LOEB & LOEB LLP

Changes in Children's Privacy Protection in Response to the Pandemic

Jessica B. Lee CIPP/US, CIPP/E, CIPM
Nerissa Coyle McGinn
Client Alerts/Reports July 2022

Hashed & Salted | A Privacy and Data Security Update

Three years ago, having children stare at a screen for eight hours a day for their education was unthinkable. But for more than two years, having children attend school on the internet was the new normal. Fortunately, many of these children are back in "real life" school. But children's increased use of the internet has amplified the need in the United States and abroad for broader online privacy protection for children, which has in turn led to a flurry of activity in the children's privacy area, from stricter enforcement by the Federal Trade Commission (FTC) to the introduction and passage of new laws focusing on children's privacy and education technology both in the United States and in Europe.

The United States and Children's Privacy

At the federal level, the push for additional protections for children's privacy has come straight from the top. In President Joe Biden's 2022 State of the Union address, he spotlighted the need for stronger privacy protections for children, calling for the outlawing of targeted advertising to children and a ban on the collection of children's personal data by tech companies. In addition, there are several proposed bills in Congress related to children's privacy. These bills seek to expand not only the age of the "children" covered by federal privacy laws but also the types of information considered "personal information."

Even if Congress fails to pass children's privacy legislation, it is likely that the FTC will take action by amending the rules governing the Children's Online Privacy Protection Act (COPPA). At the beginning of May, the FTC announced at the BBB National Programs' Children's Advertising Review Unit (CARU) annual meeting that it intended to conduct a "comprehensive" review of COPPA that will explore "basically everything" in the COPPA rules. Coupled with the announcement two weeks later that the FTC will host a virtual workshop on Oct. 19 called "Protecting Kids from Stealth Advertising in Digital Media" to explore how to best protect children's data privacy, it appears that the FTC may amend the COPPA

rules in the near future.

While we are still waiting for federal action on children's privacy, several states have passed comprehensive privacy bills that have implications for children's privacy. Below is a list of the recent state privacy bills that address children's privacy.

California

California enacted the California Consumer Privacy Act (CCPA), which took effect in 2020, and the California Privacy Rights Act (CPRA), which California voters approved in the November 2020 election and which takes effect in 2023.

Both the CCPA and the CPRA prohibit businesses from selling a consumer's personal information if the business has actual knowledge that the consumer is under the age of 16. Exceptions exist for consumers who are at least 13 and under 16 and affirmatively authorize the sale of their personal information. Parents or guardians of children under 13 also may affirmatively authorize the sale of the consumer's personal information.

California also has had a law on the books since 2019 that protects the online privacy of individuals under age 18 in certain circumstances. The Privacy Rights of California Minors in the Digital World Act, Calif. Bus. & Prof. Code sections 22580-22582, allows individuals under age 18 to remove, or to request and obtain removal of, content posted on a website, online service or mobile app.

Virginia's Consumer Data Protection Act (VCDPA)

The VCDPA, which will be effective on Jan. 1, 2023, defines sensitive data under the act to include any "personal data collected from a known child." The act further defines a child as "any natural person younger than 13 years of age." The VCDPA intends to mirror many of the requirements of COPPA. For instance, controllers must process children's personal data in accordance with COPPA (i.e., only after obtaining verifiable parental consent), and controllers and processors can obtain verifiable parental consent by complying with COPPA's verifiable parental consent requirements. However, unlike COPPA, which applies only to information collected online from children, the VCDPA applies to any information collected from children, and therefore the VCDPA includes information collected online and off-line. In addition, the definition of personal information under the VCDPA is much broader than COPPA's definition. COPPA has a specific list of the types of information considered personal information. However, the VCDPA defines personal information as "any information that is linked or reasonably associated to an identified or identifiable natural person." Therefore, biometric information, for instance, may not be considered personal information under COPPA but would be considered personal information under the VCDPA.

Colorado Privacy Act (CPA)

The definitions of "personal data," "child" and "sensitive information" under the CPA are similar to those of the VCDPA. Therefore, under the CPA, which will be effective on July 1, 2023, the types of information considered personal data also are broader than under COPPA. Like the VCDPA, personal information under the CPA includes information that is collected off-line, and personal data will go beyond the limited classes of information listed in the COPPA rules. Unlike the VCDPA, the CPA excludes personal data regulated by COPPA. However, any other personal data that is collected from children will have to be processed in accordance with the CPA and will require opt-in consent from the child's parent or lawful guardian.

