Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

California Senate Approves Landmark California Age-Appropriate Design Code Act

September 6, 2022

On August 29, 2022, the California Senate passed the landmark Assembly Bill 2273, which would enact the California Age-Appropriate Design Code Act (the "**Act**"). If signed into law by Governor Newsom, the Act could have significant implications for businesses that provide online services, products or features "likely to be accessed" by children (i.e., consumers under the age of 18). Modeled on the United Kingdom's Age Appropriate Design Code, the Act would serve as the first piece of legislation in the United States (U.S.) that imposes a number of novel restrictions and data protection obligations on businesses providing services to users under the age of 18, including requirements to conduct a data protection impact assessment before any new services are offered, configure all default privacy settings to a high level of privacy (unless there are compelling reasons to suggest it is otherwise in the best interests of children), and provide an obvious signal to the child when they are being monitored or tracked by their parent, guardian or another consumer. Businesses subject to the Act are expressly prohibited from taking certain actions, including profiling a child by default unless certain criteria are satisfied, using the personal information of any child in a way that is materially detrimental to their well-being and using dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected. The Act, which was unanimously approved by the state Senate by a vote of 33-0, could have broad implications once operative on July 1, 2024, requiring businesses to proactively amend their data management practices. We set out below 10 key features of the Act and the potential implications for businesses.

Background to the Act

Recognizing that children spend more of their time interacting with the online world, lawmakers in California and globally have increasingly focused on the potential impact of online products and services on children's wellbeing in an effort to create a safer online space for children. The Act emphasizes that the best interests of the child should be taken into consideration by all businesses that develop and provide online services, products or features ("**Services**") that children are likely to access and, in the event of a conflict between the businesses' commercial interests and the best interests of children, the privacy and well-being of children must be prioritized.

Contact Information:

If you have questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Rachel Claire Kurzweil
Counsel
rkurzweil@akingump.com
Washington D.C.
+1 202.887.4253

Sahar Abas
Associate
sahar.abas@akingump.com
Dubai
+971 4.317.3052

10 Key Features of the Act

1. Broad Scope of Application: The protections under the Act extend to all "children," defined as consumers under the age of 18, and in respect of online products and services (i) specifically directed at children and (ii) that are "likely to be accessed" by children. The Act clarifies that Services are "likely to be accessed" by children where it is reasonable to expect that it would be accessed by a child based on certain indicators, including whether the product or feature is directed to children, routinely accessed by a significant number of children or if there are design elements that are known to be of interest to children (such as cartoons or music). The application to users below the age of 18 is significant, since the federal Children's Online Privacy Protection Act of 1998 only applies to users below the age of 13 (and is generally focused on online services directed at children).

2. Requirement to Conduct a Data Protection Impact Assessment (DPIA): Prior to any new Services being offered to the public which are likely to be accessed by children, the Act requires that the business complete a DPIA and maintain documentation of this assessment for as long as the Services are likely to be accessed by children. The DPIA must (i) be reviewed biennially and (ii) contain certain prescribed information, including the purpose of the Services, how it uses children's personal information and the risk of material detriment to children that arise from the businesses' data management practices. In the event any risk of material detriment is identified, the business must create a timed plan to mitigate or eliminate such risks prior to the Services being accessed by children. Moreover, within three business days of a request by the Attorney General, a business is required to share a list of all DPIAs conducted, although the DPIA shall be deemed confidential and exempt from public disclosure.

3. High Privacy Default Settings: All default privacy settings provided to children by the Services must be configured to offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.

4. Clear, Age-Appropriate Privacy Information: Any privacy information, terms of service, policies or community standards must be concise, prominently displayed and use clear language suited to the age of children likely to access the Service. Any published terms, policies and standards established by the business must be enforced.

5. Tracking and Geolocation Settings: Any Services allowing a child's parent or guardian (or other consumer) to monitor a child's activity or track their location must be supplemented by an obvious signal to the child when the child is being monitored or tracked. Businesses are prohibited under the Act from (i) collecting, sharing or selling any precise geolocation information about children by default unless such collection is "strictly necessary" and only for a limited time, and (ii) collecting such information without providing an obvious sign to the child for the duration of the collection.

6. Rights and Reporting Tools: Businesses must provide prominent, accessible and responsive tools to help children exercise their rights and report concerns.

