Insight

Sammy’s Law of 2023: A Novel Approach to Protecting Children Online

JOSHUA LEVINE | JANUARY 23, 2024

Executive Summary

- A bipartisan group of lawmakers on the House Energy and Commerce Committee introduced Sammy’s Law of 2023, also known as the Let Parents Choose Protection Act, to make more tools available for parents to protect their children from harmful online interactions.
- Whereas previous child online safety bills sought to place significant restrictions on social media platforms regarding the type of content they could host for minors, Sammy’s Law opts for a different approach by requiring platforms to allow third-party safety software providers to access their application programing interfaces; these tools, the bill’s proponents claim, would help parents better manage their children’s online interactions.
- Sammy’s Law, however, could raise concerns surrounding digital privacy, heightened parental tracking and restrictions of internet exploration, and the FTC’s greater role in the oversight of these tools the bill ascribes to it.

Introduction

In an effort to improve kids’ online safety, Representative Debbie Wasserman Schulz (D-FL) introduced Sammy’s Law of 2023, also referred to as the Let Parents Choose Protection Act to help keep kids safe online. The bill is named after Sammy Chapman, a 16-year-old who overdosed after taking fentanyl-laced drugs he acquired through the social media platform Snapchat. It currently has five cosponsors.

Whereas previous child online safety bills sought to place significant restrictions on social media platforms regarding the type of content they could host for minors, Sammy’s Law opts for a different approach by requiring large social media platforms (LSMPs) to allow third-party safety software providers (TPSSPs) access to the platform’s application programing interface (API), rules that enable various apps and tools to communicate with one another. These TPSSP tools are designed to allow a child or parent to utilize APIs to manage a user’s experience – such as by notifying a parent about the users or content their child is interacting with – which could alert parents of concerning behavior.

The bill’s drafters argue that this approach empowers children and their parents to craft an online experience they deem appropriate and safe, notably differing from other online safety legislation that would require platforms adhere to a duty of care or age-gate their services. This approach also creates the opportunity for the growth of “middleware,” a concept whereby software or API tools act as an intermediary or add-on to a platform, providing an end-user a more tailored, individualized experience. This would, in theory, give parents greater control over the content shown to their child and data collected about them.

Some of the bill's provisions could raise concerns; notably, its embrace of third-party tools incentivizes increased tracking and collection of sensitive information on minors and ignores the potential second and third order effects of allowing parents to curate and track their child's online interactions. Further, the bill empowers the Federal Trade Commission (FTC) to issue guidance defining what platforms qualify as LSMPs and TPSSP and to act as the chief enforcer of those guidelines, raising concerns about impartiality and effectiveness.

Sammy's Law and Efforts To Protect Kids Online

Federal and state lawmakers are increasingly focused on mitigating potential harms related to children's use of the internet, particularly social media. Congress has held hearings on the topic, and lawmakers have introduced legislation that would impose a duty of care on platforms when designing their products, expand the scope and requirements of the Children Online Privacy Protection Act, and remove civil liability protections for platforms in cases related to child sexual abuse material, respectively. At the state level, lawmakers have passed laws that require users to provide a government ID to access social media platforms, impose duty-of-care requirements on online platforms, and have even banned users under the age of 18 from using social media.

Sammy's Law takes a different approach and attempts to address concerns raised around children's use of social media by allowing users and their parents to utilize TPSSPs on LSMPs. The law would require that LSMPs allow third-party TPSSPs to access APIs to monitor, screen, or prevent users from accessing certain features of social media platforms and/or inform parents of what types of content with which children are engaging or even with whom they are communicating on an app or platform. Proponents of the bill argue allowing TPSSPs access to APIs would give parents greater control over the online content and users their child interacts with.

Platforms, Safety Providers, and the FTC

There are three main components of the bill, including thresholds and requirements for LSMPs, those for TPSSPs, and the delegation of enforcement powers to the FTC and outlining the agency's responsibilities for establishing guidelines for covered firms.

LSMPs

Sammy's Law would designate any platform that has more than 100 million monthly generally active users or generates more than $1 billion in gross revenue per year as an LSMP, with certain exclusions such as platforms for professional services or those that lack a messaging feature. Within 30 days of a platform being designated a LSMP, it must make information available to any registered TPSSP to facilitate the use of software that allows users and parents to manage an account's settings related to interactions on the platform, visibility and access of user's profile, and data portability. After designation, the LSMP must register with the FTC. Critically, LSMPs are protected from court claims arising from data transfers to TPSSPs if they complied with the law "in good faith."

TPSSPs

For TPSSPs, the bill would establish requirements for market participation and set guidelines for revocation of a license to offer services. In order to qualify as a TPSSP, the firm must be based in the United States, engaged solely in the business of "internet safety," only collect and use data as a means to protect children from harm, and disclose to all users of such software how it functions and what data is being collected. If a provider violates the terms of the law, the FTC can move to de-register the service as an approved provider.