Connecticut Data Privacy Act (CTDPA)

The CTDPA, which will be effective July 1, 2023, similarly defines personal data collected from a child under the age of 13 as "sensitive data." The act also requires that information collected from children must be processed in accordance with COPPA. Unlike the VCDPA and the CPA, the CTDPA also requires consent from a consumer who is known to be between 13 and 16 years old to process their personal data for targeted advertising or to sell their data.

Utah Consumer Privacy Act (UCPA)

The UCPA, which has an effective date of Dec. 31, 2023, has a definition of personal data that is similar to the definition in the VCDPA and the CPA; it defines personal data "as information that is linked or reasonably linkable to an identified individual or an identifiable individual." Therefore, the definition of personal data is again broader than COPPA's definition. However, unlike the other state laws, the UCPA requires that any personal data "concerning" a known child (defined as "individuals younger than 13 years old") be processed in accordance with COPPA which will require obtaining verifiable parental consent. This language broadens COPPA in two distinct ways. First, it broadens the definition of personal information beyond the distinct categories listed in COPPA. Second, it expands the definition to information concerning a child, not just information directly collected from a child.

In addition to this legislation, several states have proposed privacy bills. These include California, Massachusetts, Michigan, Ohio and Pennsylvania. Of these laws, the one that is most likely to pass is California's Age-Appropriate Design Code. Guidance on children's privacy is coming not only from the government. Self-regulatory groups also are issuing their own guidance. The Center for Industry Self-Regulation, the BBB National Programs' nonprofit foundation, unveiled the TeenAge Privacy Program (TAPP) Roadmap on April 19 to guide companies in developing digital products and services that take into account the heightened potential risks to teen consumers' data privacy. These are some of the significant changes recommended by the TAPP Roadmap.

- **Personal information collection**: Opt-in consent for the collection of information where possible.
- **Precise geolocation data**: For businesses that collect and share precise geolocation information, the guidance suggests having default settings set so that the teen user has to opt in. It also advises sending routine reminders of the ongoing collection of precise geolocation data, both in the online service and through other media, such as email. Collection and use of such data also should be turned off by default after inactivity or the end of the session.
- **User-generated content:** The TAPP Roadmap recommends providing mechanisms that allow teen users to limit harmful or potentially harmful interactions.
- **Inappropriate content**: The guidance advises implementing technical features to monitor for inappropriate interactions and removing users based on strikes or extreme policy violations.
- **Algorithmic content monitoring**: The TAPP Roadmap suggests monitoring for harmful content based on algorithms and automating the suppression of such harmful content.
- **Information retention**: The TAPP Roadmap recommends taking steps to minimize the potential for profiling adults based on teenage interests, behaviors and activities.

The United States and Education Technology

At a federal level, the FTC has taken the lead in protection of children's information collected by education technology companies. On May 19, the FTC issued a policy statement announcing its intent to investigate and "closely scrutinize" edtech providers and to take action if providers fail to meet their obligations under COPPA. The policy statement does not change COPPA's rules or requirements or its applicability to edtech companies, but rather it indicates that the FTC will be focusing its efforts on enforcing requirements that already exist in the law. As part of its investigation, the FTC will focus on the following four areas:

Prohibition against mandatory data collection. Companies, including edtech providers, covered by COPPA are not allowed to stop students under 13 from participating in an edtech-based activity if the children refuse to provide information that is not "reasonably necessary" for the student to participate in that activity.

Prohibitions on data use. Edtech providers may use only the personal information collected from children for the requested online education service. If they have permission to use the children's personal information only for educational purposes, the edtech providers are prohibited from using the information for any commercial purpose, including marketing and advertising that is unrelated to educational purposes.

Limitations on data retention. Under COPPA, edtech providers must not retain personal information collected from a child longer than is reasonably necessary to fulfill the purpose for which the data was collected.

Security requirements. Edtech providers must have procedures in place to maintain the confidentiality, security and integrity of children's personal information.

In addition to the FTC's focus on edtech companies and their collection of information from students, several states have enacted laws over the past several years regarding the collection of personal information from students. Many of these laws restrict edtech companies from engaging in the following types of behavior: (1) targeted advertising on the edtech application; (2) targeted advertising based on information acquired through an edtech application; (3) using the information collected through an edtech application to amass a profile, except if it is in furtherance of school purposes; (4) selling or renting information collected through an edtech application; and (5) disclosing information collected through an edtech application, except in furtherance of school purposes. These states include Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Illinois, Iowa, Kansas, Maine, Maryland, Michigan, Montana, Nebraska, New Hampshire, North Carolina, Oregon, Tennessee, Texas, Utah, Vermont, Virginia and Washington.

