CLIENT ALERTS & INSIGHTS

Proposed Federal Data Protection Law Amended and Advanced for a Full Chamber Vote in the House

JULY 26, 2022

While progress has been made in finalizing the text—language around state law preemption and the creation of a small business exception—passage remains unlikely as key-Democrats continue to withhold support and mid-term elections right around the corner.

The House Committee on Energy & Commerce recently voted 53-2 to advance an amended version of the American Data Privacy and Protection Act ("**ADPPA**") to full House consideration. This vote marks the first time an omnibus federal privacy bill will be available for a full chamber vote by both the House and the Senate.

Scope and Applicability

While the amendments expand on or add different exemptions or exceptions, the ADPPA, as currently proposed, would regulate an entity if they are a "covered entity" that collects and/or uses "covered data."

A "covered entity" includes any entity or person that collects, processes, or transfers covered data, and that meets one of the following: (1) is subject to the Federal Trade Commission Act; (2) is a common carrier under the Communications Act; or (3) is a non-profit. The covered entity status flows through to any affiliated or related (i.e., using common branding) entities of a covered entity.

This definition casts a wide net and includes any businesses partaking in "commerce" within the U.S. by making reference to the FTC, calls explicitly out those businesses that transport goods of people, and also goes further than state data protection laws by including non-profits in the scope of the ADPPA.

Accordingly, "covered data" is broadly defined to include any information that identifies or is linked or is reasonably linkable to an individual or a device that identifies or is linked or is reasonably linkable to one or more persons; including any data derived from any such information and any unique identifiers created from such information. This last category of covered data-"unique identifiers"-is broad enough to include IP addresses, cookies, targeted advertising identifiers, and other sorts of tracking technologies that some third party service providers might insist are "non-identifying" but that are otherwise considered identifying under the ADPPA, and also already considered personal data under existing state and international laws.

Approved Amendments

This broad definition largely tracks with the broad definitions of "personal data" and "personal information" that businesses have grown accustomed to under the GDPR and U.S. state laws.

Several amendments to the ADPPA came via an amendment in the nature of a substitute

submitted by Energy & Commerce Committee Chair Rep. Frank Pallone, D-N.J. Other committee members offered additional bi-partisan amendments which were largely passed on voice votes.

Some of the most important amendments to the proposed ADPPA include:

- Express inclusion of the California Privacy Protection Agency as a State Privacy Authority that can enforce the ADPPA in California.
- Changing the private right of action's effective date from four years to two years post-adoption, meaning qualifying businesses could now be sued two years after the ADPPA's effective date instead of four years.
- Addition of a small business exemption, making businesses no longer subject to a private right of action if they **(1)** have an annual revenue less than $25 million, **(2)** that engage with the covered data from less than 50,000 individuals, and **(3)** earn less than half their revenue from transferring covered data would.
- Significant expansion of the employee data carveout through expanding the definition of "employee data". As currently drafted, "employee data" now includes data related to job applicants, business contact information, emergency contact information, and information related to an employee (including information about an employee's spouse or other covered family members).
- Inclusion of a tiered approach as to what "actual knowledge" that an individual is under 17 means for companies of varying sizes, as the ADPPA bans targeted ads to children and treats all information relating to minors as sensitive data.
- Technical changes to the definition of "covered entity" and "service provider" to exclude the National Center for Missing and Exploited Children ("**National Center**") to ensure the National Center can collect, process, and transfer data for its work on child trafficking, abuse, and abduction.

Rep. Anna Eshoo, D-CA proposed an amendment that would have modified the ADPPA's preemption provision to allow states to create stricter laws. The amendment would have made the ADPPA similar to the Gramm-Leech-Bliley Act ("**GLBA**")-which places certain data protection requirements on financial institutions. The GLBA sets the floor / minimum requirements financial institutions must meet to protect consumer personal information. However, the GLBA also allows states to impose stricter or enhanced requirements. This is the case for New York, which imposes additional requirements on New York-based financial institutions through the New York Cybersecurity Regulation.

The proposed amendment would have accomplished the same goal, allowing stricter data protection laws (including the entire soon-to-be-effective California Privacy Rights Act) to also apply. This amendment did not pass, however, after receiving a vote of 8-48.

Outlook

Several California representatives voiced concerns about the ADPPA undermining protections available under the California Consumer Privacy Act and the California Privacy Rights Act. Other representatives expressed they voted in support of advancing the bill but would not support the bill on a floor vote without further modifications.

The road to passage of the ADPPA is still murky with midterm elections fast approaching in November, the House starting its August recess at 3:00 p.m. on July 29, 2022, and a continued lack of support from Senate Democrats.

However, analyzing the proposed ADPPA and the debate process gives valuable insight into (1) the areas of data protection the federal government will focus on (i.e., data minimization and consumer rights), (2) how broad of a scope any such law may have, (3) how such a federal law would deal with inconsistent state law (i.e., preemption), and (4) how the federal government would enforce such a law (i.e., through the FTC, state attorney generals, and a limited private right of action).

As the federal government beings drafting laws, regulations, and guidance that continue to regulate data protection along with several U.S. state laws, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.

Megan Parker, Summer Associate, at mparker@beneschlaw.com or 216.363.6128.