

[Updates](#)

April 25, 2022

Growing Pains: New Self-Regulatory Framework for Teenage Privacy Proposed

Through its newly launched Center for Industry Self-Regulation (CISR), BBB National Programs [announced last week](#) the launch of the TeenAge Privacy Program (TAPP). The TAPP introduces a proposed self-regulatory framework that seeks to help companies to mitigate risks of harms to teenage consumers and to collect and manage teen data responsibly. Built with input from business leaders in the consumer goods, children's marketing, and wireless and media technology spheres, the TAPP reflects the growing spotlight on teen online privacy and an increasing body of research regarding the vulnerability of teens online.

The Perils of the In-Between: What Protections Exist for Teens Online?

Increased regulatory attention to the privacy of minors is not new. For years, the collection, use, and disclosure of personal information from children under age 13 online has been governed by the [Children's Online Privacy Protection Act \(COPPA\)](#). States have layered on to COPPA's protections by, for instance, limiting the types of products and services that can be marketed to them and the right to request deletion of information they post online, including through California's act on [Privacy Rights for California Minors in the Digital World](#) and the [Delaware Online Privacy Protection Act \(DOPPA\)](#). COPPA provides robust protections for children under 13, requiring companies to, among other things, (1) obtain the verifiable consent of a child's parent or legal guardian prior to collecting personal information from a child, and (2) allow parents or legal guardians to request access to or deletion of any personal information collected from that child.

By contrast, regulation of teens' (consumers aged 13 to 18) online privacy has traditionally been less robust. In 2020, the [California Consumer Privacy Act \(CCPA\)](#) introduced the obligation to obtain consent (from the parent for consumers under 13 and from teens for consumers 13-15) before selling the personal information of an individual under 16. The California Privacy Rights Act (CPR), which will go into effect in 2023, adds to these obligations with respect to "sharing" personal information for targeted advertising purposes and imposes a two-step, request-and-confirm process. Other newly adopted omnibus consumer privacy laws such as the Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (CPA) do not, however, impose specific obligations with respect to teen consumers.

There have been some legislative proposals in the works that would expand online privacy protections for teens. In February of this year, California proposed an [Age Appropriate Design Code](#), (modeled off of the [U.K.'s legislation of the same name](#)), which would require businesses to take into account certain privacy and safety considerations when designing digital products and services that could be used by consumers under age 18. On the federal level, in May of last year, [legislation was introduced in the Senate](#) to broaden COPPA's protections to children aged 13 to 15. However, the bill has not moved out of committee, signaling a low likelihood of passage.

The CISR Best Practices: A New Framework for an Old Problem

Against this void, the TAPP CISR [roadmap](#) seeks to help companies build services with the unique needs of teens in mind. The guidance offered by the CISR is divided into three parts:

1. Collection of Teen Data. Chief among the CISR's concerns is the unauthorized and unnecessary collection of teens' information, the normalization of overcollection, related harms with respect to physical and mental health and safety, increased risks of data breach, and the creation of a digital footprint beyond the teen's awareness or

control. To address these concerns, the CISR suggests the following:

- For general collection of teens' **personal information**, companies should consider minimizing data collection to what is necessary and expected by the teen consumer, and implementing clear disclosures and controls (for instance, affirmative opt-in consent) where collection might exceed the consumer's expectations.
- If the company collects or uses teens' personal information for **targeted advertising purposes**, the CISR suggests that providers obtain opt-in consent from the teen or refrain from targeting ads to them at all. The roadmap further suggests that providers refrain from targeting teens using a single, particularly sensitive criterion (for instance, body weight) and supplement such targeted advertising with positive messaging.
- While the CISR suggests that the default should be for providers not to collect or share teens' **precise geographic location data**, it further recommends that any such collection be accompanied by clear, opt-in disclosures, routine reminders, limitations on the precision of the data collected, and controls to disable collection after inactivity or the end of a use session.

2. Use and Retention of Teen Data. The roadmap also seeks to address potential harm to teens (mental, emotional, physical, reputational, and otherwise) that may result from the content presented to them or that they can post. To that end, the CISR suggests:

- With respect to **user-generated content**, the CISR advises providers to put in place controls allowing teens to (1) flag harmful content, limit future harmful engagement (e.g., by blocking, muting, or pausing other users, filtering keywords, or using audience controls), and to implement policies for ensuring up-to-date monitoring software; (2) suspending, removing, and banning certain users; (3) identifying, escalating, and reporting harmful or illegal content through both automated and manual review; (4) facilitating easy-to-find and understandable safety mechanisms; (5) allowing teen users to remove or modify unwanted content engagement (for instance, photo tags or abusive messages); and (6) increasing buy-in from teens to build trust and encourage community enforcement.
- For content that may be considered **inappropriate for teens**, the CISR suggests that providers follow [Common Sense Media Guides](#) for consumers aged 13 to 14 and 15 to 17, and that they avoid directing particularly polarizing, incendiary, or sensitive content (e.g., political topics or weight loss material) to teens.
- If the company is using **algorithms to curate content**, it should ensure that state-of-the-art business practices are in place to monitor and remove harmful or addictive content (and to flag any content that may be sensitive for teen consumers) and should allow consumers to understand and adjust their preferences over time as their needs and interests change.
- Finally, in order to avoid the development of an online "permanent record" that could harm the teen as they grow into adulthood, companies should be mindful of **retention practices** by (1) reducing the use of targeted ads on adults based on their teenaged interests, (2) empowering teens to control their digital footprint, (3) assessing whether the retention of certain information (whether or not it is still in use) could harm the teen, and (4) shortening retention periods where a particular risk of harm is identified.

3. Sharing of Teen Data. To reduce the risk of data breaches and other misuses of teens' personal information, the CISR advises that providers thoroughly vet the privacy practices of their service providers and data processors. Providers should also encourage privacy literacy by empowering teens to seek further information, mapping data types to uses to allow teens and their parents to easily see how their personal information is being used, and openly facilitating the choice to stop sharing personal information when not necessary for the functionality of the product or service.

What's Next: Next Steps and New Challenges

While the CISR's roadmap sets forth useful guideposts for considering how to protect teens online, it does not answer key questions such as how companies are expected to understand if they have teen users or when they are likely to attract such users, though it does suggest that, in general, companies should either establish the age of consumers to which they will provide or offer services, or broadly apply the TAPP protections to all users. How widely the TAPP is adopted remains to be seen, but it is sure to provide useful guideposts to companies and to inform debates around teen services in the years ahead.

TAPP is available for download [here](#).

© 2022 Perkins Coie LLP

Authors

Explore more in

[Privacy & Security](#) [Technology Transactions & Privacy Law](#) [Retail & Consumer Products](#)

Related insights

Update

[**Two Tools for Trump To Dismantle Biden-Era Rules: the Regulatory Freeze and the Congressional Review Act**](#)

Update

[**The FY 2025 National Defense Authorization Act: What's New for Defense Contractors**](#)