A National Federal Privacy Law? Check Out COPRA, The Most Comprehensive Privacy Bill Introduced Yet

Alyssa Z. Hutnik

December 2, 2019

On November 26, 2019, Senator Maria Cantwell (D-WA) along with other Democratic senators across four key Senate committees introduced the Consumer Online Privacy Right Act ("COPRA"). Per Senator Klobuchar's description, COPRA "*establishes digital rules of the road for companies, ensures that consumers have the right to access and control how their personal data is being used, and gives the Federal Trade Commission and state attorneys general the tools they need to hold big tech companies accountable*."

The bill would empower consumers with control over their personal information, including access, deletion, correction, and portability rights. The bill also would provide the FTC with broader powers to combat privacy harms. Notably, the bill would establish a private right of action for consumers and would *not* preempt more stringent state privacy laws. The following chart highlights key aspects of the Scope, Rules, Exceptions, and Enforcement of the COPRA bill.

Scope & Jurisdiction	COPRA covers all businesses with an average annual revenue over $25 MM (among other requirements), who are subject to the FTC Act and process or transfer information that identifies, or is "reasonably linkable" to an individual or consumer device. COPRA excludes small businesses, non-profit organizations, political campaigns, banks, or other entities not already subject to the FTC's jurisdiction.
Privacy & Data Security Rights	*Duty of Loyalty & Right to Data Security*: Codifies the FTC's interpretation of reasonable privacy and data security standards. Requires businesses to designate privacy and data security officers in charge of ensuring compliance with COPRA. *Right to Access & Transparency*: Incorporates provisions similar to the CCPA right to access data and privacy policy disclosure requirements. *Right to Delete*: Broader than the CCPA in that there are no business purpose exceptions to retain consumer data. If a consumer requests that a business delete covered data, the business must delete the data and inform service providers and third parties of the deletion request. *Right to Correct Inaccuracies*: Businesses must provide a consumer a mechanism to correct inaccurate or incomplete data and must notify service providers and third parties of the correction.

	Right to Controls: Incorporates provisions similar to the CCPA right to opt-out of the sale or transfer of consumer information. The FTC would be responsible for promulgating rules for compliance with this right. *Right to Data Minimization*: Businesses can not process or transfer data unless it is "reasonably necessary, proportionate, and limited" to carry out the specific processing and transfer purposes described in the privacy policy; carry out a specific processing purpose or transfer after a covered entity has obtained affirmative express consent; or for a purpose specifically permitted by the Act.
Civil Rights	Businesses cannot discriminate based on data that differentiates people based on their perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful employment, or disability. Businesses must offer people the same housing, employment, credit, educational opportunity, and public accommodation to every person. Businesses are also required to conduct impact assessments to ensure algorithmic decision-making is not discriminating based on data that may differentiate people using those traits.
Exceptions	Businesses do not need to comply with the Rights above if: • It is demonstrably impossible • It would prevent the business from carrying out internal audits, performing accounting functions, processing refunds, or fulfilling warranty claims • The request is made about publically available information • It would interfere with First Amendment rights • It would impair the privacy rights of another consumer • The request would prevent the business processing the data for a specific purpose that a consumer authorized or the authorization fell under an exemption
Third Parties & Service Providers	Service providers are exempt from several provisions in the Act. However, they must delete, correct, or de-identify data subject to consumers' requests under the Act. Service providers must only use data in the way their contract provides and can't sell data to a third party without affirmative express consent from the business. Third parties cannot process data inconsistent with the expectations of a reasonable consumer. In receiving data, third parties can reasonably rely on the representations of the businesses and service providers. Businesses must conduct reasonable oversight and due diligence on service providers and third party transfers of data.
Private Right of Action	COPRA provides a private right of action for individuals to assert violations. Any violation of the Act, or of a regulation promulgated under it, will be considered an "injury in fact." Damages range from $100 to $1000 per violation per day. Arbitration agreements and class action waivers are invalid in disputes arising under COPRA.

	Within two years, the FTC must create a new bureau to assist in exercising their authority under the Act and other Federal laws addressing privacy, data security, and related issues. A violation of this Act is treated as a violation of the FTC Act. One year after enactment, a CEO (or equivalent) and data privacy officers must review and certify to the FTC that they maintain adequate internal controls and reporting structures to ensure compliance with this Act.
Federal & State Enforcement	Businesses will be required to have a privacy and data security officer, who ensures the business has a comprehensive written privacy and data security program, annually conducts risk assessments and facilitates ongoing compliance with this Act. This Act does not preempt any state laws that afford "a greater level of protection to individuals protected under this Act." It only preempts directly conflicting state laws. The Act does not preempt any other private rights of action but the FTC can intervene in individual enforcement actions under COPRA.

COPRA was introduced in anticipation of the Senate Committee on Commerce, Science, and Transportation December 4th hearings entitled "*Examining Legislative Proposals to Protect Consumer Data Privacy*." While it remains unclear if there will be enough momentum for this bill to advance, the scope and direction of the legislation underscore the change in the privacy law landscape in the US, and that California's CCPA may only be the start. If you have further questions about how these developments may apply to your business, please feel free to contact any of our Privacy team members at Kelley Drye.