

House and Senate Release a Bipartisan U.S. Federal Privacy Bill

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

On June 3, 2022, House Energy and Commerce Chair Rep. Frank Pallone (D-NJ), Ranking Member Rep. Cathy McMorris Rodgers (R-WA) and Senate Commerce, Science and Transportation Committee Ranking Member Sen. Roger Wicker (R-MS) released a new comprehensive federal privacy bill, the [American Data Privacy and Protection Act](#) ("ADPPA").

While the ADPPA contains a number of similarities to the Consumer Online Privacy Rights Act ("COPRA"), which was previously introduced in 2019 by Senate Commerce Committee Ranking Member Maria Cantwell (WA), Senators Brian Schatz (HI), Amy Klobuchar (MN) and Ed Markey (MA), the ADPPA also contains some notable differences. We have summarized some of these similarities and differences below. Read our [previous post](#) on the COPRA.

Similar to the COPRA, the ADPPA:

- provides individuals with a number of privacy rights, including rights to access, delete and correct their data, as well as a right of data portability;
- imposes data minimization obligations, requiring covered entities to avoid collecting, processing or transferring data beyond what is reasonably necessary and proportionate;
- requires covered entities to obtain express, affirmative consent to collect, process or transfer "sensitive covered data," which is broadly defined;
- requires covered entities to provide individuals with privacy policies detailing their data collection, processing and transfer activities, and data security practices;
- requires certain covered entities ("large data holders") to annually certify that they maintain reasonable internal controls and reporting structures for compliance with the respective bills and obligations to implement comprehensive privacy and security programs that include training programs, reporting processes and privacy impact assessments;
- prohibits covered entities from collecting, processing or transferring data in a manner that discriminates against individuals; and

-
- requires covered entities to implement and maintain reasonable data security practices, which at a minimum must contain certain prescribed activities such as vulnerability assessments.

Notable differences between the COPRA and the ADPPA include the following:

- The COPRA does not address children's privacy, however, the ADPPA contains a provision devoted to the data protections of children and minors. For example, the ADPPA prohibits covered entities from engaging in targeted advertising to individuals under the age of 17 (provided the covered entity has actual knowledge of the individual's age). The ADPPA also prescribes restrictions on the transfer of data related to minors without affirmative express consent from the individual or the individual's parent or guardian, if the individual is between ages of 13 and 17. The ADPPA will establish a Youth Privacy and Marketing Division at the Federal Trade Commission, responsible for addressing privacy and marketing concerns with respect to children and minors.
- The ADPPA requires covered entities to publicly disclose whether individuals' data is made available to China, Russia, Iran or North Korea. The COPRA does not require this type of disclosure.
- The ADPPA requires certain covered entities ("Third-Party Collecting Entities") to provide clear and conspicuous notice on their websites or mobile applications informing individuals that they are Third-Party Collecting Entities using language required by FTC regulations. The ADPPA requires the FTC to promulgate regulations requiring such entities to allow for auditing of any access to or disclosure of data processed by the entities. Third-Party Collecting Entities that process data of more than 5,000 individuals will be required to register with the FTC on an annual basis, pay a registration fee, and may be at risk of civil fines for failing to comply with these requirements. The COPRA does not contain such a requirement.
- While both bills provide a small business exception, the ADPPA provides a higher revenue threshold, and the small business must meet this threshold for a certain number of years. The ADPPA exempts businesses that for the prior three calendar years had (1) annual revenue of less than \$41 million; (2) did not collect or process the data of more than 100,000 individuals; and (3) did not derive more than 50% of its revenue from transferring personal information.
- Both the ADPPA and COPRA impose a duty of loyalty on covered entities; however, the ADPPA appears to be more prescriptive. The COPRA provides a general prohibition against deceptive and harmful data practices. The ADPPA enumerates specific data practices that are prohibited (e.g., the collection, processing, or transferring of Social Security numbers, except when necessary to facilitate extensions of credit, authentication, or the payment and collection of taxes).
- Under the ADPPA, large data holders that use algorithms, solely or in part, to collect, process or transfer data must conduct and submit annual impact assessments of their algorithms to the FTC. The COPRA requires any covered entity engaging in algorithmic decision-making

(or assist others in algorithmic decision-making) for certain activities, such as determining eligibility for housing, education, employment or credit opportunities, must conduct annual impact assessments and make these assessments available to the FTC upon request.

- The ADPPA proposes that the FTC conduct a study to determine the feasibility on the creation of a unified opt-out mechanism and if the FTC finds that a centralized mechanism would be feasible, it must promulgate regulations establishing such mechanisms for covered entities. The COPRA does not contain such a proposal.
- The COPRA provides whistleblower protections that prohibit a wide range of retaliatory acts against whistleblowers for reporting violations of COPRA and grants whistleblowers a private right of action. The ADPPA does not address whistleblowers.
- The COPRA preempts state laws that “directly conflict” with the COPRA and specifies that a state law that provides greater protection is not in conflict. The ADPPA preempts state laws covered by the provisions of the ADPPA; however, a number of exceptions are enumerated, including consumer protection laws of general applicability, laws that solely address facial recognition or facial recognition technologies, electronic surveillance, wiretapping or telephone monitoring, Illinois’ Biometric Information Privacy Act and the limited privacy right of action for certain security breach damages under the California Consumer Privacy Act and California Privacy Rights Act.
- Both the COPRA and ADPPA grant individuals a private right of action; however, there are a number of restrictions with respect to this right under the ADPPA that may ultimately serve as a deterrent. For example, the right is not accessible to individuals under the ADPPA until four years after the Act takes effect. The ADPPA does not permit statutory damages; instead, individuals are only permitted to seek injunctive or declaratory relief, compensatory damages and reasonable attorneys’ fees and litigation costs. Also, to bring an action, individuals must notify the FTC and the attorney general of their state of residence prior to bringing suit. These regulators subsequently have 60 days to determine whether they will independently seek to take action. Demand for monetary payments sent to the covered entity prior or after these regulators determine to take action will be considered made in bad faith and unlawful.

On June 14, 2022, the House Energy and Commerce Committee held a hearing to discuss the ADPPA.

Copyright © 2024, Hunton Andrews Kurth LLP. All Rights Reserved.

National Law Review, Volumess XII, Number 166

Source URL: <https://www.natlawreview.com/article/house-and-senate-release-bipartisan-us-federal-privacy-bill>