Reuters Legal News

Federal data privacy legislation: Differences with state laws raise preemption issues

By Gary Kibel, Esq., and Emily Catron, Esq., Davis+Gilbert LLP

AUGUST 10, 2022

For over two years now businesses have been dealing with the complexities of compliance with the California Consumer Privacy Act (CCPA); the nation's first comprehensive consumer privacy law. Compliance became more complex with the enactment of comprehensive consumer privacy laws in Virginia, Colorado, Utah and Connecticut, plus the new California Privacy Rights Act (CPRA), a/k/a CCPA 2.0.

The ADPPA in its current form would preempt most, but not all, state privacy and data protection laws. Preemption had been one of the bigger stumbling blocks to getting a federal privacy law enacted.

As a result, industry has been screaming for one, consistent federal standard. Congress may finally be answering the call with the introduction of the American Data Privacy Protection Act, H.R. 8152, (ADPPA). The ADPPA in its current form would preempt most, but not all, state privacy and data protection laws.

Preemption had been one of the bigger stumbling blocks to getting a federal privacy law enacted. Whether a federal law would be treated as a floor or a ceiling divided lawmakers, industry and privacy advocates alike. Despite the progress seen by the ADPPA in the current Congress, this preemption debate is not over as the California delegation in Congress is objecting to any bill that would preempt California law. This article highlights many of the key differences between the ADPPA, on the one hand, and current state privacy laws, on the other.

Who is covered?

The ADPPA applies to entities that process "Covered Data" and are subject to the Federal Trade Commission Act (FTC Act), are common carriers, or are nonprofits. Covered Data is any "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers." This definition covers data more than the privacy laws of Connecticut, Colorado, Utah, Connecticut, and, arguably, California.

ADPPA's relationship to state and federal privacy laws

Interaction with state privacy laws

The ADPPA preempts the majority of state or local laws, invalidating any similar provisions enacted under state law. Specifically, the ADPPA states "No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, standard, requirement, or other provision having the force and effect of law of any State, or political subdivision of a State, covered by the provisions of this Act, or a rule, regulation, or requirement promulgated under this Act."

However, the ADPPA does not preempt all state privacy laws, such as the Illinois Biometric Information Privacy Act (BIPA).

Notably, the Connecticut, Colorado, Utah, and Virginia privacy and data protection laws are subject to the ADPPA's preemption provision. The result of this strange preemption landscape is a continuation of the patchwork of multiple, non-comprehensive privacy and data protection laws that exists today. For example, many businesses would need to separately comply with the differing requirements of the ADPPA and certain state privacy laws.

Interaction with other federal laws

The ADPPA also contemplates the impact on other federal privacy laws. Under the ADPPA, "covered entities" (a type of organization subject to the ADPPA) that must comply with the privacy obligations contained within the Gramm-Leach Bliley Act (GLBA), the Health Information Technology for Economic and Clinical Health Act, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act (FERPA), the Social Security Act, and the Health Insurance Portability and Accountability Act (HIPAA) regulations are deemed in compliance with the ADPPA if they are compliant with these applicable federal privacy laws.

Key differences between the ADPPA and state privacy laws

Large data holders

The ADPPA provides special requirements for Large Data Holders, or covered entities with over $250 million in gross annual revenue

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

that process Covered Data of more than five million individuals, or Sensitive Data of 200,000 individuals, annually. Large Data Holders must submit annual certifications of compliance and conduct audits and impact assessments, among other requirements.

Compared to the state privacy laws, the ADPPA uniquely requires Large Data Holders that use algorithms that may cause potential harm to an individual to collect, process, or transfer Covered Data to conduct an algorithm impact assessment.

While each of the five state privacy laws contain strengthened protections for sensitive categories of data, the ADPPA's definition of "Sensitive Data" varies from the state law definitions.

Among other requirements, these assessments must provide detailed descriptions of design processes and algorithm methodologies, detailed descriptions of the data and outputs involved, statements on the algorithms' purposes and capabilities, and necessity and proportionality assessments. If the ADPPA is enacted, algorithm impact assessments will become a significant new requirement for impacted organizations.

Protections for sensitive data

While each of the five state privacy laws contains strengthened protections for sensitive categories of data, the ADPPA's definition of "Sensitive Data" varies from the state law definitions. The ADPPA follows state privacy law by including within its categories of sensitive data race, ethnicity, religion, health data, genetic data, biometric data, precise geolocation, and children's data.

Like California law, the ADPPA also includes government identifiers, union membership information, and financial account numbers, while adding information about individuals' income level or bank balances. The ADPPA further exceeds current state law protections by including login credentials and security codes for any account or device within its definition of Sensitive Data.

Most significantly, the ADPPA may require the consent of a user to use their internet search or browsing history for purposes of targeted advertising.

Children's data

The ADPPA offers significant departure from state privacy law with respect to its treatment of children's data. The ADPPA defines children as anyone under age 17, whereas state privacy laws apply to children under either 13 or 16. The ADPPA prohibits targeted advertising to anyone "known" to be a child and prohibits the transfer of children's data without parental consent.

Compliance programs and privacy and security officers

The newly proposed federal law requires covered entities and service providers to designate one or more privacy officers and one or more security officers. The ADPPA further requires Large Data Holders to enact compliance programs to manage their data.

Enforcement

The ADPPA calls for the creation of a Bureau of Privacy within the FTC. The ADPPA is enforceable by the FTC, state attorneys general or privacy authorities, and private citizens, although private rights of action are prohibited within the first two years following enactment.

The ADPPA requires individuals to inform the covered entity and the FTC or their state attorney general of their intent to bring an action under the ADPPA. The ADPPA preserves the private right of action under California privacy law for data breached of non-encrypted and non-redacted personal information.

Conclusion

Despite the desperate need for a comprehensive federal consumer privacy law, enactment of the ADPPA is still up in the air. The combination of objections from the California delegation, the lack of support from a key Senator in the Senate and the shrinking number of days left in the 117th Congress make enactment of the ADPPA a significant challenge.

Gary Kibel is a regular contributing columnist on data privacy for Reuters Legal News and Westlaw Today.

About the authors

Gary Kibel (L) is a partner at **Davis+Gilbert LLP**, where he is a member of the Privacy + Data Security and Advertising + Marketing practice groups. He provides clients perspective on cutting-edge issues in digital media, advertising, technology and privacy. He is based in New York and can be reached at gkibel@dglaw.com. **Emily Catron** (R) is an associate at the firm, where she is a member of the Privacy + Data Security and Advertising + Marketing practice groups. She is based in New York and can be reached at ecatron@dglaw.com.

This article was first published on Reuters Legal News and Westlaw Today on August 10, 2022.