In addition to these laws, two states, Illinois and Utah, have passed laws that have substantially changed the responsibilities of edtech providers. Below is a short description of the additional responsibilities and requirements placed on edtech providers by these laws.

Illinois Student Online Privacy Protection Act (SOPPA). SOPPA applies to the collection of covered information by the operator of an internet website, online service, online application or mobile application that is used primarily for kindergarten through grade 12 purposes and was designed and marketed for K–12 school purposes. Under the act, covered information means "personally identifiable information or material or information that is linked to personally identifiable information or material in any media or format that is not publicly available … ." SOPPA not only includes prohibited uses of a student's covered information (as described above) but also includes several "duties" for the operator who collects covered information through an edtech technology. These duties include the following:

- Implement and maintain reasonable security procedures and practices.
- Delete a student's covered information within a reasonable time period.
- Have a publicly available privacy policy.
- Have a written agreement with the school district, which must include a listing of the categories of covered information provided to the operator, a description of the costs and expenses that would be

incurred by the school if there is a breach, and a statement that the school must post the agreement on the school's website.

Utah Higher Education Data Privacy Act. In March 2022, Utah expanded the responsibilities of edtech providers to beyond K–12 with the passage of the Higher Education Data Privacy and Governance Act. The act expands the K–12 privacy laws to colleges and universities and prohibits many of the same types of activities as the privacy laws for K–12 students, including the use of student data for targeted advertising and the selling of student data.

The United Kingdom and Children's Privacy

The United States is not the only jurisdiction that is taking action on children's privacy: The United Kingdom's Information Commissioner's Office (ICO) also has increased its focus on children's privacy. In September 2020, the ICO issued the Age-Appropriate Design Code. After a 12-month transition period, businesses and organizations were required to comply with the code by Sept. 2, 2021. The code is not a law, but it is intended to explain how to comply with the United Kingdom's General Data Protection Regulation. The code applies to anyone under the age of 18 and sets out 15 standards. Unlike the United States privacy laws, the UK's code does not require parental consent. Instead, it focuses on having age-appropriate disclosures of privacy practices and giving children the opportunity to make their own privacy decisions. The standards are as follows:

- The primary consideration for the design and development of online services should be the best interests of the child.
- Undertake data protection impact assessments to mitigate risks to the rights and freedoms of children.
- The code should be applied appropriately based on the age of the user.
- Privacy information should be transparent and appropriate to the age of the user.
- Do not use children's personal data in ways that are detrimental to the child.
- Uphold policies and community standards.
- Settings should be set at "high privacy" by default.
- Collect and maintain the minimum amount of personal data needed.
- Do not disclose children's data unless there is a compelling reason to do so.
- Geolocation options should be off by default. Provide children information about parental controls.

- Profiling options should be off by default.
- Do not use nudge techniques to encourage children to provide unnecessary personal data.
- Connected toys and devices must conform to this code.
- Provide prominent and accessible online tools to help children exercise their data protection rights.

The ICO also recently announced a three-year plan titled ICO25. As part of that plan, the ICO listed children's privacy as one of its main priorities. In particular, the ICO intends to enforce the standards set out in the Age-Appropriate Design Code. It also stated that over the next year, it intends to press for further changes by social media platforms, video and music streaming sites, and gaming platforms to correctly assess children's ages and provide age-appropriate privacy notices and to continue its investigations and take enforcement actions to ensure compliance with the code.

What Should You Do Now?

a. Determine whether the restrictions apply to your business (keeping in mind that the age range for these laws is increasing into the teens).

b. Audit your practice. Evaluate whether you are engaging in any advertising, and review the consent and the user journey with an eye to unintentional dark patterns.

c. Identify any potential harms. If your website is personalized or driven toward retaining visitors on-site, evaluate whether and how those techniques impact children.

d. Update your governance policies, and confirm the appropriate controls are in place so that children's data is not disclosed or is retained longer than necessary.

e. Track the updates to the laws and regulations so your practices can remain current.

Click here to download a PDF of the full alert.

RELATED SERVICES

Privacy, Security & Data Innovations

RELATED PROFESSIONALS

Jessica B. Lee CIPP/US, CIPP/E, CIPM

Chair, Privacy, Security & Data Innovations

+1.212.407.4073 jblee@loeb.com

Nerissa Coyle McGinn

(she/her)
Partner

+1.312.464.3130 nmcginn@loeb.com