FTC

The legislation would empower the FTC to draft operational guidance for both LSMPs and TPSSPs, issue biennial reports on compliance by both types of firms, and bring enforcement actions for violations of the law. As a condition to access LSMPs' APIs, participating TPSSPs must register their service with the FTC and affirm they satisfy the requirements listed above. The FTC would publish guidance for maintenance of reasonable safety standards for LSMPs and TPSSPs within 180 days of enactment and publish a list of approved TPSSPs on the FTC website. If a TPSSP violates any of the terms of the law or fails to follow the FTC's guidance, it could be de-registered by the agency and removed from the approved list of providers. The FTC would also be required to establish a system for reporting violations of the law.

A violation of the law shall be treated as an unfair or deceptive act or practice under the FTC Act, which empowers the agency to bring enforcement actions against violators including civil penalties up to $50,120 per violation.

Proving Ground for Middleware?

The law's requirements could create a test-case for "middleware" tools to better curate an individual users' experience on a LSMP. The concept first emerged in the 1980s, and refers to software that connects applications and operating systems. With rising concerns about the practices of dominant online platforms and the implications for free speech, privacy, and safety online, middleware solutions can allow users to better exercise control over their online experience. While conceived as a way to increase competition and personalization within the market for digital platforms, the concept can be used in the online safety context as well.

For example, the TPSSPs would function as an intermediate layer between what platforms such as TikTok or Instagram present and what the user is interacting with on their own personal device. The software could add additional content filters, restrict problematic functionalities, and impose greater control over data collection and use. And though leading parental control software companies already offer some of these functions on-device or on-network, allowing them to connect to platform's APIs would create greater functionality and increase control by users and their parents.

Why Can't You Just Meet Me in the Middle?

Despite the potential benefits and innovative approach to mitigating online harm, the bill does have some potential problems with regard to digital privacy, unintended harms of heightened parental tracking, and the ability for the FTC to carry out the duties ascribed to the agency.

First, the bill could incentivize additional tracking of minors on large platforms, which increases user value as a target for hackers and cybercriminals. Under current law, sites may not collect or monetize data on users under the age of 13 without parental consent. This bill would cover any user under the age of 17, so it would impact between 40–65 million potential users in the United States. Cybercrime and hacking operations are continuing to increase, with notable breaches of allegedly secure parental safety tools. Research on the costs of data breaches notes that in addition to initial costs to firms and users such as reputational harms, security upgrades, lawsuits, and fraud, there are longer-run effects. These long-run effects include difficulty securing credit cards and various types of loans as well as negative psychological impacts. Opening-up APIs to third-party software providers could increase the chances of a security breach or potential network security issues, especially when data must be expressly transferred to the third parties.

Second, the bill could encourage further digital surveillance of children by their parents, which if not done in conjunction with education, may curtail the internet's many benefits and may delay potential harm until after a child turns 17. Protecting children from harmful content and interactions is a worthy endeavor, but parents, educators, and lawmakers should consider the tradeoffs of various levels of control. Research has shown that minors who encounter more potentially harmful content are also those best equipped to navigate it in the future. Literature on digital literacy supports the idea that educating children on how to use the internet safely and allowing them to learn by doing can be an effective way to mitigate potential online harm. Researchers from the National Academies of Sciences, Engineering, and Medicine recently published a study that recommends digital literacy education to help children learn to navigate the tradeoffs of spending time online. Depending on how the TPSSPs are marshalled, parents may prevent their children from ever developing these independent skills, which could have harmful second and third order effects as they age.

Finally, the bill ascribes the FTC power to enact, judge, and enforce a regulatory regime for TPSSPs. A case before the Supreme Court, *Axon v. FTC*, calls into question the ability of the agency to adjudicate civil claims with its in-house administrative law judge, which could alter how the FTC carries out its duties. Considering there are active cases challenging such authority, lawmakers may want to consider how a ruling limiting the FTC's administrative authority could impact its ability to carry-out and enforce the law. Further, while the agency is the pre-eminent data protection agency in the United States, specifically on issues related to online data and children, the National Institute of Standards and Technology (NIST) has extensive experience developing standards related to cybersecurity and could be a worthwhile partner. Drafters could include more specifics in the bill related to guidance or creating alternatives for certifying the providers as trustworthy sources or considering existing standards as a starting point for guidelines.

Conclusion

By allowing third-party access to APIs, Sammy's Law could better equip children and their parents to navigate online spaces, as well as promote the use of "middleware" tools as a potential solution to larger issues of online content policy. This approach diverges from other notable proposals focused on kids' online safety by empowering parents with new tools to tailor their own child's experience online rather than require platforms adhere to a duty-of-care or require age verification for all minors. Despite the potential benefits, however, the bill could also encourage additional data collection on minors and raise potential cybersecurity concerns. Lawmakers should work to minimize these risks and consider the potential costs to users, firms, and digital markets broadly as they debate the bill.