LOEB & LOEB LLP

BBB National Programs' Center Releases Roadmap for Teen Online Privacy

Nerissa Coyle McGinn
Chanda Marlowe CIPP/US, CIPP/E
Client Alerts/Reports May 2022

For the first time in the United States, a business self-regulatory group has introduced a framework aimed at protecting the online privacy of teenage consumers ages 13 to 17. The online privacy of children under age 13 is protected by federal law under the Children's Online Privacy Protection Act (COPPA). But until now, no industry guidance has focused on protecting the online privacy of teenagers.

The Center for Industry Self-Regulation (CISR), 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.

The new guidance comes amid a push to increase consumer online privacy for both children and teens at the state and federal levels, as well as related legislative developments outside the U.S.

Teen Specific Harm

According to the BBB National Programs announcement of the TAPP Roadmap, teens who use websites, apps, games and other digital media tend to be unaware of the hidden systems running such media. Teen-directed digital products are more likely to engage in ad serving, include more third-party trackers, ask for more permissions and offer more in-app purchases than apps developed for a general user audience. This significantly increases teen privacy risks. Separate guidance is needed for businesses producing online content for teen consumers because teenagers are very different from children under the age of 13 in terms of mental development and interests. Youths ages 13 to 18 are between childhood and adulthood and require their own set of consumer privacy standards, noted the BBB National Programs, citing its 2020 white paper, "Risky Business: The Current State of Teen Privacy in the Android App Marketplace."

According to the TAPP Roadmap, potential harms specific to teenagers who use digital technologies, products and services include:

- Normalization of a lack of privacy and over-collection of data
- Creation of a digital footprint outside of a teen's control or awareness
- Inadequate information provided for teen comprehension
- Exposure to age-inappropriate or potentially harmful or addictive content
- Damage to digital reputation that may persist into adulthood
- Amplification of interests or insecurities in a way that intensifies harmful thoughts or behaviors
- Safety risks that can lead to cyberbullying, stalking, and harassment and abduction

From a business perspective, the failure to implement practices to protect teen consumers' online privacy can result in:

- Brand/reputation damage
- Potential legal exposure
- Inability to enforce terms of use
- Potential for bias due to relying on inaccurate or outdated information

TAPP Roadmap Guidance

The TAPP Roadmap aims to provide data privacy and safety practices that address teen-specific stages of cognitive and social development. The 23-page publication outlines four guiding considerations that businesses should keep in mind when developing digital products and services that collect teens' personal data:

a. **Fostering teen awareness of data privacy**. Businesses should help teen consumers become informed about privacy risks and their individual responsibilities to manage their privacy choices. To do this, businesses must inform teens about the types of personal data that will be collected or inferred about them and how they can manage their personal information. Businesses also should provide parents with educational resources, where appropriate.

b. **Encouraging responsible processing of teen data**. Even the potential presence of teen consumers should prompt businesses to examine their privacy practices in the context of teens' unique needs, including the implementation of default settings, use of sensitive personal information, the presence and accessibility of privacy choices, and the retention of personal information.

c. **Building "guardrails" for teen interactions with others through digital systems**. Trust and safety should be considered with an eye to the needs of teens, particularly when systems facilitate interaction or sharing of information among individuals.

d. **Reflecting on appropriate content for teens**. The potential for harm that is unique to teens should be considered when systems deliver content to individuals, especially when such content is tailored based on individual interests and behaviors.

Privacy and Safety Questions

The TAPP Roadmap provides what it calls "Signposts for Teen Privacy & Safety" across several categories—general information and the collection, use and retention, and sharing of teens' personal data. These sections advise businesses to ask specific privacy-related questions when designing business practices and consider implementing recommended practices to avoid identified risks or harms to teens.

General information. When designing business practices that involve a product, service or system appealing to teen audiences or interests, one general question businesses should initially ask themselves is: "Do you know the definitive age of the consumers/users?"

