Insight

Assessing Child Online Safety Legislation

JOSHUA LEVINE | MARCH 29, 2023

Executive Summary

- House and Senate lawmakers plan to re-introduce several bills intended to protect children's safety online, key among them the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act and the Kids Online Safety Act; additionally, policymakers are considering the more sweeping Making Age-Verification Technology Uniform, Robust, and Effective Act introduced by Senator Josh Hawley in February.
- These bills are not likely to substantially improve online safety for children, yet all could have the unintended effect of exposing children to more harm while eroding all users' online experience and raising constitutional concerns.
- This piece examines each bill's approach to improving children's digital safety and explains how these proposals could fail to meet their goals and jeopardize the functionality of features on which users rely; it also considers alternative approaches to protecting children online, such as creating a federal data privacy law, crafting legislation targeting specific technological features, and improving existing digital literacy initiatives and resources.

Introduction

House and Senate lawmakers plan to re-introduce several bills intended to protect children's safety online, key among them the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN-IT) and the Kids Online Safety Act (KOSA). These bills gained significant traction in the last Congress and offer different approaches to protecting children online. EARN-IT would allow victims of digitally shared child sexual abuse material (CSAM) to hold platforms liable for failing to implement measures to adequately protect children, while KOSA would restrict algorithmic recommendation of content harmful to

children. A more radical approach is embodied in the Making Age-Verification Technology Uniform, Robust, and Effective Act (MATURE) introduced by Senator Josh Hawley (R-MO) in February, would prohibit the use of social media by minors writ large. Federal legislation will likely inform efforts in states across the country where lawmakers have already begun to propose complementary legislation.

While these bills are intended to make the online experience safer for minors, they are not likely to achieve their stated goals, and may well degrade the internet experience for all users. For example, some provisions in these bills would force websites to collect and retain sensitive user data, as well as push websites to limit access to content or gate services based on subjective assessments of harm. These requirements would erode the quality of online services for users of all ages and even jeopardize children's private information.

This insight explains how each bill would attempt to make the internet safer for children and examines how such attempts could exacerbate existing harms – and may create new ones. It also considers alternative approaches to addressing concerns about children's safety, such as passing a federal online privacy standard, reviewing the specific technologies drawing criticism from lawmakers, and improving existing resources for digital literacy to help children safely navigate the internet.

Proposed Legislation to Protect Children Online

EARN-IT

The EARN-IT Act would amend Section 230 of the Communications Act of 1934 to allow for civil action against internet platforms under federal child sexual exploitation laws, meaning victims can hold platforms liable if they fail to take adequate steps to identify and remove CSAM. Currently, platforms can be held criminally liable for these claims, but the EARN-IT Act would give victims leverage to bring civil action and seek damages from platforms, as well. EARN-IT also would create a commission to develop best practices for digital platforms to prevent and respond to CSAM online. While adherence to these best practices isn't required, courts will likely look to these guidelines to provide clarity on the types of actions platforms should be taking to address CSAM, and thus may find platforms liable if they fail to comply with these best practices.

The bill presents serious tradeoffs related to privacy-enhancing technologies such as end-to-end encryption (E2EE). Encryption ensures minors can communicate with friends and family without fear of their information being exposed online. The bill states that offering E2EE cannot be an "independent basis for liability," but this does not preclude the technology from being used as evidence alongside other charges to argue a site failed to respond to

CSAM. An attorney could argue that offering E2EE contributed to the spread of CSAM on a platform alongside other factors such as inadequately blocking flagged content. In response, platforms could be incentivized to scan users' messages and cease offering E2EE. As cybercrime and phishing attacks grow in frequency, and large social media platforms are targeted by hackers who expose sensitive user data, reducing platforms' offering of E2EE would likely erode users' privacy.

Further, by effectively pushing platforms to adhere to the commission's best practices, the platforms' actions would likely run afoul of the Fourth Amendment, potentially imperiling law enforcement actions related to CSAM. For example, proactively scanning messages at the behest of law enforcement could be construed by courts as an unreasonable search. If courts refuse to allow evidence from such searches, those distributing CSAM will not be held accountable, a result at odds with the intentions of EARN-IT's drafters.

KOSA

KOSA would impose a "duty of care" that online platforms must meet to protect underage users, largely targeting the algorithmic amplification of potentially harmful content to minors. Specifically, the duty of care would require platforms to act in the "best interests of a minor that uses the platform's products or services." The duty of care would give enforcement agencies broad authority to target practices, such as algorithmic ranking and recommendations, as well as content that could result in harm to minors such as posts related to mental health disorders, addiction, and sexual exploitation. This could encourage platforms to proactively address concerns raised about the impact their services have on children, and if they fall short, allow regulators to act. In addition to the duty of care, the bill would also impose default safeguard settings and built-in tools for parents to monitor online activity and restrict certain technological offerings.

