BCLP. Client Intelligent

Insights

COMPARISON OF THE CCPA & CPRA WITH PENDING 2021 COMPREHENSIVE FEDERAL PRIVACY LEGISLATION – H.R. 1816

Dec 30, 2021

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.

INFORMATION TRANSPARENCY & PERSONAL DATA CONTROL ACT (H.R. 1816)

H.R. 1816, or the Information Transparency & Personal Data Control Act, was proposed by Representative Suzan K. DelBene of Washington on March 11, 2021 and has been referred to the Subcommittee on Consumer Protection and Commerce. As of this writing, there are twenty Democratic co-sponsors, though there are no Republican co-sponsors, and the U.S. Chamber of Commerce has voiced support for the bill.

The bill – and the regulatory authority it would delegate to the Federal Trade Commission ("FTC") – would apply to controllers, processors, and third parties that collect, transmit, sell, use, etc. the "sensitive personal information"[1] ("SPI") of "persons operating in or persons located in the" United States. Similar to the CCPA, the definition of SPI excludes certain employee personal information and the personal information of employees acting on behalf of their employer during a business-to-business ("B2B") transaction. Recall that the CPRA *will* apply to employee data and B2B transactions.

Like the CCPA and CPRA, privacy notices are generally required for the covered entities. However, if a *controller* seeks to share SPI in a manner inconsistent with their privacy notice, the controller must obtain express, opt-in consent for this disclosure.

This bill has several other important differences from the CCPA and CPRA, including no explicit rights of access, correction, or deletion. The bill does state that the privacy policy must address issues like user access to their SPI, but it is unclear whether access is a user right. The bill also includes a different opt-out right. The opt-out right in California applies to the sale (for the CCPA) or sharing (for the CPRA) of personal information, among other concepts, while the proposed bill's opt-out right applies to "any collection, transmission, storage, processing, selling, sharing, or other use of *non-sensitive personal information*." It is unclear what non-SPI entails beyond information that is not in the list of enumerated SPI categories. The bill requires that processors have contracts with controllers and that processors only process personal data consistent with that contract. Note also that "privacy audits" by an independent third-party are required at least once every two years for entities that collect, transmit, store, etc. SPI, and whether the entity is compliant must be made publicly available. The audit must also be provided to the FTC and, if there are allegations of violations of the law, to a requesting state Attorney General.

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 term "sensitive personal information" means information relating to an identified or identifiable individual that is—(i) financial account numbers; (ii) health information; (iii) genetic data; (iv) any information pertaining to children under 13 years of age; (v) Social Security numbers; (vi) unique government-issued identifiers; (vii) authentication credentials for a financial account, such as a username and password; (viii) precise geolocation information; (ix) content of a personal wire communication, oral communication, or electronic communication such as e-mail or direct messaging with respect to any entity that is not the intended recipient of the communication; (x) call detail records for calls conducted in a personal and not a business capacity; (xi) biometric information; (xii) sexual orientation, gender identity, or intersex status; (xiii) citizenship or immigration status; (xiv) mental or physical health diagnosis; (xv) religious beliefs; or (xvi) web browsing history, application usage history, and the functional equivalent of either that is data described in this subparagraph that is not aggregated data. De-identified and publicly available information are excluded from this definition.

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

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and 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.

© 2025 Bryan Cave Leighton Paisner LLP.