Professional Perspective

Increased U.S. Regulation & Enforcement of Privacy of Minors

Ken D. Kumayama and Brianna M. van Kan, Skadden, Arps, Slate, Meagher & Flom

Bloomberg Law

Increased U.S. Regulation & Enforcement of Privacy of Minors

Contributed by Ken D. Kumayama and Brianna M. van Kan, Skadden, Arps, Slate, Meagher & Flom

The US legal landscape appears to be shifting in favor of more robust regulation of business practices regarding data of children and teens. The shift follows former Facebook employee Frances Haugen's 2021 whistleblower revelations, certain overseas regulatory precedents, and President Joe Biden's entreaties in his State of the Union address in March 2022.

On both federal and state levels, substantial new legislation has been proposed and advanced recently that would expand requirements of online products and services operators with respect to their interactions with youth data. In particular, California's passage of the California Age-Appropriate Design Code Act (CA ADCA), signed into law Sept. 15, 2022, as well as the advancement of two federal children's privacy bills in late July demonstrate the current momentum on this front. Additionally, the comprehensive American Data Privacy Protection Act (ADPPA)–which, although not specifically aimed at youth data privacy, contains certain noteworthy restrictions on the subject–also advanced this summer.

All of the legislative developments discussed here focus on common themes responsive to Biden's call to action, including prohibiting targeted advertising and excessive data collection in relation to children and requiring the design of online products with youth safety in mind. Additionally, all reflect certain key departures from the status quo represented by the Children's Online Privacy Protection Act of 1998 (COPPA), by extending coverage to teenagers and beyond businesses directed specifically at children.

In addition to novel legislation, on Aug. 11, 2022, the Federal Trade Commission (FTC) issued an Advance Notice of Proposed Rulemaking (ANPR) to explore the possible promulgation of a sweeping trade regulation rule on "commercial surveillance" and data security. The commission includes as one of ten headline areas of focus "Harms to Children," posing targeted questions regarding the impact of data practices on children and teens that echo many of the key themes seen across the legislation discussed in this article. Outside of this process, the FTC and certain of its approved safe harbor organizations also have shown movement toward greater enforcement of existing COPPA restrictions.

Below, we provide an overview of these legislative and regulatory developments.

California Age-Appropriate Design Code Act

The CA ADCA, which becomes operative on July 1, 2024, will impose significant privacy-by-design requirements on online services, products, and features "likely to be accessed" by consumers under the age of 18–covering ages that are higher than any other currently enacted child privacy law in the US–in addition to those that are specifically directed to children under COPPA. The "likelihood" in the language of the law may be determined by, among other things, "competent and reliable evidence regarding audience composition," internal company research, or the presence of advertisements marketed to or design elements appealing to children. The CA ADCA would not apply, however, to broadband internet services, telecommunications services, or physical products.

Based in part on the U.K.'s Age Appropriate Design Code, the CA ADCA requires covered businesses to consider and prioritize "the best interests of children" over any conflicting commercial interests in the design and provision of its online products or services. This general requirement is accompanied (subject to limited exceptions) by a variety of specific obligations, including to:

- Configure default privacy settings to a "high level of privacy"
- Refrain from profiling a child by default unless necessary to provide the service and accompanied by appropriate safeguards
- Observe strict data minimization principles
- Prominently present privacy information and policies in age-appropriate language
- Refrain from collecting, selling or sharing geolocation information unless strictly necessary

The CA ADCA additionally prohibits use of so-called "dark patterns" to encourage children to provide personal information beyond what is reasonably expected for provision of the service or otherwise forgo privacy protections. In furtherance of applying these requirements to services, products or features that are likely to be accessed by children, businesses will be required to estimate the ages of child users "with a reasonable level of certainty appropriate to the risks," or otherwise to apply the privacy and data protections afforded to children to all users.

In addition to these design requirements, the CA ADCA will require covered entities to generate Data Protection Impact Assessments for each product, service or feature likely to be accessed by a child prior to public launch, to be reviewed biennially. These assessments, though not public, must be provided to the California attorney general upon request.

