BCLP. Client Intelligent

Insights

COMPARISON OF THE CCPA & CPRA WITH PENDING 2021 COMPREHENSIVE FEDERAL PRIVACY LEGISLATION – S. 1494

Jan 20, 2022

In the last year, we continued to see a shift in the privacy landscape of the United States, including the passage of comprehensive privacy legislation in both Virginia and Colorado, while other states still have bills under consideration. At the federal level, dozens of privacy-related bills have been proposed in Congress. These bills variously seek to address contact tracing, amendments to COPPA, financial privacy, social media privacy, and biometric surveillance by the federal government. Several comprehensive federal privacy bills have also been introduced into the 117th Congress. In this article series, we look back at the comprehensive federal bills proposed in the last year and compare their provisions to those of the current California Consumer Privacy Act ("CCPA") and the California Privacy Rights Act ("CPRA"), which goes into effect on January 1, 2023. See our previous article in this series on H.R. 1816 here.

Consumer Data Privacy and Security Act of 2021 (S. 1494)

S. 1494, or the Consumer Data Privacy and Security Act of 2021, was introduced by Senator Jerry Moran of Kansas on April 29, 2021 and has been referred to the Senate Committee on Commerce, Science, and Transportation. As of this writing, there are no other co-sponsors and no other actions have been taken.

The proposed law requires that a "covered entity…not collect or process personal data of an individual unless" (1) the covered entity has obtained explicit or implicit consent to process the data for a specific purpose, or (2) the collection is done "in accordance with a permissible purpose" under the proposed statute. Explicit consent – obtained for the processing of sensitive personal data (addressed below) and certain other disclosures – requires an unmistakable, affirmative action. Implicit consent, of course, does not require affirmative action – consent is implied if, after being provided with notice and a reasonable amount of time to respond, the individual fails to decline the relevant request. A covered entity, like a "Business" under the CCPA and CPRA (or a "controller" under the GDPR), is an entity that "determines the purpose and means of collecting or processing personal data." However, unlike the various thresholds in the CCPA or CPRA, a covered entity here is either an entity subject to the FTC Act, subject to the Communications Act of 1934, or a non-profit

organization. Note that “covered entity” does not include service providers (which are addressed below). Similar to both the CCPA and CPRA, personal data is “information that identifies or is linked or reasonably linkable to a specific individual.” Information is linked or reasonably linkable to an individual if that information can be used to identify the individual, including device-related identifiers like IP address. “Personal data” includes exclusions like those found in the CCPA, including employee data, publicly available information, and de-identified data; however, employee data collected in the course of a B2B transaction is not addressed.

As noted above, consent is not always required by the proposed law. A third party (an unaffiliated covered entity) that obtains personal data may collect or process this data without consent if, for example, “the covered entity from whom the third party received the personal data” provided the individual with notice that the data would be disclosed to a third party and the purposes of this disclosure, and the individual has consented to the relevant disclosure or processing. Consent is also not required if the collection or processing of personal data is reasonably necessary and limited to certain enumerated purposes, including provision of services or performance of a contract, compliance with the law, data security, or research.

Also as noted above, express affirmative consent is required to collect or process an individual’s sensitive personal data. Similar to the definition in H.R. 1816 and the CPRA, sensitive personal data includes expected categories of data like unique government identifiers (e.g., SSN), biometric information, the content of certain electronic communications, certain medical and financial information, race, religious beliefs, sexual orientation, precise geolocation data, and other data determined to be sensitive by FTC regulations.[1] There is also a data minimization requirement for sensitive personal data that limits how long a covered entity or service provider can retain this data or maintain it in an identifiable format.

Both implicit and explicit consent require a notice, which must be concise, meaningful, and easy to understand, and must include, similar to the CCPA and CPRA, the types of personal data collected, the purposes for which the data is collected or processed, and how an individual can exercise their rights. These rights include the right to withdraw consent at any time, the right to know (which is similar to the privacy policy requirements under the CCPA and CPRA), and individual control rights like rights of access, portability, accuracy, correction (which is new to the CPRA), and deletion (with limitations).

The bill also requires a comprehensive data security program with reasonable safeguards, depending on the nature and scope of the entity’s activities, the sensitivity of the data, and the risks of a security incident. If certain thresholds are met, the proposed law also requires a privacy officer and a comprehensive privacy program.

Like the CCPA and CPRA, personal data may only be disclosed from a covered entity to a service provider pursuant to a binding contract, and the contract must have purpose restrictions. Service

providers are also, among other things, required to cooperate with covered entities in order for covered entities to respond to rights requests by individuals.

Violations of the proposed law are considered unfair or deceptive trade practices, and enforcement is delegated to the FTC. In recognition of this new authority, the bill expands the FTC workforce by providing for the appointment of at least 440 new staff. State attorneys general may also enforce the proposed law, but there is no private right of action. There is a broad preemption clause that preempts all state privacy and security laws, except the proposed law would not preempt state data breach notification laws – to the extent the state law is not inconsistent with the proposed law. And the proposed law should not affect a number of federal laws like the Health Insurance Portability and Accountability Act ("HIPAA"), the Family Educational Rights and Privacy Act of 1974 ("FERPA"), or the Gramm-Leach-Bliley Act ("GLBA").

Regarding foreign data privacy laws, the bill directs the Secretary of Commerce, in consultation with the FTC and other relevant agencies, to engage with foreign officials regarding their data privacy regimes and to develop mechanisms to address cross-border transfers of personal data. This, of course, is already ongoing in the GDPR context with the EU-US Privacy Shield 2.0 negotiations.

This article is part of a multi-part series published by BCLP to help companies understand and cope with data security and privacy issues developing within the United States. Please contact any member of the BCLP Data Privacy & Security Team for further discussion.

---

1. The full definition includes the following:

(A) a unique, government-issued identifier, such as a social security number, passport number, driver's license number, or taxpayer identification number; (B) a user name or email address in combination with a password or security question and answer that would permit access to an online account; (C) biometric information of an individual; (D) the content of a wire communication, oral communication, or electronic communication, as those terms are defined in section 2510 of title 18, United States Code, to which the individual is a party, unless the covered entity is the intended recipient of the communication; (E) information that relates to—(i) the past, present, or future diagnosed physical or mental health or condition of an individual; (ii) the provision of health care to an individual; or (iii) the past, present, or future payment for the provision of health care to an individual; (F) a financial account number, debit card number, credit card number, if combined with an access code, password, or credentials that provide access to such an account; (G) the race or ethnicity of the individual; (H) the religious beliefs or affiliation of the individual; (I) the sexual orientation of the individual; (J) the precise geolocation of an individual that is technically derived and that is capable of determining with reasonable specificity the past or present actual physical location of the individual more precisely than a zip code, street, or town or city level; or (K) such other specific categories of personal data as the Commission may define by rule issued in

accordance with section 553 of title 5, United States Code, the collection or processing of which could lead to reasonably foreseeable harm to an individual.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.