

# Cracks in the Privacy Wall Between Kids and Teens: Is Teen Privacy Legislation on the Horizon?

October 13, 2021

Since Congress enacted the Children’s Online Privacy Protection Act ([COPPA](#)) in 1998, the regulatory wall between kids and teens has been a remarkably durable one. During all this time, COPPA, the primary U.S. law protecting kids’ privacy, has protected children under 13 but hasn’t provided any protections for teens. While California’s privacy law grants some rights to teens under 16, these protections are narrow (opt-in for data sharing) and only apply within that state. This means that teens are generally treated like adults for purposes of privacy in the U.S.

It’s not exactly clear why COPPA’s age 13 cut-off was chosen the first place. First year of teen-hood? Bar Mitzvah age? The age when children become too independent and tech-savvy to let their parents control their media? (Ahem – that happened at age six in my house.) Whatever the reasons for the original choice, age 13 has stuck, even as concerns about teens’ privacy and use of social media have grown, and [Senator Markey](#) and others have repeatedly proposed extending privacy protections to teens.

However, we might finally be seeing some cracks in the kid-teen privacy wall – cracks that could lead to a federal law protecting teens in the not-too-distant future.

These cracks are due to a confluence of events. Notably, in September 2020, the U.K. passed a law (the [Age Appropriate Design Code](#) or AADC) that requires all online commercial services “likely to be accessed by” kids and teens (including apps, programs, websites, games, community environments, and connected toys or devices) to meet 15 standards to ensure that their content is age appropriate. The law, which became fully effective in September 2021, starts with the principle that any service be designed with the “best interest of the child” as a primary consideration. It then details more specific requirements, including that defaults be set at the most protective level (e.g., location tracking and profiling are set to “off”), that data is not shared with third parties without a “compelling reason,” and that “nudge” techniques aren’t used to encourage minors to provide data or reduce their protections.

In response to the law, U.S. companies operating in the U.K. (notably, some of the large tech platforms) recently announced new protections for teens – a significant development in the long-running kid-teen debate, but one that has received relatively little attention. For example, [Facebook/Instagram](#) now says that for kids under 16, it will default them into private accounts; make it harder for “suspicious” account holders to find them; and limit the data advertisers can get about them. Meanwhile, [Google/YouTube](#) has pledged similar protections for kids under 18, including private accounts by default; allowing minors to remove their images; applying restrictive default settings; turning off location history permanently; and limiting the data collected for ad targeting.

Following these announcements, Senator Markey and two House members sent a [letter](#) to the FTC urging it to ensure that these companies keep their promises, using its authority to stop deceptive practices under the FTC Act.

And there's more. Last week, in developments widely covered in the media, a former Facebook employee detailed what she viewed as manipulation of teens using algorithms that kept them on the platform and exposed them to harmful content. Also, with broad-based privacy legislation perennially stalled, there's been talk that Congress might prefer to tackle privacy issues that are [more manageable and bipartisan](#) (like kids' and teen privacy) – talk that has only grown louder since the developments regarding Facebook.

Adding to the momentum, Senator Markey recently introduced a [bipartisan bill](#) (with Republican Senator Cassidy) that would provide privacy protections specific to teens, and Representative Castor has introduced a [similar bill](#) in the House. Further, the [FTC](#) has expressed a strong interest in protecting kids' privacy, and in undertaking enforcement and rulemakings to extend U.S. privacy protections beyond the status quo.

In short, the kid-teen privacy wall is under pressure, and we could soon see a federal law, FTC enforcement, and/or (a harder climb) an FTC rulemaking using the agency's Magnuson-Moss authority. For companies that collect teen data in connection with marketing or providing commercial products or services, this means double-checking your data practices to ensure that they're age-appropriate and don't expose teens to harms that can be avoided. (While the U.K.'s AADC principles are very ambitious, and do not apply to U.S.-only companies, they're a valuable reference point.) It also means being prepared to explain and defend your data practices with respect to teens if regulators come knocking.

We will continue to monitor developments on this issue and provide updates as they occur.

