

Self-Regulatory and FTC Efforts Focus on Children's Privacy

Key Takeaways

- The Children's Online Privacy Protection Act (COPPA) applies to all online services including online gaming services and systems, and voice assistants. It is not limited to just websites and apps.
- Businesses that are subject to COPPA must obtain verifiable parental consent before collecting any personal information from a child under the age of 13 – there are no exceptions for personal information collected during the account creation process except for the very limited data (i.e., parents' online contact information) that can only be used to obtain verifiable parental consent.
- "Personal information" is broadly defined under COPPA to include not only traditional identifiers such as name and address but also things like avatars, biometrics, vital signs and health data when collected and combined with other categories of personal information. It also includes content from any communication from an individual.
- Businesses that are subject to COPPA must not retain personal information collected from children for "longer than reasonably necessary to fulfill the purpose for which it was collected."
- AI is under increased scrutiny, and any data collected in violation of COPPA must not be used to train or improve company algorithms.
- Teen privacy should be carefully considered based on teens' unique needs. There is no "free pass" to use teen data because COPPA does not apply.
- Civil monetary penalties levied for COPPA violations are trending upward. As noted below, Epic Games had



to pay a record-breaking settlement totaling more than half a billion dollars for its use of dark patterns and its children and teen privacy violations.

If you're waiting for the effective dates of newly enacted state privacy laws related to children to draw nearer before evaluating whether any updates are needed to your privacy program, you may already be behind. There has been a lot of activity in this space, outside of legislation, due in large part to the launch of the United Kingdom's Age-Appropriate Design Code (UK AADC) – a first-of-its-kind measure to protect children's and teens' privacy and well-being online that went into force in September 2021. Since then, the United States has kept the ball rolling, as evidenced by self-regulatory initiatives and Federal Trade Commission (FTC) enforcement actions that incorporate many principles found in the UK AADC and continue to make children's privacy a priority.

Spotlight on Self-Regulation. Last fall, the BBB National Programs' Center for Industry Self-Regulation released its TeenAge Privacy Program (TAPP) Roadmap, which aims to provide companies with an operational framework for addressing teen privacy in product development.

Attorney Advertising

It defines “teens” as consumers ages 13 through 17 and outlines four guiding considerations that companies should keep in mind: fostering teen awareness of data privacy, encouraging responsible processing of teen data, building “guardrails” for teen interactions with others through digital systems and reflecting on appropriate content for teens. It also gives specific teen privacy best practices, including guidance related to:

- **Personal Information Collection.** TAPP recommends requiring teen users to give affirmative opt-in consent to the collection of their personal information.
- **Targeted Advertising.** TAPP recommends that businesses avoid targeting content to teens using a single criterion that could be especially sensitive to teens (such as body odor or weight).
- **Precise Geolocation Data.** TAPP recommends requiring opt-in consent and routine reminders of ongoing collection.
- **User-Generated Content.** TAPP recommends having mechanisms to limit harmful or potentially harmful interactions.
- **Inappropriate Content.** TAPP recommends monitoring for inappropriate conduct and removing/banning users who engage in harmful conduct.
- **Algorithmic Content.** TAPP recommends monitoring for harmful content and suppressing such content.
- **Information Retention.** TAPP recommends minimizing the potential for profiling adults based on teenage interests and behaviors (i.e., avoid including teen information as part of a “permanent record” that follows the teen into adulthood).

As discussed in our [previous alert](#), TAPP brings the United States somewhat more in line with the UK’s data privacy protections for teens and is similar in many ways to the UK AADC. Both the UK AADC and TAPP require companies that offer online services to focus on creating an age-appropriate experience for teens from a privacy and safety perspective. This includes considering unique risks and harms to teens (taking into account differing ages), implementing certain privacy settings by default, meeting notice requirements and giving teens the ability to manage privacy choices for themselves.

While companies are not required to follow the TAPP framework, many of the guideposts within the program

are now being adopted by the FTC. Therefore, if companies begin to incorporate these guidelines as best practices for the collection and use of personal information, they will not be left flat-footed as the FTC ramps up children’s privacy enforcement.

FTC Enforcement Highlights. Children’s privacy is undoubtedly a priority for the FTC. The agency has, within the past few months, announced a number of enforcement actions, an order against Meta relating to a previous settlement and a call for comment on a new parental consent mechanism. The FTC’s actions appear to be increasingly aligned with the global and self-regulatory landscape, as the agency also continues to hold companies’ feet to the fire on long-standing children’s privacy protection requirements under COPPA.