Recommended practices to avoid inappropriate treatment of teen consumers/users as adults are the establishment of the ages of consumers/users, consideration of the potential risks, and application of best practices to known teen consumers/users. Businesses also can opt to apply best practices to all users across the board.

Collection of teen data. If a business is collecting teen consumers' personal information for interest-

based or targeted advertising, one question that should be asked is: "Are teen users made aware that their information will be used for targeting ads, potentially across different sites or devices?"

To avoid the unauthorized or unnecessary collection of teens' personal information, businesses are advised to provide information at the time of obtaining the user's opt-in consent. Specifically, businesses should provide conspicuous notice or point to external resources, where appropriate, that explain the tracking technologies, such as cookies, used to facilitate the advertising. This information should be relayed in terms that are easily understandable to a teen audience.

Use and retention of teen data. When designing business practices around content generated by teen users, a key question businesses should ask is: "Are users empowered to control their own experience and limit interaction with harmful users/content?"

The lack of empowerment could result in cyberbullying, unsafe/unwanted contact, harm to users' digital reputations and even self-harm by teen users. Businesses are therefore encouraged to provide the functionality to block, mute or pause other users; filter keywords or reduce frequency of certain content; and limit visibility of their own content.

Sharing of teen data. Businesses that share teen users' personal information are advised to ask themselves: "Do we disclose the names of the entities with which data is shared, and the purposes for which they're using teen user information?"

Because sharing teens' personal information increases the misuse of their personal information and the risk of data breaches, businesses are advised to create mechanisms that empower teen users to easily seek more information about which entities receive their personal information.

Significant Changes Recommended

Guidance required by some sections could require businesses to become, in effect, content moderators for teen users, a role businesses don't currently even take on for children under the age of 13. The guidance also could require significant changes to their apps and targeted advertising. For example:

Personal information collection. The TAPP Roadmap suggests that businesses require teen users to give affirmative opt-in consent to the collection of their personal information wherever possible.

Targeted advertising. The TAPP Roadmap advises businesses that collect teen users' personal information for interest-based or targeted advertising to avoid targeting content to teens using a single criterion that could be especially sensitive to teens or amplify existing insecurities, such as body odor, hair loss, or weight. The guidance suggests that businesses supplement their messaging and advertising with content that counteracts the potential negative impact of the targeting.

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 should also 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; creating and adhering to internal policies for suspending and removing users based on strikes or extreme policy violations; and implementing mechanisms to prevent banned users from opening new accounts. It also warns against presenting to teens "salacious, incendiary, or highly polarizing content," which could include political topics.

Algorithmic content monitoring. The TAPP Roadmap suggests monitoring for harmful content based on algorithms that identify, for example, adult content and hate speech. In addition, the guidance suggests automating the suppression of such identified harmful content. The guidance also advises flagging, warning and removing users for posting such content.

Information retention. The TAPP Roadmap recommends taking steps to minimize the potential for profiling adults based on teenage interests, behaviors and activities.

Finally, it must be noted that the TAPP Roadmap includes certain protectionist features of COPPA, especially the guidance for businesses to safeguard teen consumers from "inappropriate" content. The definition of this term continues to be very broad and includes potential psychological harm from targeted advertisements focusing on personal appearance or hygiene.

Global Context

The guidance brings the U.S. somewhat more in line with the United Kingdom's data privacy protections for teens. In fact, the TAPP Roadmap is similar in many ways to the U.K.'s Age Appropriate Design Code, which imposes 15 compliance standards on digital services to protect children's online data. Parallels include making teens aware of data privacy issues and enabling them to make decisions for themselves; required default settings; and notice requirements.

On the horizon is proposed legislation in the European Union (EU) that would impose new obligations on large online platforms and strengthen consumer privacy controls, which could be viewed as another potential guide for the U.S. The Digital Services Act (DSA) would include, among other provisions,

increased protection for child consumers and limits on the use of sensitive personal data for targeted advertising.

