THOMPSON COBURN LLP

insights

TYPES NOT MAPPED YET December 23, 2019 | TTR not mapped yet | Luke Sosnicki

Proposed federal privacy bills exceed even California's CCPA requirements in some respects

On November 26, 2019, Senator Maria Cantwell (D-WA) revealed a new federal online privacy bill that highlights some of the key privacy and data security issues that Congress may start tackling next year. The law, titled the Consumer Online Privacy Rights Act (COPRA), borrows several key concepts from both the forthcoming California Consumer Privacy Act (CCPA) and the even-more-stringent data-privacy proposal that may be appearing next year on California's ballot, the California Privacy Rights and Enforcement Act (CPREA) (which we previously wrote about here).

Three days later, on November 29, 2019, Senator Roger Wicker (R-MS) circulated a Republican proposal, the "United States Consumer Data Privacy Act" (CDPA). Senator Wicker's CDPA also borrows many of the CCPA's key concepts, including the rights granted to consumers over their data and the obligations on companies to inform consumers of these rights.

While the two federal bills share much in common, there are key differences as well. These differences include whether a federal privacy bill will be privately-actionable and whether it will preempt state-level privacy laws. Senator Cantwell's COPRA is privately-actionable. Senator Wicker's CDPA is not. Senator Cantwell's COPRA would preempt state laws only to the extent these laws directly conflict with COPRA, and offering a "greater level of protection" would not be deemed a conflict. Senator Wicker's CDPA would preempt any state laws related to data privacy or security (other than breach-notification laws). Although there are other differences, these two points are expected to dominate next year's debate.

COPRA (Senator Cantwell's bill)

Most of the key rights that Senator Cantwell's COPRA grants to consumers with respect to their personal information mirror the CCPA's. Like the CCPA, COPRA grants consumers rights to access their information, to transparency, to opt out of transfers and to delete information.

Senator Cantwell's COPRA also borrows from California's 2020 initiative, CPREA, the concept of a special category of "sensitive data" that covered businesses must treat with even more care (notably, COPRA requires opt-in consent for the transfer of such information by a business). COPRA's definition of "sensitive data" is even broader than CPREA's, however, and includes such things as e-mail addresses, telephone numbers and account logon credentials (in addition to Social Security numbers, passport and driver's license numbers, information relating to physical or mental health, financial information, biometric information, geolocation information, and information revealing race, ethnicity, national origin or sexual orientation).

Senator Cantwell's COPRA also borrows from CPREA a specific right to correct inaccuracies in the consumer data that businesses maintain.

The statutes' definitions of a covered business are also similar. Senator Cantwell's COPRA applies to entities with more than $25 million in revenue, or that process more than 100,000 consumer records annually, or that derive more than 50% their income from the sale of consumer information. The $25 million and 50% thresholds are identical to both the CCPA's and CPREA's. COPRA also has adopted the 100,000-record figure from CPREA (the CCPA's cut-off is 50,000).

While Senator Cantwell's COPRA borrows heavily from California's forthcoming and proposed laws, COPRA also exceeds both in many respects. For example, it imposes a "duty of loyalty" that prohibits "deceptive" and "harmful" data practices, and that specifically incorporates relevant definitions from the Federal Trade Commission Act. It

also prohibits discriminatory practices relating to data processing and transfers, requires impact assessments of algorithmic decision-making, grants a right to data minimization, and provides specific protections for whistleblowers.

COPRA further imposes certain data-security requirements—including those relating to vulnerability assessments, information retention and disposal, and training—that companies are "at a minimum" required to adopt.

CDPA (Senator Wicker's bill)

Senator Wicker's CDPA also shares many key concepts with Senator Cantwell's COPRA. The CDPA adopts the same criteria for a covered business—i.e. $25 million in revenue, 100,000 records or more than 50% of income from the sale of consumer data—although it still imposes an obligation on small businesses to seek opt-in consent to sell sensitive consumer information. Senator Wicker's CDPA also grants consumers similar rights of access, correction, deletion, as well as the right to be free from discrimination for exercising other rights.

Senator Wicker's CDPA, like COPRA, also imposes additional requirements on companies that California's CCPA does not. For example, the CDPA requires covered companies to seek affirmative opt-in consent before sensitive information can be sold, to designate a privacy officer and data security officer, and to adopt internal controls that ensure appropriate senior management is involved in CDPA compliance.

Enforcement and preemption under COPRA and the CDPA

Two key areas where Senator Cantwell's COPRA and Senator Wicker's CDPA diverge relate to the methods of enforcement and to preemption of state privacy laws.

Both COPRA and the CDPA are enforceable by the Federal Trade Commission and state Attorneys General. Senator Cantwell's COPRA is also privately-actionable **in its entirety**. Even the CCPA is only actionable by consumers whose data has been breached. COPRA goes one step beyond, providing that **any** violation of the statute—including very technical provisions—could result in a private lawsuit with statutory damages. Senator Wicker' CDPA, conversely, does not include a private right of action at all.

As to preemption, COPRA would preempt state laws only to the extent they directly conflict with it. A "greater level of protection" offered by a state statute would not be a conflict. CDPA, on the other hand, would preempt any state laws related to data privacy or security (other than breach-notification laws).

It remains to be seen whether either bill will advance. Even though Republicans and Democrats agree on most points, it is possible (if not likely) that disagreement as to a private right of action and preemption will suffice to stall both bills. Furthermore, multiple committees on both sides of the Hill have previously asserted jurisdiction over bills relating to privacy and cybersecurity, creating a long potential road to passage that could involve several hearings and committee votes. Until some resolution is reached, the only certainty is that states will continue to fill in the gaps.

authorsTest

luke

Luke Sosnicki