Although the CA ADCA prohibits private causes of action, it imposes significant fines for noncompliance (up to $2,500 per affected child for each negligent violation, and $7,500 for each intentional violation) in addition to risk of injunction.

While the CA ADCA is only the regulation of one state, it could in practice become the de facto law of the land for many businesses given the size and prominence of California in online commerce and complexities of state-by-state differentiations. This impact has also allowed California to serve in many instances as a trailblazer, clearing (or at least, thinning) the path for other likeminded states to pursue similar legislation. In New York, for example, a bill was introduced in the state senate a week following the CA ADCA's passage that is modeled in significant part on the California law. Accordingly, the enactment of this law marks a significant shift in the US youth privacy landscape.

Pending National Legislation

COPPA 2.0

On July 27, 2022, the Senate Committee on Commerce, Science and Transportation passed the Children and Teens' Online Privacy Protection Act. This act, sometimes referred to as "COPPA 2.0," would amend COPPA by extending its coverage to "minors" from ages 12 to 16, adding certain new protections and expanding application of the original law not only to online products directed to children and minors, but also to products whose operators have constructive knowledge that they are collecting personal information from children or minors (including where the operator has data or analytics, receives complaints or interacts with ad networks in a manner indicating that such data is being collected).

Among the additional restrictions imposed by COPPA 2.0 would be (1) prohibiting targeted marketing to children (and allowing such marketing to minors only with verifiable consent), (2) requiring operators to provide a mechanism to erase a user's information, (3) establishing a "Digital Marketing Bill of Rights for Minors" that prohibits collection of personal information from minors without adherence to certain data minimization, accuracy, transparency, cybersecurity and retention principles, and (4) requiring that internet-connected devices targeted at children meet certain cybersecurity standards and prominently display certain privacy notices on packaging.

COPPA 2.0 also would establish a Youth Privacy and Marketing Division within the FTC that would be tasked with reporting, on an annual basis, emerging concerns related to youth privacy and marketing practices and assessing how effectively the FTC has addressed such privacy and practices under the law.

Kids Online Safety Act

In addition to COPPA 2.0, the Senate Committee on Commerce, Science and Transportation unanimously advanced the Kids Online Safety Act (KOSA) on July 27, 2022. Whereas COPPA 2.0 focuses on restricting the operation of online services and applications in relation to the processing of youth data, KOSA tracks closer to the CA ADCA, focusing on requiring the very design of such services to address risk of harms to youth posed by processing of personal information.

KOSA would apply to commercial software and electronic services connected to the internet that are reasonably likely to be used by individuals under the age of 17, and, similar to the CA ADCA, would impose an overarching duty on such services to act in the best interests of such minor users, including specifically to prevent and mitigate "the heightened risks of physical, emotional, developmental, or material harms to minors posed by materials on, or engagement with, the platform."

To comply, the covered platform would be required to provide accessible and easy-to-understand:

- Safeguards to control the users' personal information and experience, including options to restrict the ability for others to find or contact the user, restrict public access to their data, limit autoplay or other mechanisms designed to increase or sustain use of the platform, opt out of algorithmic recommendations, delete the user's account and data, and restrict collection of geolocation data
- Parental tools to supervise use by a minor, including the ability to control the minor's privacy settings, track time spent on the platform, and restrict financial transactions (subject to notice to the minors when such controls are in effect)
- Transparency notices, including notices of privacy policies, tools, and heightened risks (with user or parent acknowledgement prior to use of the service), overviews of how algorithmic recommendation systems are used by the service, including the users' options to modify, opt out or down-rank choices, and certain information regarding the origin and basis of serving each ad presented to the user. Similar to the CA ADCA, when a user is known or reasonably believed to be a minor, the strongest privacy settings would have to be in place as a default.

In addition to these design and transparency requirements, each covered platform would be obligated to generate an annual public report (with detailed content requirements) outlining the foreseeable risk of harm to minors using the platform and describing mitigative measures taken by the platform. Further, KOSA would order the creation of a program under which a covered platform would be required to provide eligible researchers access to data assets in order to conduct public interest research regarding harms to minors.

KOSA, which would become effective 18 months after its enactment, would require covered platforms to provide users a mechanism for reporting harm. However, it would not provide for any private cause of action. Instead, KOSA would be enforced by the FTC or state attorneys general.