The DSA also would require assessment and impose risk mitigation responsibilities on digital service providers including hosting services; online platforms such as marketplaces, app stores and social media platforms; and network infrastructure services such as Internet access providers and domain name registrars. "Very large online platforms" would be required to take action to prevent misuse and to submit to independent audits of their risk-management systems. Specific rules are proposed for platforms that reach more than 10% of the EU's 450 million consumers.

Proposed by the European Commission, the DSA is awaiting approval by the European Parliament and the European Commission.

The passage of similar online privacy policies by the U.S., the U.K. and the EU that include protection for children and teen consumers may prove helpful for multinational companies, which have been forced to comply with a patchwork of international regulations. Some have responded by tightening their own privacy policies.

For example, Unilever, a multinational consumer goods company headquartered in London, ceased marketing food and beverages to children under age 12 in traditional media, and to children under 13 through social media. The company, which owns ice cream brands Ben & Jerry's and Magnum, among many others, recently announced it would now stop marketing food and beverages to children and teens under 16 in traditional and social media.

Unilever also committed to stop collecting or storing data on children and teens under 16 and to stop using influencers, celebrities or social media stars who are under the age of 16 or primarily appeal to children under that age. The company said it would adopt these principles by 2023.

U.S. Federal Law and Proposed Legislation

A patchwork of laws protecting the online privacy of consumers under age 18 remains in the U.S. The CISR's TAPP Roadmap guidance arrives as momentum gains to increase federal regulation of online privacy protection for both teens and children. President Joseph Biden briefly spotlighted the issue in his March 1 State of the Union address, calling for even stronger privacy protections for children, outlawing of targeted advertising to children, and a ban on the collection of children's personal data by tech companies.

Numerous bills have been introduced in Congress to protect the online privacy of teens as well as children. Several bills specifically seek to extend COPPA's scope to consumers ages 13 to 16. (Currently, there is no comprehensive federal data privacy law targeting consumers over age 13.)

COPPA requires operators of commercial websites and online services, including mobile apps and smart toys, to notify parents and obtain their verifiable consent before collecting, using or disclosing personal information of children under 13. With enforcement by the Federal Trade Commission (FTC), COPPA also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using or disclosing personal information from children under 13.

The federal bills introduced include the following:

Kids Online Safety Act (S. 3663).
Introduced in the Senate in February 2022, this bill would require covered digital platforms to provide minors, defined as age 16 or younger, or a parent acting on their behalf, with accessible and easy-to-use safeguards to control their personal data. Platforms would also be required to submit an annual public report identifying foreseeable risks of harm to minors based on an independent audit, and to outline prevention and mitigation measures taken to address such risks. While the bill states that a covered platform has a duty to act in the "best interests" of a minor who uses the platform's products or services, it does not define "best interests."

Kids Internet Design and Safety (KIDS) Act (H.R. 5439 and S. 2918). Identical bills introduced in September 2021 would prohibit the operators of commercial online platforms directed to users under age 16 from implementing features that encourage additional engagement with the platform, promote certain types of content and use certain advertising methods. Banned content would include material that is sexual or that promotes physical or emotional violence. Also prohibited would be online advertising methods that include influencer marketing; material with commercial content involving alcohol, nicotine or tobacco; and content that includes product placement

Protecting the Information of Our Vulnerable Children and Youth Act (H.R. 4801). This bill, introduced in July 2021, would extend COPPA protections to teenagers, defined as individuals over age 12 and under age 18. The bill also would require digital platforms to conduct "privacy and security impact assessment and mitigation" regarding the privacy risks posed to children and teens.

Children and Teens' Online Privacy Protection Act (S. 1628). This bill would amend COPPA to extend privacy protections to minors ages 12 to 16. It would prohibit operators of websites, online services, online applications or mobile applications directed to minors, which have constructive knowledge the user is a minor, from collecting the minor's personal information without notice or consent. The bill, introduced in May 2021, also would ban the sale of internet-connected devices targeted to children and minors unless they meet certain cybersecurity and data security standards.

