BCLP. Client Intelligent

Insights

COMPARISON OF THE CCPA & CPRA WITH PENDING 2021 COMPREHENSIVE FEDERAL PRIVACY LEGISLATION – S. 2134

Mar 08, 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 other articles in this series: H.R. 1816 here and S. 1494 here.

Data Protection Act of 2021 (S. 2134)

S. 2134, or the Data Protection Act of 2021, was introduced by Senator Kirsten E. Gillibrand of New York on June 17, 2021, and is co-sponsored by Senator Sherrod Brown of Ohio. The bill 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, though a number of advocacy groups and privacy experts have endorsed the bill.

Similar to the CPRA's creation of a new state privacy agency, the proposed law addresses the creation of a new federal agency, the Data Protection Agency ("DPA"), to regulate the collection and processing of personal data. The bill addresses director appointments and other personnel issues, as well as the structure of the Agency, enforcement of the proposed law, and funding for the Agency. According to Senator Gillibrand, the Agency would have three core missions:

1. Give Americans control and protection over their own data by authorizing the DPA to create and enforce data protection rules.

2. Maintain the most innovative, successful tech sector in the world by ensuring fair competition within the digital marketplace.

3. Prepare the American government for the digital age.

To that end, the Agency would have authority to develop and enforce regulations that are "necessary or appropriate" given "the purposes and objectives of" the bill, which include protecting individuals from violations of the proposed law and other federal privacy laws, promoting equal opportunity to the extent it relates to the processing of personal information, overseeing high-risk data practices, "promot[ing] the minimization of collection of personal data for commercial purposes," and addressing certain defined privacy harms.

The bill also provides that the Agency shall issue regulations applicable to data aggregators and their service providers, and the regulations should address high-risk data practices, data processing practices that may cause specific privacy harms or are unfair or deceptive, individual privacy rights, and obligations on data aggregators.[1] "Personal data," similar to the definitions under the CCPA and CPRA, means data that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, household, or device; or could be used to determine that an individual or household is part of a protected class" – exceptions to this definition are not addressed. An individual is any natural person and is not explicitly limited to U.S. residents. A high-risk data practice is an action by a data aggregator that involves, among other things, the use of an automated decision system, the processing of particular sensitive data, large-scale profiling (which is addressed in the CPRA), or the use of precise geolocation.[2] A data aggregator is "any person that collects, uses, or shares, in or affecting interstate commerce, an amount of personal data that is not de minimis, as well as entities related to that person by common ownership or corporate control." Beyond "de minimis," there are no thresholds like we see in the CCPA and CPRA.

The bill directs the Agency to promulgate regulations that require rights similar to the CCPA and CPRA, like rights of access and deletion. The bill also provides for a right of correction, which is not included in the CCPA, but is included in the CPRA, and a general right to limit the processing of personal data, though it is unclear what this limit entails.

The prohibited acts in the bill apply to data aggregators and service providers and make unlawful violations of the proposed law, other federal privacy laws, or any regulations passed by the Agency. The bill also penalizes entities for unfair and deceptive trade practices in connection with data processing, certain record-keeping failures, and the re-identification of previously anonymized data.

The bill provides for substantial and detailed enforcement and investigatory powers, including administrative proceedings, judicial review, civil actions brought by the Agency, and penalties for violations, including fines for re-identifying data and enhanced fines for violations involving children under 13. State attorneys general may also enforce the proposed law. Whether there is a private

right of action is not addressed in the bill, though individuals may be able to file complaints with the Agency.

Large data aggregators – data aggregators that meet certain thresholds[3] – may be subject to additional reporting and examination requirements by the Agency, including review of certain mergers.

And finally, the bill only preempts state law to the extent the state laws are inconsistent with the proposed law or any subsequent regulations or agency actions.

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. These obligations include "transparency about business practices, data collection limitations, processing and disclosure limitations, purpose specification and legal basis for processing requirements, accountability requirements, confidentiality and security requirements, and data accuracy requirements."

2. A high-risk data practice is an action by a data aggregator that involves: (A) the use of an automated decision system; (B) the processing of data in a manner that involves an individual's protected class, familial status, lawful source of income, financial status such as the individual's income or assets), veteran status, criminal convictions or arrests, citizenship, past, present, or future physical or mental health or condition, psychological states, or any other factor used as a proxy for identifying any of these characteristics; (C) a systematic processing of publicly accessible data on a large scale; (D) processing involving the use of new technologies, or combinations of technologies, that causes or materially contributes to privacy harm; (E) decisions about an individual's access to a product, service, opportunity, or benefit which is based to any extent on automated decision system processing; (F) any profiling of individuals on a large scale; (G) any processing of biometric information for the purpose of uniquely identifying an individual, with the exception of one-to-one biometric authentication; (H) combining, comparing, or matching personal data obtained from multiple sources; (I) processing which involves an individual's precise geolocation; (J) the processing of personal data of children and teens under 17 or other vulnerable individuals such as the elderly, people with disabilities, and other groups known to be susceptible for exploitation for marketing purposes, profiling, or automated processing; or (K) consumer scoring or other business practices that pertain to the eligibility of an individual, and related terms, rights, benefits, and privileges, for employment (including hiring, firing, promotion, demotion, and compensation), credit, insurance, housing, education, professional certification, or the provision of health care and related services.

3. The data aggregator has an annual gross revenue over $25,000,000 or the data aggregator annually collects, uses, or shares the personal data of 50,000 or more individuals, households, or devices.

RELATED PRACTICE AREAS

- 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

Samual A. Garner

Washington

sam.garner@bclplaw.com
+1 202 508 6039