American Data Privacy Protection Act

A survey of the trend towards heightened regulation of youth privacy in the US is not complete without discussing the ADPPA, which cleared the House of Representatives Energy and Commerce Committee in July 2022. Though not singularly aimed at minors, the ADPPA aims to establish a comprehensive federal data protection regulation that would generally preempt state privacy laws and, if enacted in its current form, would prohibit targeted advertising to children under the age of 17 and require affirmative consent to transfer such children's data to third parties.

Similar to the other proposed legislation discussed in this article, the ADPPA would not require actual knowledge of an individual's age for such restrictions to apply; rather, such determinations would be based on data otherwise collected in the normal course of business.

Protections under the ADPPA would be expressly in addition to, and not in lieu of, those existing under COPPA. Additionally, in overlap with COPPA 2.0, the ADPPA would establish a Youth Privacy and Marketing Division within the FTC that, among other responsibilities, would biennially review the effectiveness of the safe harbor provisions under COPPA and make related policy recommendations.

One of the most notable—and controversial—features of the ADPPA that is distinct from any other legislation discussed in this article is that the proposed legislation would provide a private right of action against covered entities who violate the ADPPA, subject to a notice and cure period and an opportunity for the FTC or applicable state attorneys general to intervene.

The ADPPA still faces many hurdles before becoming law. Speaker Nancy Pelosi hasn't brought the bill to the House floor, stating Sept. 1, 2022 that she has concerns about its preemption over state laws, specifically that it doesn't provide the same protections as existing California laws.

Concerns regarding preemption have been echoed by other representatives, some of whom cite a lack of faith that a federal law so intertwined with technological advancements will be updated effectively prior to obsolescence and who are thus apprehensive about a law that could preclude state innovation, and others who propose that the law should be a floor, rather than a ceiling, to state legislation.

The next few months will be critical for the fate of the ADPPA. It is unclear whether a resolution on the issue of state preemption can be reached while preserving the bipartisan support the ADPPA currently enjoys, and with midterm elections ahead and more privacy laws slated for introduction into state legislatures, the ADPPA risks losing critical momentum gained over the last year.

As of now, the ADPPA remains a bipartisan bill with progress to date that is unprecedented for a federal privacy law of this scope. Those endeavoring to build privacy programs suited for long-term compliance with laws concerning youth data should therefore keep an eye on the progression of the ADPPA, as well as laws specifically targeting minors.

Rulemaking & Enforcement

FTC Advanced Notice of Proposed Rulemaking

On Aug. 11, 2022, the FTC issued an ANPR on "commercial surveillance" and data security practices. This notice marked the first step in a lengthy process under which the commission may seek to exercise its authority under Section 18 of the FTC Act to promulgate a trade regulation rule regarding unfair or deceptive practices deemed to be prevalent – which, based on "recent Commission actions, news reporting, and public research," the FTC believes harmful commercial surveillance and lax data security practices may have become. In addition to protecting consumers against these prevalent harms, the FTC posits that new rules could decrease the uncertainty that companies face due to the agency's current approach of case-by-case enforcement.

Although the 95 questions presented for public comment in the ANPR are expansive in scope and suggest potential for a trade regulation rule that could touch all corners of the internet-connected economy, the FTC has dedicated one of ten headline focus categories to the topic of harm to children. In this section, the Commission seeks to examine what harmful or manipulative practices may be more likely to impact, or most harmful to, children or teenagers, and what measures beyond COPPA may be required to address these harms.

The ANPR questions on data practices affecting children mirror themes appearing throughout the legislation discussed above—including personalized advertising, consideration of teenagers, and enhanced protections even for services not targeted at minors, which is likely intentional given its relation to pending federal laws. Although the ANPR is supported by only three of the five FTC Commissioners, all of the Commissioners have been transparent in stating that the ANPR is being used as a pressure mechanism, with the aim of galvanizing Congress to adopt a federal privacy law to address these issues.

All five commissioners stated in their respective opinions that they would prefer Congress pass the ADPPA instead of having the FTC engage in this rulemaking process. Additionally, the ANPR itself notes that it is aimed at generating a public record about these practices, and that the comments will refine the FTC's work and inform reform by Congress and other policymakers "even if the FTC does not ultimately promulgate new trade regulation rules."

