June 11, 2025

Senator Chuck Grassley
Chair
Senate Judiciary Committee
135 Hart Senate Office Building
Washington, DC 20510

Senator Dick Durbin
Ranking Member
Senate Judiciary Committee
711 Hart Senate Office Building
Washington, DC 20510

Dear Chair Grassley, Ranking Member Durbin, and Members of the Senate Judiciary Committee,

We, the undersigned groups, including civil liberties groups and privacy advocates, write to share our opposition to S. 1829, the Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act (STOP CSAM Act).[1] The bill, as reintroduced in the 119th Congress,[2] walks back a number of important privacy protections that had been included in a previous version of the bill.[3] The current bill creates enormous incentives for platforms to stop offering encrypted services that are critical for enabling all of us to have private conversations and securely store files from our most personal moments, like photos from a child's birthday. While all of our groups want to stop the harmful transmission of child sexual abuse material (CSAM), its transmission is already illegal, and these modifications to the bill do nothing more than undermine privacy and security.

The STOP CSAM Act Would Enable The Government and Others to Spy on Private Communications

End-to-end encrypted communications cannot be read by anyone but the sender or recipient. This means government actors, malicious third parties (including foreign governments and criminals), and even the platforms themselves are unable to access private communications as they are being transmitted, or later when they are stored. That is why encrypted services are popular amongst journalists who use encrypted messages to contact their sources, protesters organizing to raise their voices against unjust government action, doctors speaking with patients, domestic violence victims who rely on completely private communications to escape dangerous situations at home, and businesses discussing finances with clients. But there would also be severe consequences for groups that are being targeted by governments both domestically and globally. Encryption not only ensures private and confidential communications,

[1] STOP CSAM Act, S. 1829 (119th Cong.).
[2] *Id*.
[3] S.Amdt.2011, as proposed to Securing Growth and Robust Leadership in American Aviation Act, H.R. 3935 (118th Cong.), https://www.congress.gov/amendment/118th-congress/senate-amendment/2011/text.

but also authentic ones. When messages are encrypted, the sender and recipient know the conversation has not been hijacked.

However, by reintroducing a recklessness standard for certain CSAM-related offenses,[4] the STOP CSAM Act would incentivize platforms to break or abandon end–to-end encryption; which would make it exceedingly difficult to communicate without the threat of surveillance. Under this standard, common platforms could be subject to civil or criminal liability for offering encrypted services, because a court could find that encrypted services may be used for the transmission or storage of CSAM, and offering such services is therefore reckless. Essentially, the recklessness standard threatens to hold providers liable for content that is impossible for the providers to monitor without breaking encryption. A knowledge requirement with regard to each alleged instance of CSAM would be far more appropriate.

This risk of liability creates strong incentives to implement surveillance technologies that break encryption. It is a common myth that encryption can be broken to target only communications from bad actors, but in reality, any carveout is impossible to control, both technically and politically.

If a system allows the platform to access its users' content so that law enforcement or other government agencies can get data, such access could be abused. For example, a rogue (blackmailed, disgruntled, or compromised) employee can access user data, or the platform itself would have the financial incentive to monetize the content of private messages, leading to abuses such as Cambridge Analytica, where the company used personal information taken without authorization to create a system to profile voters. Criminals, competitors or foreign governments could also hack the platform's systems. Furthermore, when a platform has broken encryption for a US government demand, it opens the floodgates to demands from other governments around the globe.

The STOP CSAM Act appears to offer some protections for providers of encrypted services, but these protections are wholly inadequate to safeguard against the incentives to break encryption. For example, the bill provides that the use of encryption cannot be an "independent basis" for holding a provider liable, but the bill does not prohibit a court from considering the use of encryption, so long as it is not the *only* basis for liability, which it never would be. The bill should generally prohibit courts from considering the use of encryption as evidence of a platform's knowledge of CSAM. The bill also provides that it is a defense if it is "technologically impossible" to comply due to encryption, but this only applies to certain offenses, and the mere fact that this

[4] STOP CSAM Act, S. 1829, Sec. 5 (119th Cong.).

defense must be proven after a legal action has been initiated incentivizes providers to preemptively break encryption and avoid litigation costs and the risks of adverse rulings or publicity.

Ultimately, the STOP CSAM Act would severely jeopardize the rights of Americans to communicate online freely, and privately. We urge you to vote “no” on advancing the bill to the Senate floor. The risks are simply too great.

Sincerely,

American Civil Liberties Union
Center for Democracy & Technology
Defending Rights & Dissent
EFF-Austin
Electronic Frontier Foundation
Electronic Frontiers Georgia
Fight for the Future
Free Press Action
Freedom of the Press Foundation
Indivisible Washington’s 8th District
LGBT Tech
Library Futures
New America’s Open Technology Institute
Organization for Transformative Works
Public Knowledge
Restore The Fourth
RootsAction
Society of Environmental Journalists
TechFreedom
TransOhio
Woodhull Freedom Foundation
Yale Privacy Lab