7. Data Privacy Restrictions: The Act imposes a number of restrictions on the actions of businesses that provide Services likely to be accessed by children, including stipulating that businesses must not:

- Use the personal information of a child in a way that is materially detrimental to their mental or physical health or wellbeing;
- Profile a child by default unless certain prescribed conditions can be satisfied;
- Collect, sell, share or retain any personal information that is not necessary to provide the Services, unless the business can demonstrate a compelling reason that it is otherwise in the best interests of the child;
- Use personal information for any reason other than the reason for which it was collected if the end user is a child, unless the business can demonstrate a compelling reason that it is otherwise in the best interests of the child; and
- Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected or to take any action that is materially detrimental to the child's wellbeing.

8. Age Assurance: The Act requires businesses to estimate the age of child users with a "reasonable" level of certainty appropriate to the risks that arise from their data management practices or to apply privacy and data protections afforded to children to all of their consumers. Businesses are, however, prohibited from using personal information collected to estimate age for any other purpose or to retain such information longer than necessary to estimate age.

9. Establishment of Working Group: The Act creates the California Children's Data Protection Working Group, which is tasked with delivering a report to the legislature regarding best practices for implementing the Act. The Working Group shall be comprised of members with expertise in areas of children's data privacy and rights and shall take input from a broad range of stakeholders.

10. Penalties and Enforcement: A violation of the Act can result in the California Attorney General seeking an injunction and civil penalty of up to $2,500 per affected child for each negligent violation or up to $7,500 per affected child for each intentional violation. Businesses that substantially comply with the DPIA requirements may, however, benefit from a 90-day cure period. The Act expressly confirms that it does not serve as a basis for a private right of action.

Implications and Next Steps

The Act has now been passed to Governor Newsom for signing. If signed, the Act would go into effect on July 1, 2024. Businesses must complete a DPIA on or before July 1, 2024 for any Services likely to be accessed by children before July 1, 2024.

The Act is one of a number of privacy bills specifically concerning children's data that have been introduced both in California (including Assembly Bill 2486 (the California Rights Act of 2020: Office for the Protection of Children) and Assembly Bill 1545 (the Kids Internet Design and Safety Act)) and at the federal level (including H.R. 4801 (Protecting the Information of our Vulnerable Children and Youth Act, or the Kids PRIVCY Act), and S. 1628 (the Children and Teen's Online Privacy Protection Act)).

Indeed, on August 30, 2022, just one day after the passing of the Act, the California Senate also unanimously passed Assembly Bill 587 ("**AB 587**") which would, if enacted, require certain social media companies to post their terms of service (defined as the policy/policies adopted that specify, at the minimum, the user behavior and activities that are permitted on the internet-based service and the user behavior and activities that may subject a user or item of content to being actioned) for each social media platform owned or operated by the company in a specified manner and with additional prescribed information. AB 587 would also require social media companies to submit reports to the California Attorney General (on a semi-annual basis) by no later than January 1, 2024, specifying, among other things, the current terms of service, the policies in place to address specified categories of content (such as hate speech, misinformation and foreign political interference) and data related to violations of their terms of service; significantly, AB 587 would require the California Attorney General to make all terms of service reports available to the public in a searchable repository online. Violation of AB 587, if enacted, would result in liability for a civil penalty up to $15,000 per violation per day. AB 587 has now also been sent to Governor Newsom for his consideration and signing and may have significant implications for social media companies going forward.

The Act itself is largely modelled on the U.K. Children's Code (the Age Appropriate Design: A Code of Practice for Online Services), which entered into effect in September 2020, and the Act notes that businesses may look to guidance in response to the U.K.'s Children Code when developing Services. However, although a California statute (and expressly stated to further the purposes of the California Privacy Rights Act of 2020), if enacted, the Act could result in service providers introducing nationwide or global changes to their services. Other state legislatures may similarly utilize the Act as a model for the creation of similar protections.

The question of the extent of preemption by the federal Children's Online Privacy Protection Act (COPPA) remains unsettled The scope of COPPA preemption has not been decided by courts, but the Federal Trade Commission, which enforces COPPA, has taken the position that it believes Congress did not intend for COPPA to displace state laws that create additional protections for children above the age of 13. Regardless of preemption, the Act's framework will wield substantial influence as Congress develops federal privacy law and any amendments to COPPA.

The Act has come at a time where there is increasing attention on the potential adverse effects of social media and online platforms on children and the potential exploitation of children's data. Nevertheless, passage of the Act has not been without public debate, particularly amongst those who view the Act as a necessary means to reduce the risks to children online and those who perceive the Act as broadly drafted, burdensome and unclear in certain respects (such as regarding appropriate age verification mechanisms). The Act will likely result in additional compliance obligations for businesses subject to it, not least as it extends broadly to Services *likely* to be accessed by children. In any event, if passed, the Act will have significant implications for businesses offering Services in California and would serve as an historic development in the online privacy sphere.

We continue to monitor developments in this area.

akingump.com