- Late last year (Dec. 19, 2022), the FTC announced two proposed settlements with Epic Games Inc., the maker of Fortnite – a popular video game designed to match players together (with no regard for age) – for a combined total of \$520 million in fines. In the first action, the FTC alleged that Epic violated COPPA by collecting personal information from Fortnite players under the age of 13 without providing notice or obtaining verifiable parental consent, and that Epic also violated Section 5 of the FTC Act by enabling real-time voice and text communications for children under the age of 13 and teens 13 through 17 by default, which exposed them to bullying, harassment and toxic content. The FTC addressed these issues by requiring Epic to delete all personal information it had previously collected from Fortnite players in violation of COPPA and prohibiting Epic from enabling voice and text communications from children and teens without affirmative consent from parents (or from teens age 13 through 17). Notably, this is the first FTC COPPA settlement that has afforded teens any special privacy protections. The FTC alleged in a second action that Epic used dark patterns (i.e., deceptive designs) “to dupe millions of players into making unintentional purchases.” There were a number of design features at issue, including one that allowed children to make in-game purchases without requiring parental consent or any other action by the credit card holder. Of the total \$520 million penalty, \$245 million has been finalized, as of March 2023, to refund consumers affected by Epic’s deceptive design practices.

- On May 3, the FTC announced proposed changes to its 2020 consent decree order with Meta (formerly Facebook) after alleging that the company violated the order in a number of ways, including by misrepresenting the extent to which third-party developers would have access to users' nonpublic information and misleading parents about their ability to control with whom their children communicated on its Messenger Kids app. The FTC says the misrepresentations related to children were also a violation of the FTC Act and COPPA. Under the new proposed order, Meta would be prohibited from "[c]ollecting, using, selling, licensing, transferring, sharing, disclosing, or otherwise benefiting" from the data it collects from minors under the age of 18 except for specific purposes, such as operating a service, performing authentication or maintaining security. Notably, this would prevent Meta from using minors' personal information for targeted advertising or to train or improve its algorithms. The updated order would also require Meta to pause the launch of new products and services without written confirmation from an independent third-party assessor that its privacy program is in full compliance with the order's requirements; ensure compliance with the order for any companies it acquires or merges with; disclose and obtain users' affirmative consent for any future uses of facial recognition technology; and be subject to expanded obligations related to third-party monitoring, data inventory and access controls, and employee training.
- On May 31, the FTC announced a \$25 million settlement with a popular voice assistant maker regarding alleged COPPA violations, including that the company retained voice recordings of children indefinitely by default (rather than keeping them for only as long as reasonably necessary to fulfill the purpose of collection as required under COPPA) and failed to honor deletion requests in accordance with requirements under COPPA and its stated privacy practices. Notably, the FTC called out the company for using kids' data to feed its algorithms to aid in developing artificial intelligence, specifically explaining that children's speech patterns are markedly different from those of adults, so the voice recordings gave the company a valuable data set for training the voice assistant algorithm and furthered the company's commercial interest in developing new products. The settlement order, which was agreed to on July 17, 2022, requires the company to identify and delete inactive child profiles that have not been used for 18 months, unless a parent requests that they be retained. The order also prohibits the company from making misrepresentations about the retention of profiles and access to or deletion of geolocation information or voice information, including children's voice information, and mandates this information be deleted upon the request of the user or parent (for children under the age of 13). This sends a strong message that children's data must not be retained indefinitely for any reason and "certainly not to train their algorithms."
- On June 5, the FTC announced a \$20 million proposed settlement with Microsoft for COPPA violations. Microsoft allegedly collected personal information from children under 13 during the sign-up process for its Xbox live game (which consumers use to connect online and with others through the Xbox brand of gaming consoles) before getting their parents involved. Microsoft was also dinged for having several deficiencies in the notice that it provided to parents describing its data practices. According to the FTC, parents did not have the information needed to help them decide whether to give consent. Finally, Microsoft's data retention and deletion practices did not meet COPPA's requirements because Microsoft held on to data collected from children under 13 even if it ultimately did not get parental consent. In addition to the monetary fine, the proposed settlement sets forth a number of other requirements, including the requirement that Microsoft delete all personal information that it collects for the purposes of obtaining parental consent if parental consent is not secured within two weeks. Microsoft must also notify video game publishers when it discloses personal information from children that the users are children (which will require the publishers to apply COPPA's protections to those children).
- On July 19, the FTC announced that it is seeking public comments on the use of "privacy-protective facial age estimation" technology as a potential new method that COPPA-subject entities can use for obtaining verifiable parental consent prior to collecting personal information from children under the age of 13 as

required by COPPA. This technology analyzes the geometry of a user's face to confirm that they are an adult. According to the Entertainment Software Rating Board (ESRB) and other entities that are requesting the FTC's approval of this new consent method, facial age estimation technology can be implemented in a way that is consistent with COPPA's data minimization, confidentiality, security, integrity, and retention and deletion provisions, and that addresses the FTC's concerns about potential bias and discrimination. Furthermore, industry groups argue that allowing this method would modernize currently approved consent methods, which have been criticized for being outdated (e.g., printed consent forms that parents can return by "postal mail, facsimile, or electronic scan"). The public will have until Aug. 21 to submit comments. Then the FTC will have 120 days to review proposed verifiable parental consent methods and set forth its conclusions in writing.

Related Professionals

Nerissa Coyle McGinn nmcginn@loeb.com
Chanda Marlowe cmarlowe@loeb.com

This is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This publication does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

© 2023 Loeb & Loeb LLP. All rights reserved.

7380 REV1 08-23-2023