The STOP CSAM Act Would Put Security and Free Speech at Risk

A new U.S. Senate bill introduced this week threatens security and free speech on the internet. EFF urges Congress to reject the STOP CSAM Act of 2023, which would undermine services offering end-to-end encryption, and force internet companies to take down lawful user content.

TAKE ACTION

TELL CONGRESS NOT TO OUTLAW ENCRYPTED APPS

The bill is aimed at removing from the internet child sexual abuse material (CSAM), also known as child pornography. Existing law already requires online service providers who have actual knowledge of "apparent" CSAM on their platforms to report that content to the National Center for Missing and Exploited Children (NCMEC), which is essentially a government entity. NCMEC then forwards actionable reports to law enforcement agencies for investigation.

The STOP CSAM Act goes much further. The bill applies to "interactive computer services," which broadly includes private messaging and email apps, social media platforms, cloud storage providers, and many other internet intermediaries and online service providers. The bill does four main things:

- It makes it a crime for providers to "knowingly host or store" CSAM or "knowingly promote or facilitate" the sexual exploitation of children,

including the creation of CSAM, on their platforms.
- It creates a new civil claim and corresponding Section 230 carveout to encourage private lawsuits against internet companies and app stores for the "promotion or facilitation" of child exploitation, the "hosting or storing of child pornography," or for "making child pornography available to any person"—all based on the very low standard of negligence.
- It requires providers to remove (in addition to reporting and preserving) "apparent" CSAM when they obtain actual knowledge of the content on their platforms.
- It creates a notice-and-takedown system overseen by a newly created Child Online Protection Board, requiring providers to remove or disable content upon request even before an administrative or judicial determination that the content is in fact CSAM.

The Bill Threatens Security by Undermining the Viability of End-to-End Encryption Services

The bill makes it a crime to *knowingly* "host or store child pornography" or "promote or facilitate" the sexual exploitation of children. The bill also opens the door for civil lawsuits against providers for the *negligent* "promotion or facilitation" of conduct relating to child exploitation, the "hosting or storing of child pornography," or for "making child pornography available to any person."

The terms "promote" and "facilitate" are broad, and civil liability may be imposed based on a very low negligence standard, the lowest state-of-mind standard under the law. This is the same standard applied to legal cases involving car accidents and other situations where the defendant did not intend for harm to result, but it did nevertheless due to carelessness or even simply a failure to act.

Creating new criminal and civil claims against providers based on broad terms and low standards will undermine digital security for all internet users. Because the law already prohibits the *distribution* of CSAM, the bill's broad terms could be interpreted as reaching more *passive* conduct like merely providing an encrypted app.

Due to the nature of their services, encrypted communications providers who receive a takedown notice may be deemed to have "knowledge" under the criminal law even if they cannot verify and act on that takedown notice. And there is no doubt that plaintiffs' lawyers will (wrongly) argue that merely providing an encrypted service that can be used to store any image—not necessarily CSAM—negligently facilitates the sharing of illegal content.

Not every platform will have the resources to fight these threats in court, especially newcomers that compete with entrenched giants like Meta and Google. Encrypted platforms should not have to rely on prosecutorial discretion

or favorable court rulings after protracted litigation. Instead, specific exemptions for encrypted providers should be addressed in the text of the bill.

TAKE ACTION

TELL CONGRESS NOT TO OUTLAW ENCRYPTED APPS

The Bill Threatens Free Speech by Creating a New Exception to Section 230

The new civil claim in the bill comes with an exception to Section 230, the foundational law of the internet and online speech and innovation. Section 230 provides partial immunity to internet intermediaries when sued for content posted by their users. Creating a new exception to Section 230 that allows providers to be sued for "facilitating" child sexual exploitation merely based on the provision of a platform that hosts third-party content will harm free speech online.

Section 230 creates the legal breathing room for internet intermediaries to create online spaces for people to freely communicate around the world, with low barriers to entry. However, creating a new exception that exposes providers to more lawsuits will cause them to limit that legal exposure. Online services will censor more and more user content and accounts, with minimal regard as to whether that content is in fact legal. Some platforms may even be forced to shut down or may not even get off the ground in the first place, for fear of being swept up in a flood of litigation and claims around alleged CSAM. On balance, this harms all internet users who rely on intermediaries to connect with their communities and the world at large.

The Bill Threatens Free Speech by Requiring Providers to Take Down Potentially Lawful Content Before a Legal Determination That It Is CSAM

The STOP CSAM Act's removal provisions pose significant threats to free speech online.

In one provision, not only must providers report "apparent" CSAM to NCMEC after obtaining actual knowledge as required by existing law; they must now remove it from their services without a judicial determination that the content is, in fact, illegal CSAM. We already know that some reports can be incorrect.

In another provision, the bill creates a convoluted notice-and-takedown regime overseen by a new Child Online Protection Board, where individuals may file complaints against companies to remove alleged CSAM from their platforms. This system is ripe to be gamed by bad actors, leaving lawful user content

exposed to bogus takedown requests. First Amendment-protected content involving sexuality, sexual orientation, or gender identity will likely be targets of frivolous takedown notices.

The notice-and-takedown procedures work like this: in response to a takedown notice, providers must either (1) remove the content within two days or (2) notify the user that they are unable to do so through reasonable means. A provider can also informally contact the complainant if it believes the content is, in fact, protected speech. But if that doesn't work, a provider's only remedy is to disable the content and challenge the takedown notice at the Board. Even if a provider wins a challenge to a takedown notice, the fact that legal content can be taken offline before a final decision is antithetical to free speech. Moreover, because of patently unconstitutional gag rules surrounding the Board's review, the *creator* of protected content that is the subject of a frivolous takedown request will not be put on notice of the process until a final determination.

There are other reasons to question the quasi-judicial Board process. It is likely to be underfunded and understaffed to adjudicate internet-wide takedown disputes. Additionally, the Board process appears to be voluntary, and to participate parties must first agree to give up the right to "have the dispute decided" by a federal court.

This all assumes, however, that providers will fight frivolous content complaints at the Board in the first place. It is more likely that providers will be incentivized to simply remove lawful content subject to a complaint to avoid the expense and burden of an administrative or judicial process.

Congress should avoid passing a law that will undermine security and free speech online. Instead, Congress can encourage the executive branch to enforce existing laws. Since 2008, providers have faced large fines if they fail to report CSAM after receiving actual knowledge of its presence on their platforms. Yet we know of no case where the federal government has ever enforced this provision. Similarly, the FTC has authority to police deceptive conduct under Section 5 of the FTC Act. To the extent providers make promises to their users about removing CSAM, the FTC can enforce those promises by investigating any claims that providers failed to follow their own content policies.