPRA), passed by ballot measure in 2020 and taking effect on 1 January 2023, narrowly expands this private right of action (to include email addresses in combination with a password or security question and answer) to the definition of covered personal information categories.

Virginia's Consumer Data Protection Act (CDPA), signed into law on 2 March 2021 and also taking effect on 1 January 2023, has no private right of action.[5] Instead, the Virginia AG is solely responsible for enforcement.

Other proposed state privacy bills split on the inclusion of a private right of action. The Massachusetts Information Privacy Act would allow "[a]ny individual alleging a violation of this chapter or a regulation promulgated under this chapter" to "bring a civil action in any court of competent jurisdiction."[6] And three proposed New York bills — the New York Privacy Act[7], the Digital Fairness Act[8], and SB 567[9] — all also contain provisions that would allow individual consumers to bring actions. Colorado's SB 190[10], Connecticut's SB 893[11], Illinois's Consumer Privacy Act[12], and Texas's HB 374113, however, would not grant private rights of action and limit enforcement to the state attorneys general.

Opt-out vs. opt-in consent

State privacy proposals also differ with respect to the choices consumers can exercise over the processing of personal information. While the three state laws that have passed thus far – California's CCPA and CPRA and Virginia's CDPA — primarily provide consumers with the ability to opt out of certain processing of personal information, Virginia's CDPA also requires covered entities to obtain opt-in consent from consumers for the collection or processing of certain sensitive categories of personal data, such as racial origin or citizenship status.

Other proposed state privacy bills also take divergent approaches. For example, the Massachusetts Information Privacy Act would require that businesses obtain opt-in consent from individuals before processing personal information. New York's Digital Fairness Act would similarly mandate that covered entities collect the "freely given, specific, informed, and unambiguous opt-in consent from an individual" before processing or making any changes in the processing of that individual's personal data. However, two other proposed New York bills and bills in Colorado, Connecticut, and Illinois would all require opt-out consent.

Privacy risk assessments and disclosure requirements

Whether state privacy laws require businesses to conduct privacy risk assessments is a third way in which these laws differ from one other. Although California's CCPA did not include a requirement to complete privacy risk assessments, the CPRA does include such an obligation. Virginia's CDPA also requires businesses to conduct mandatory data protection assessments and determine the risk associated with certain types of processing activities that present a heightened risk.

Bills considered in Colorado, Connecticut, and Illinois would also require businesses to perform certain risk assessments. However, the New York Digital Fairness Act would require only automated decision system impact assessments, rather than general risk assessments for privacy practices. In contrast, the Massachusetts Information Privacy Act, the New York Privacy Act, New York's SB 567, and the Texas's HB 3741 would not require covered entities to perform data processing risk assessments.

Fiduciary duty

Whether businesses have a fiduciary duty over their processing of personal information is a fourth area in which the state proposals take different approaches. While the California and Virginia laws do not impose any new fiduciary duties on businesses, the New York Privacy Act — if enacted — would create a new fiduciary duty to guard against privacy risk. This obligation, which is similar to the proposed federal Data Care Act, would prohibit businesses from disclosing personal data except as consistent with the duties of care or loyalty.

State influence on federal legislation

An important factor affecting whether Congress will pass a federal privacy law is whether the states enact privacy laws that impose divergent or conflicting obligations. As demonstrated by the various differences in the state proposals highlighted above, a tangled maze of state law requirements could easily emerge for businesses that operate their brick-and-mortar businesses or offer their websites and services across state lines, if more states enact privacy legislation. This could motivate support for a single, federal privacy standard.

Furthermore, the state laws also could influence the timing of federal action. Both the California CPRA and the Virginia CDPA go into effect 1 January 2023, potentially motivating congressional action before then.

Given how influential state action could be on passage of federal privacy legislation, businesses should continue to monitor developments in the states over the next 18 months.

AUTHORS

Lindsey Tonsager is Partner at Covington & Burling LLP in California, and Tian Kisch is a summer associate at the same firm.
Email: ltonsager@cov.com

