New Federal Bill to Protect Kids' Privacy: Will This One Break Through?

Laura Riposo VanDruff

February 22, 2022

Last October, we blogged that bipartisan momentum was building in Congress to enact stronger privacy protections for children, even if (and especially if) Congress remains stalled on broader federal privacy legislation. Of particular significance, we noted a strong push to protect, not just kids under 13 (the cutoff under COPPA), but also *teens*.

Since then, the momentum to enact stronger privacy protections for kids and teens has only increased, fueled by charges that social media and algorithms are causing self-harm and addictive behaviors by minors; multiple rounds of testimony from a former social media insider; and the desire in Congress to find common ground on *some* aspect of consumer privacy. Several kid/teen bills have been proposed in just the last couple months. (See for example here and here.)

The latest of these bills, introduced last week by Senators Blumenthal and Blackburn, has drawn a lot of attention – both because it's bipartisan, and because these two Senators lead a key Senate subcommittee and held multiple hearings on algorithmic harms to teens. The bill (the Kids Online Safety Act or "KOSA") has been endorsed by a number of organizations that focus on protecting kids' safety and mental health. It also has drawn praise from Senator Cantwell, Chair of the Senate Commerce Committee, who told at least one media outlet that she is considering a committee markup on the bill.

KOSA's stated purpose is to "require social media platforms to put the interests of children first" by establishing a "duty of care" to prevent harms to minors, "mak[ing] safety the default," and enabling kids and parents "to help prevent the harmful effects of social media." In announcing the bill, Blumenthal stated that it "would finally give kids and their parents the tools and safeguards they need to protect against toxic content—and hold Big Tech accountable for deeply dangerous algorithms." Portions of the bill appear to be modeled after the UK's Age Appropriate Design Code, a law that establishes content standards for minors, but is styled more like a guide setting forth principles and best practices. Here's our summary of the bill's key features:

- **It covers a wide range of entities.** Although the press release and bill summary focus on social media platforms, the bill would extend to any "covered platform," defined as "a commercial software application or electronic service that connects to the internet and that is used, or is reasonably likely to be used, by a minor." This definition would reach a huge range of

Internet-connected devices and online services. It also leaves open the question of what it means to be "reasonably likely to be used" by a minor. (Some of the bill's provisions are triggered when a platform "reasonably believes" a user is a minor – a phrase that raises similar questions.)

- **It extends protections to any minor 16 or under.** This contrasts with the under-13 cutoff in COPPA, the primary U.S. federal law protecting kids' privacy. It's not clear how this bill would interact with COPPA.

- **A covered platform has a duty of care to minors.** It must act in the "best interests" of minors, including by preventing and mitigating "heightened risks of physical, emotional, developmental, or material harms" posed by materials on, or engagement with, the platform. Examples of such harm include: (1) self-harm, eating disorders, or other physical or mental health risks; (2) patterns of use indicating or encouraging addictive behaviors; (3) physical harm, online bullying, or harassment; (4) sexual exploitation; (5) promoting products that are illegal to minors; and (6) predatory, unfair, or deceptive marketing practices.

- **The platform must provide tools allowing minors *or their parents* to control the minor's experience.** These include "readily-accessible and easy-to-use" settings that can: (1) limit the ability of strangers to contact the minors; (2) prevent third-party or public access to a minor's data; (3) limit features that would increase, sustain, or extend a minor's use of the covered platform (e.g., automatically playing media); (4) permit opting out of algorithmic recommendations; (5) delete the minor's account and personal data; (6) restrict sharing a minor's geolocation information; and (7) limit time spent on the platform. The defaults for these settings must be the "strongest option[s] available" and the platform can't use features that would encourage minors to weaken or turn off the safeguards. The bill does not specify whose choice would control if the parent and child both try to change the same settings.

- **The platform must enable parental controls by default for any user it reasonably believes to be a minor.** These include tools allowing parents to: (1) control the minor's privacy settings; (2) restrict purchases; (3) track the minor's time on the platform; (4) change the default settings; and (5) control options necessary to prevent the harms described above. The platforms also must provide clear and conspicuous notice to the minor when parental controls are on, as well as a mechanism for a parent to submit reports of harm to a minor.

- **The platform must provide detailed disclosures about its safeguards, risks, algorithms, and advertising.** As part of these requirements, the platform must obtain the minor's or parent's acknowledgement of the risks before the minor can use the platform; label and explain any advertising (including targeted advertising) aimed at minors; and allow minors or their parents to "modify the results of the algorithmic recommendation system" (as well as opt-out, as noted above).

- **Each year, the platform must obtain a third-party audit of the risks posed to minors and issue a public report.** In addition to identifying the risks, the audit must address (1) what efforts the platform has taken to prevent or mitigate them; (2) how algorithms and targeted ads can harm minors; (3) how the platform collects and uses sensitive data, including geolocation, contacts, and health data; and (4) who is using the platform and for how long, by age ranges.

- **The bill gives the FTC APA rulemaking and civil penalty authority, and authorizes AG enforcement.** Other provisions (1) give independent researchers access to the platform's datasets; (2) direct the FTC and the Department of Commerce to establish guidelines for market

or product research; (3) require a multi-agency study on age verification options; and (4) establish a Kids Online Safety Council to advise on the Act's implementation.

Will this be the bill that breaks the federal privacy law stalemate and makes it into law? We suppose it's possible. This bill is bipartisan, and Chair Cantwell is dangling the possibility of a markup – a rare event (at least lately) for a federal privacy bill. On the other hand, we're already in an election year and Congress has a lot of other matters on its plate. Further, the extraordinary reach of the bill, coupled with its lack of clarity on a number of issues, suggest that many changes would be needed before this bill could become law.

Still, regardless of the outcome of this particular bill, it confirms what we predicted in October – that Congress has its sights on kids' privacy, and that "kids" now includes teens 16 and under. Stay tuned.

Please join us on Thursday, February 24 at 4:00 pm EST for Privacy Priorities for 2022**,** the second installment of Kelley Drye's 2022 practical privacy series. Register here.