

# STOP CSAM Only Harms Americans' Privacy

---

The STOP CSAM Act of 2025 (S. 1829) risks weakening digital security and opening the door to private lawsuits against services that use encryption. It's the wrong tool for combating child exploitation online.

## **CSAM is Already Illegal—and Responsible Services Already Cooperate**

Federal law already makes it a crime to possess, distribute, or promote child sexual abuse material (CSAM). Platforms with actual knowledge must report it to the National Center for Missing and Exploited Children or face serious criminal and civil penalties under 18 U.S.C. § 2258A. Knowing about CSAM and doing nothing is **not legal** under current law.

## **This Bill Specifically Enables Lawsuits Over Encryption**

S. 1829 would allow civil lawsuits against providers that “recklessly” host CSAM or “facilitate” child exploitation. While this is an improvement over last year’s negligence standard, the risk remains: plaintiffs can target tech providers, large or small, **merely for protecting their users** with technologies like end-to-end encryption.

Plaintiffs can and will argue it’s “reckless” not to scan all user content, even when it would require breaking encryption to do so. These lawsuits will go forward regardless.

## **Encryption is Not the Problem—it’s Part of the Solution**

The bill allows encrypted services to raise a legal defense—but only after they’ve been sued. That’s not good enough. STOP CSAM will require encryption providers to defend against costly lawsuits over content they can’t see or control. And a jury could still consider the use of encryption to be evidence of wrongdoing.

Even if a platform ultimately prevails in court, the accusation of facilitating child abuse will do irreparable damage to its public reputation and user trust. **Americans’ private, secure communications will be put on trial**, over and over again. That’s bad for everyone—including children, domestic violence survivors, and national security.

## **STOP CSAM is a Major Overreach**

Current law has strict reporting requirements about CSAM. It creates new legal exposure that invites speculative lawsuits, even against apps and websites that are working in good faith to fight abuse. It could damage smaller platforms, reduce competition, and drive encrypted apps out of the U.S. market, **without meaningfully advancing child protection**.

EFF urges Congress to oppose the STOP CSAM Act.

**Want more information?** Please contact India McKinney, Director of Federal Affairs at [india@eff.org](mailto:india@eff.org).



The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation.  
Learn More: <https://www.eff.org>