March 11, 2025

The Honorable Chuck Grassley
Chairman
Senate Committee on the Judiciary
Washington, DC 20510

The Honorable Dick Durbin
Ranking Member
Senate Committee on the Judiciary
Washington, DC 20510

Re: STOP CSAM Act Would Harm Vulnerable Americans

Dear Chairman Grassley, Ranking Member Durbin, and Members of the Committee:

The Electronic Frontier Foundation (EFF) writes to reiterate our opposition to the Strengthening Transparency and Obligation to Protect Children Suffering from Abuse and Mistreatment Act of 2023 (STOP CSAM Act).[1] We opposed the original version of the STOP CSAM Act in the previous Congress, and we are concerned to see the Committee moving to consider the same flawed ideas in the current Congress. While we appreciate the robust conversations we've had with the staff of the sponsors of the bills, our concerns remain. We urge the Committee to find a different way to address this problem.

EFF is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 39,000 members. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law to technology.

We understand that the sponsors of these bills say their legislation is intended to protect children from online sexual exploitation—an important and laudable goal. But laudable goals do not always make good law.

STOP CSAM Endangers Encrypted Messages

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). NCMEC then forwards actionable reports to law enforcement agencies for investigation. Existing law also already makes it a crime for anyone, including platforms, to "distribute," "promote," "facilitate" or "possess" CSAM.

STOP CSAM makes it a crime to "promote or facilitate" the sexual exploitation of children. The bill also opens the door for civil lawsuits against providers for the negligent "promotion

[1] S. 1199 in the 118th Congress. https://www.congress.gov/bill/118th-congress/house-bill/7949/all-actions?s=9&r=3&q=%7B%22search%22%3A%22CSAM%22%7D

or facilitation" of conduct relating to child exploitation, the "hosting or storing of child pornography," or for "making child pornography available to any person."

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 application.

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. And due to the nature of their services, encrypted communications providers who receive a takedown notice under a separate section of this bill may be deemed to have "knowledge" under the criminal law even if they cannot verify and act on that takedown notice.

STOP CSAM also creates a new legal exception that allows providers to be sued for "facilitating" child sexual exploitation based on the fact that they host third-party content—including content that they haven't been able to review or moderate.

Finally, the bill creates a convoluted notice-and-takedown regime overseen by a new Child Online Protection Board, where providers may be required to remove lawful content prior to any adjudication that the content is in fact CSAM. This system is ripe to be gamed by bad actors, leaving lawful user content exposed to bogus takedown requests.

The prior versions of the STOP CSAM Act of 2023 threatened the privacy, security, and free expression of digital communications for all users, including children. Giving states and private litigants the power to threaten private companies with criminal prosecution and costly civil litigation unless they scan all users' private messages shows blatant disregard for the millions of law-abiding people who depend on secure messaging to safely communicate. Military families, survivors of domestic violence, victims of identity theft and numerous others: there are many people for whom true end-to-end encryption is vital for personal safety and peace of mind.

Strong Encryption Protects Everyone's Safety and Privacy

In the digital world, end-to-end encryption is our best chance to maintain our privacy and security.

In October 2024, the U.S. public learned about a major breach of telecom systems stemming from Salt Typhoon, a sophisticated Chinese-government backed hacking group.[2] This hack infiltrated the same systems that major ISPs like Verizon, AT&T and Lumen Technologies had set up for U.S. law enforcement and intelligence agencies to get "lawful access" to user

[2] Joe Mullin and Cindy Cohn, "Salt Typhoon Hack Shows There's No Security Backdoor That's Only For The "Good Guys,"" Electronic Frontier Foundation (October 9, 2024), available at https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys

data. It's still unknown how extensive the damage is from this hack, which included people under surveillance by U.S. agencies but went far beyond that.

If there's any upside to a terrible breach like Salt Typhoon, it's that it is waking up some officials to understand that encryption is vital to both individual and national security. In fact, in response to this breach, a top U.S. cybersecurity chief said, "encryption is your friend."[3] It's unfortunate that other agencies, including the FBI, continue to push the idea that strong encryption can be coupled with easy access by law enforcement.[4]

It's also notable that key members of the current administration—including Director of National Intelligence Tulsi Gabbard[5] and President Trump himself [6]—have criticized recent efforts by the UK government to circumvent end-to-end encryption relied on by users of Apple's iCloud.

Strong encryption isn't in tension with protection—it's vital for real public safety.

The STOP CSAM Act risks weakening this vital protection. Making communications less secure should not be a policy aim of Congress. Vulnerable people, including victims of domestic violence and children, rely on encrypted communications to establish safe relationships.[7] [8]

Given its significant problems and potential vast impact on internet users, we urge the Committee to reject this bill. This bill will jeopardize the privacy, security, and free speech of every American, and fundamentally alter our online communications.

Tools to Fight CSAM Already Exist

The government has unused tools to fight CSAM. Since 2008, providers have faced large fines if they fail to report CSAM after receiving actual knowledge of its presence on their

---

[3] Raphael Satter, "US Official Fighting Chinese Telecom Intrusions Urge More Encryption," Reuters (December 3, 2024), available at https://www.reuters.com/technology/cybersecurity/us-official-fighting-chinese-telecom-intrusions-urges-more-encryption-2024-12-03/

[4] Matt Sledge, "How to Protect Yourself from the Salt Typhoon Hack, No Matter What the FBI Says, " The Intercept (December 11, 2024), available at https://theintercept.com/2024/12/11/fbi-phone-encryption-salt-typhoon/

[5] Tulsi Gabbard, Response to Senator Wyden and Representative Biggs, Office of the Director of National Intelligence (February 25, 2025), available at https://www.documentcloud.org/documents/25545430-dni-wyden-biggs-response/

[6] "Trump Compares UK's Demand for Apple User Data to Chinese Monitoring," Reuters (February 28, 2025), available at https://www.reuters.com/technology/trump-compares-uks-demand-apple-user-data-chinese-monitoring-2025-02-28/

[7] India McKinney and Erica Portnoy, "Apple's Plan to "Think Different" About Encryption Opens a Backdoor to Your Private Life," Electronic Frontier Foundation (August 5, 2021), available at https://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-opens-backdoor-your-private-life

[8] Fact Sheet: Understanding Encryption: The Connections to Survivor Safety (December 18, 2020), available at https://www.internetsociety.org/resources/doc/2020/understanding-encryption-the-connections-to-survivor-safety/

platforms.[9] Yet EFF knows 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.[10] 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.

Sincerely,

India McKinney
Director of Federal Affairs
Electronic Frontier Foundation

[9] 18 U.S. Code § 2258A - Reporting requirements of providers, https://www.law.cornell.edu/uscode/text/18/2258A

[10] A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority, revised May 2021, https://www.ftc.gov/about-ftc/mission/enforcement-authority