MINTZ

California Assembly Passes Sweeping Age-Appropriate Privacy Legislation

September 06, 2022 | Blog | By **Kevin K. Hiraki**, **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

- Privacy & Cybersecurity

RELATED INDUSTRIES

California is leading the way on privacy regulation --- again. The California State Assembly has passed **AB 2273**, which, if approved by the California Governor, would require businesses that provide online services, products, or features likely to be accessed by children or teens under the age of 18 to increase their privacy and safety protections. Although California AB 2273, also known as the California Age-Appropriate Design Code Act, aims to protect children and teens, the bill's requirements could impact a broad range of online businesses and goes beyond the federal **Children's Online Privacy Protection Act, known as COPPA.**.

Among other provisions, the bill would require the following:

- Any business that provides an online service, product, or feature likely to be accessed by children must conduct a "Data Protection Impact Assessment," which must include (if applicable) an assessment of:
  - whether the design of the product, service, or feature could lead to children experiencing or being targeted by harmful contacts,
  - whether algorithms used could harm children,
  - whether targeted advertising could harm children, and
  - whether and how the products, services, or features use systems designed to increase, sustain, or extend usage, including but not limited to automatic playing of media, rewards for time spent, and user notifications.
- Within five days following an Attorney General request, a business must deliver any requested Data Protection Impact Assessment.
- Any business that provides an online service, product, or feature likely to be accessed by children must configure all default privacy settings provided to a child, to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of the child.
- Any business that provides an online service, product, or feature likely to be accessed by children must refrain from using personal information of a child, which the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child.
- Any business that provides an online service, product, or feature likely to be accessed by children must not collect, sell, or share any precise geolocation information of a child by default unless strictly necessary for the business to provide the service, product, or feature requested and if collected, only for the limited time that the collection of geolocation information is necessary to provide the service, product or feature.

The California Age-Appropriate Design Code Act would authorize the California Attorney General to seek injunctive penalties or civil penalties of not more than $2,500 for each affected child in connection with a negligent violation and not more than $7,500 for each affected child in the event of an intentional violation.

If the California Governor signs the bill into law, it would come into effect on July 1, 2024; however, businesses would be wise to consider immediate assessments so they can determine the extent of child and teen usage, the design and systems employed that could leave children and teens exposed, and to ensure all Data Protection Impact Assessments are completed on or before the effective date.

If you have any questions about your Privacy and Cybersecurity compliance program, or need to get one implemented, feel free to contact the **Mintz Privacy Team**.

Authors

Kevin Hiraki

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.