One Privacy Law to Rule them All?

Related Professionals

Marcel C. Duhamel

Christopher L. Ingram

John L. Landolfi

Christopher A. LaRocco

Gretchen Rutz Leist

Related Services

Data Strategy, Privacy and Security

Related Industries

Financial Institutions

Retail and Consumer Products

CLIENT ALERT | 6.10.2022

Last week, the U.S. House and Senate released a discussion draft of the American Data Privacy and Protection Act (ADPPA). This is the first bipartisan data privacy bill released at the federal level. The introduction of the ADPPA comes in the wake of a profusion of comprehensive state data privacy laws passed and considered over the last few months. To date, five states have passed comprehensive privacy laws, including Connecticut just last month. If passed, the ADPPA would largely preempt state privacy laws, with some narrow exceptions.

Scope of the ADPPA

If passed, the ADPPA would have broad applicability, covering all companies subject to the Federal Trade Commission Act, as well as non-profits, common carriers, and any entity under common control or that shares common branding with another covered entity, and that collect, process, or transfer "covered data." Small businesses, falling below a certain revenue and data processing threshold, would be exempt from compliance with certain provisions of the ADPPA.

Enforcement of the ADPPA

The ADPPA would give exclusive rulemaking authority to the Federal Trade Commission (FTC), but would allow enforcement by the FTC or state attorneys general. In what could be an industry-changing development, the bill also includes a private right of action that would allow individuals or classes to file civil suits in federal court. The private right of action would only apply after a four-year grace period, but after that period it would allow plaintiffs to recover compensatory damages, injunctive or declaratory relief, and attorney's fees stemming from violations. Punitive damages and statutory damages are not available. The draft includes some substantial guardrails on the private right of action including: (1) giving the FTC and/or state AG the right of first refusal on any case; and (2) a right to cure violations within 45 days for small businesses or for cases seeking injunctive relief.

Definition of "Covered Data"

The term "covered data" replaces the more-familiar "personal information" or "personal data" from existing privacy laws. Like those laws, this term is defined broadly to include all "information that identifies or is linked or reasonably linkable to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals." "Covered data" includes derived data and unique identifiers, but does not include de-identified data, employee data, or publicly available information.

Preemption of State Privacy Laws

The ADPPA would largely preempt existing comprehensive state privacy laws. One notable exception is that the limited private right of action under the CCPA (California) for data breaches would not be preempted. Similarly, the ADPPA would also not preempt state laws such as BIPA (Illinois) or any other laws on facial recognition, state security breach notification laws, student privacy laws, or civil rights laws.

Affirmative Consent and Opt-Out Rights

Similar to state privacy laws, the ADPPA requires affirmative consent from an individual before collecting, processing, or transferring their sensitive data (e.g., biometric data). For non-sensitive data, individuals have the right to opt out of the transfer of their covered data to a third party. However, the covered data of children age 13-17 is subject to additional restrictions.

Privacy Policy Requirements

As with its predecessors, the ADPPA requires that companies post a comprehensive privacy policy. Going further than the adopted state privacy laws, the ADPPA requires that the privacy policy must list all service providers or third parties to which the company transfers covered data. The privacy policy also must be available in each language that the company conducts its business.

Executive Accountability

Under the ADPPA, companies must designate a privacy officer and a data security officer. For companies who have more than $250 million in annual gross revenue, have covered data of more than 5 million individuals, or have the sensitive covered data of more than 1 million individuals, the CEO, privacy officer, and data security officer of such company must annually certify that the company maintains reasonable internal controls to comply with the ADPPA and reporting structures to ensure that the certifying officers are involved in any decisions that impact compliance with the ADPPA.

In what has already been a busy year for privacy, the introduction of the ADPPA could prove to be the most substantial development yet. If you would like to read the full text of the proposed ADPPA bill, it can be accessed here. For more information about the ADPPA or privacy laws in general, please contact John Landolfi, Christopher Ingram, Christopher LaRocco, Gretchen Rutz, or your Vorys attorney.