KOSA's requirements for protection by design comes with significant risks. The bill would increase the amount and types of sensitive information collected about minors and potentially diminish the online experience for children and all users. For example, the bill's duty of care would likely require onerous data collection from users to determine whether they are minors in order to avoid legal jeopardy. Further, the bill would specifically target recommendation algorithms, acting on recent reports about how algorithmic amplification of some content can harm children online. Algorithms are proprietary technologies that distinguish firms from one another, serve relevant content to users, and outcompete rivals. The bill's duty of care, however, makes platforms potentially liable for serving content that could be construed as "harmful," which could lead to educational content trying to prevent addiction, self-harm, and sexual exploitation being censored to avoid liability. Worse, compelling firms to build algorithms that conform to what lawmakers and regulators deem

appropriate is a slippery slope legally and ignores consumer and producer welfare created from algorithmic recommendations and educational content, respectively.

MATURE

The MATURE Act would restrict children under the age of 16 from creating an account on a social media site. To enforce the ban, the bill would require users to provide a scan of government-issued identification to create an account. In addition to verifying and storing this sensitive information, companies would be required to satisfy compliance audits with the Federal Trade Commission (FTC) to ensure age verification for all accounts. If a platform does not meet compliance requirements, it could face litigation from individuals through a private right of action and from the FTC under Section 2 of the Federal Trade Commission Act.

MATURE would require invasive data collection from anyone seeking access to a wide array of websites, not just large social media platforms. The bill is reminiscent of China's "Great Firewall," which restricts the number of websites users can access and conditions access on providing government-issued identification. Two-thirds of Americans do not feel comfortable providing government-issued identification to access social media, rising to 70 percent when asked about providing the identification of their children.

Following MATURE's design, state legislatures across the country are proposing and passing legislation that would require individuals to provide government-issued identification to access online platforms. Nevertheless, previous attempts to restrict minors from using certain social media platforms have not curtailed online interactions and have instead merely pushed such users onto less-curated platforms where less is done to identify potential harms. Such a policy disregards any benefits minors glean from online communities, and could put American children at a disadvantage compared to their international peers in terms of building digital skills and evaluating the tradeoffs of digital technology. The bill would also effectively eliminate online anonymity, which promotes free expression and privacy for users of all ages. Rather than grapple with the difficult tradeoffs of children accessing content online, MATURE would undermine users' privacy, impose onerous regulations on a variety of websites, and effectively eliminate online anonymity.

Recommendations

To accomplish the goal of protecting children online, lawmakers may find that a more targeted review of problematic technological features could better avoid the pitfalls of KOSA, MATURE, and EARN-IT. To that end, lawmakers can pursue more comprehensive legislation to improve the experience for all users, including children.

First, lawmakers could consider creating a federal data privacy law. Providing a uniform privacy standard that applies to all users would establish a baseline for how websites handle, collect, store, and use consumer data. Such an approach would provide consistent regulatory clarity, no matter the website's size or a user's location. This consistency ensures users that startups and incumbents face the same incentives to protect their data, which lowers the cost of switching platforms or experimenting with a new entrant. This approach would also nudge developers to design products with privacy in mind, protecting consumers, fostering trust between users and platforms, and promoting innovation without compromising individual privacy. With a federal privacy law, platforms would have strong incentives to better manage and protect children's information, limiting the risk that nefarious actors could use such information to harm children.

Further, if specific technologies such as E2EE, algorithmic amplification of harmful content, or even social media generally present concerns for lawmakers, Congress should review the aspects of these technologies it believes may be harmful. By holding platforms liable for the use of these technologies and their role in providing subjectively harmful content, the bills would incentivize firms to limit their use and offering entirely. Because legislation designed to protect children could have significant ripple effects for such technologies broadly, Congress should evaluate the benefits and costs these technologies offer rather than ban them per se under the auspices of protecting children.

Beyond regulation, lawmakers should evaluate the benefits of existing digital literacy programs and consider potential improvements. Some research has shown that minors with higher digital literacy skills were better prepared to deal with online harms, avoid harmful experiences, and cope with negative emotions related to digital interactions. The Department of Education, several state and city education departments and organizations, and international organizations have resources for students, parents, and educators related to digital literacy.

Conclusion

Congress designed EARN-IT, KOSA, and MATURE to improve protections for children online, but these bills threaten to exacerbate existing harms and may even create new ones. While protecting children online is an important goal, lawmakers must work to ensure that legislation does not inadvertently expose children to additional harm or unnecessarily erode all users' online experience. Instead, Congress should more narrowly target areas of concern by passing a federal data privacy standard, as well as evaluating existing digital literacy programs and considering improvements that would enable users to better navigate the benefits and costs presented by online platforms.