Clean Slate for Kids Online Act of 2021 (S. 1423). Introduced in April 2021, the bill would amend COPPA to permit individuals over age 13 (or their guardians, if applicable) to request the deletion of personal

information collected from or about them when they were under age 13 by a website or online service that is directed to children. The bill requires the operator of such a website or service to provide notice on their website on how an individual over age 13 can request the deletion of such personal information, to promptly delete all such personal information upon request and to provide written confirmation of deletion.

Preventing Real Online Threats Endangering Children Today (PROTECT Kids) Act (H.R. 1781). This bill amends COPPA to raise the age for parental consent protections for children online from under 13 to under 16, adds geolocation and biometric information to protected personal information, and extends all protections for children online to mobile applications. Introduced in March 2021, the bill additionally requires the FTC to study and report on the appropriateness of the existing actual knowledge standard—preventing an operator from collecting personal information without meeting certain requirements when it has actual knowledge that it is collecting such information from a child—and how changing that standard would affect children's online privacy.

Proposed State Measures

Several states have enacted their own data privacy laws, some of which are also aimed at protecting teens and children.

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

Both the CCPA and CPRA prohibit businesses from selling consumers' personal information if the business has actual knowledge that the consumer is under age 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 for 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.

The law bars operators of a website, online service or mobile app directed to individuals under 18 from marketing or advertising products or services that are illegal for that age group. It also prohibits marketing or advertising certain products based on the personal information of individuals under age 18, or knowingly using, disclosing, compiling or allowing a third party to do so.

Bills also have been introduced in at least two states. Proposed legislation pending in California includes:

California Age-Appropriate Design Code Act (A.B. 2273). Introduced in February 2022, this bill would require businesses that create or provide a good, service or product feature likely to be accessed by children, defined as consumers under age 18, to comply with specified standards. These standards include considering the best interests of children when designing, developing and providing that good, service or product feature. It also would prohibit such businesses from collecting or using data they collect on consumers who are children.

The bill does not define "best interests of children." Critics also debate whether the proposed rules should apply to online sites and apps "likely to be accessed by children" or only to sites and apps specifically made for children.

Kids Internet Design and Safety Act (A.B. 1545). This bill, introduced in February 2021, would amend the CCPA to prohibit an operator of an online platform from incorporating certain features viewable by users under 13. These include settings that allow users under 13 to make purchases, submit content or communicate with other individuals on the platform without first obtaining consent from the user's parent or guardian.

Washington introduced a bill on children's online privacy in January 2022:

Establishing Data Privacy Protections to Strengthen a Consumer's Ability to Access, Manage, and Protect Their Personal Data (S.B. 5813).

This bill would establish additional protections for the personal data of children under age 13 and adolescents, defined as individuals under age 18, who are residents of Washington.

The bill requires a business to clearly notify consumers about the types of personal information it collects from children or adolescents. A business must provide a secure and reliable mechanism allowing the parents or guardians of children or adolescents to access, correct or delete such personal information. A business is prohibited from processing a child's or adolescent's personal information without express consent from the child's parent or guardian, or from the adolescent.

Looking Ahead

While the TAPP Roadmap provides guidance and a framework around teen data privacy, the Roadmap does not have the force of law, and the BBB does not currently have a program for enforcement of the Roadmap. (The Children's Advertising Review Unit (CARU), the COPPA safe harbor program run by the BBB, only applies to children 13 and under.) However, with the number of proposed state and federal bills related to children's and teens' privacy, it is likely that there will soon be laws governing the collection and

use of teenagers' information. It is unclear which of these laws will be enacted, but many of these laws include elements of the Roadmap. Therefore, in anticipation of the passage of these laws, businesses should consider following the guidance laid out by the TAPP Roadmap.

Click here to download a PDF of the new alert.

RELATED SERVICES

Privacy, Security & Data Innovations

RELATED PROFESSIONALS

Nerissa Coyle McGinn

(she/her)
Partner

+1.312.464.3130 nmcginn@loeb.com

Chanda Marlowe CIPP/US, CIPP/E

Associate

+1.202.618.8468 cmarlowe@loeb.com