Whether the ANPR is intended to light a fire under or serve as a failsafe to Congressional efforts toward federal privacy legislation, it creates another avenue by which the first comprehensive, nationwide privacy regulation may come into effect. In addition to providing market-wide rules, such a regulation would allow the FTC to levy civil penalties for first-time violations—which it generally cannot do in case-by-case enforcement actions under Section 5 alone. As noted, the ANPR is only the first step in a lengthy, enhanced rulemaking process, but it represents yet another unprecedented development signaling shifts in the US privacy landscape, and the youth privacy landscape in particular.

FTC Policy Statement on COPPA & Edtech

While legislative bodies consider new laws to address youth privacy, in addition to newly exploring the promulgation of broad privacy rules, the FTC indicated renewed commitment to enforcing the full breadth of the current COPPA Rule in a policy statement issued on May 19, 2022, with particular emphasis on education technology (edtech) providers.

The FTC specifically highlights two developments supporting the need for such enforcement: proliferation of business models that rely on collection and monetization of personal information, with increasingly sophisticated technologies and targeting practices, and the reliance on edtech devices and apps in the classroom, the use of which was exacerbated by the Covid-19 pandemic and the proliferation of remote learning.

It will place particular emphasis on:

- Prohibiting mandatory data collection of more data than is necessary to participate in a given activity
- Strict limits on uses of collected data, specifically in the edtech context, prohibiting commercial uses where such data is collected pursuant to school authorization
- Prohibiting retention of data longer than necessary to fulfill the purpose for which it was collected
- Information security requirements

Children's Advertising Review Unit

The Children's Advertising Review Unit (CARU),an FTC-approved safe harbor program under COPPA that conducts routine monitoring of online services for COPPA compliance, has recently found two entities—TickTalk Tech, LLC and Firefly Games—to be in violation of COPPA.

In the case of TickTalk, CARU found that the company's privacy policy was not presented prominently enough prior to purchase, and that such policy was inconsistent with its terms of service and other online statements regarding the collection, use, disclosure and other processing of children's personal information. Further, TickTalk did not include a verifiable parental consent mechanism prior to information collection.

Similar to TickTalk, CARU found Firefly Games to be in violation of both COPPA and CARU's self-regulatory guidelines due to inconsistencies between its main privacy policy and the privacy policy of its LOL Surprise! Room Makeover app, which contains certain child-directed subject matter. Further, CARU found that these policies conflicted not only with each other, but with Firefly Games' actual practices.

CARU also found that Firefly Games violated its Ad Guidelines by allowing ads that could not be dismissed until users had downloaded the advertised app or watched the entire ad, which often included interactive features that mimicked the app's gameplay. Since these ads blur the line between gameplay and an advertisement, CARU suggested that these ads risked manipulating or deceiving children. Notably, CARU found these ads to be a violation of its guidelines despite the ads having passed its host platform Google's review process and guidelines for family advertising.

In both instances, the subject business provided CARU with a detailed plan to remedy the concerns in response to certain CARU recommendations, and as a result neither appears to have led to FTC enforcement. However, both of these examples stress the importance of ensuring that privacy policies, public statements, and terms and conditions regarding privacy practices are uniform, clear and consistent with each other and with actual business practices.

The cases also highlight the need for companies to independently review their privacy practices for COPPA compliance rather than rely on approval processes of applicable hosting platforms.

Conclusion

This year has been incredibly active for novel legislation and a renewed drive to enforce existing laws around youth data privacy protection. Although it remains to be seen whether the aforementioned proposed federal laws and regulations will ultimately be enacted, the momentum of legislative activity makes it clear that there is an appetite for increased regulation in this area.

Indeed, following a listening session on tech platform accountability, on Sept. 8, 2022, the White House reiterated that seeking stronger privacy and online protections for children, including "prioritizing safety by design standards," remains a core priority for reform of this administration. As a result, businesses providing online products or services that may have youth users, whether or not directed at such youths, should pay close attention to these laws and related enforcement activity going forward.