NOW + NEXT

PRIVACY LAW ALERT | NIXON PEABODY LLP

NOVEMBER 27, 2019

A federal privacy law: What you need to know

By Jenny L. Holmes and Tevin Hopkins

On Tuesday, November 26, U.S. Senator Maria Cantwell, D-Wash., introduced the Consumer Online Privacy Rights Act (COPRA), a federal privacy bill that to some, seems long overdue. Following the passing of the General Data Protection Regulation (GDPR) in the European Union, the United States' privacy scheme has been in a race to catch up to the expansive individual consumer rights granted to individuals in the European Union and to provide oversight on companies who collect and process personal information. The California Consumer Privacy Act (CCPA), effective January 1, 2020, is seen as a response to the GDPR. Many states are currently drafting their own privacy laws, creating a patchwork of various obligations for multi-state companies. COPRA aims to "provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement" while also creating some semblance of order within the tangle of United States' privacy laws.

Here's what we know so far:

- COPRA covers all entities (both business and individuals) subject to the Federal Trade Commission Act (FTCA). This includes organizations engaged in commerce but likely excludes most nonprofits, certain financial institutions, and telecommunication common carrier activities. Like the CCPA, COPRA establishes a threshold that may provide relief for smaller businesses. Entities with revenue less than $25 million per year, processing covered data of fewer than 100,000 individuals, households, or devices, and deriving less than 50% of their revenue from transferring covered data for valuable consideration are excluded. There is also an exemption for entities subject to other federal sectoral privacy laws, such as the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, and the Gramm-Leach-Bliley Act.
- COPRA applies to information that identifies or is reasonably linkable to an individual residing in the United States or a consumer device.
- Like we've seen in the GDPR and the CCPA, COPRA provides certain privacy rights to individuals, including (i) consent for data processing, (ii) access to personal data in a portable format, (iii) correction and deletion of data, (iv) transparency, (v) data minimization, and (vi) data security.

- COPRA provides individuals the right to opt-out of the transfer of their covered data for "valuable consideration."

How is COPRA different from the other privacy laws?

- Covered entities that annually process personal data of more than five-million individuals, devices, or households or the sensitive data of more than 100,000 individuals, devices, or households, would be required to annually attest compliance to the Federal Trade Commission (FTC).
- COPRA requires entities engaged in algorithmic decision-making to conduct an annual impact assessment for accuracy, fairness, bias, and discrimination.
- COPRA introduces a "duty of loyalty" prohibiting covered entities from engaging in deceptive or harmful practices.
- The FTC and the National Institute of Standards and Technology (NIST) would be responsible for creating training guidelines for companies to implement concerning privacy training for all employees. Along the same lines, COPRA would mandate the appointment of qualified privacy and security officers and charge them with implementing and maintaining privacy compliance programs and conducting annual privacy and security risk assessments.

How would COPRA be enforced?

- COPRA would grant enforcement power to the FTC and state attorneys general.
- Damages for violations would range from $100 to $1,000 per violation per day and include attorney's fees and equitable relief.
- COPRA includes a private right of action.
- COPRA would establish a new bureau within the FTC and would create a new Data Privacy and Security Relief Fund in which the FTC and state attorneys general would deposit recovered funds to be used for redress, compensation to affected individuals, and other privacy initiatives.

While it is unlikely that any of the substantive provisions of COPRA would be controversial (except, of course, for the private right of action), we expect COPRA to face challenges as it preempts state laws that conflict with COPRA and encroaches a space typically left to the states to regulate. States may, however, enact non-conflicting privacy laws that have more onerous requirements.

COPRA still has a long way road ahead of it. It will likely be discussed on December 4 at a Senate Committee hearing. We will follow COPRA and keep you informed.

For more information, please contact your Nixon Peabody Data Privacy attorney or:

- Jenny L. Holmes, 585-263-1494, jholmes@nixonpeabody.com
- Jason Gonzalez, 213-629-6019, jgonzalez@nixonpeabody.com