



November 18, 2025

**RE: Civil Rights Organizations Oppose the Inclusion of a “Reckless” Standard in the STOP CSAM Act**

Dear Senator,

On behalf of the Lawyers’ Committee for Civil Rights Under Law and the American Civil Liberties Union, we write to express our strong opposition to S.1829 and urge you to join other Senators in opposing unanimous consent for the bill. The bill, the Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act of 2025 (STOP CSAM), would undermine online encryption, which protects the ability of people to communicate freely, without fear of surveillance. Undermining encryption endangers everyone, but these online protections are particularly critical for racial justice advocates, LGBTQ+ rights activists, and undocumented people at a time when those protections are actively being assailed. To be clear, action should be taken to combat child sexual abuse material (CSAM) online; however, any legislation should not threaten safety and free expression for those who rely on encrypted services to protest, organize, and demonstrate and should not further contribute to over-policing and surveillance. Specifically, no version of STOP CSAM should proceed which would discourage encryption by including a standard lower than “intentional or knowing” promotion or hosting of prohibited material contained in encrypted messages.

For decades, the Supreme Court has recognized that the “inviolability of privacy in group association” is “indispensable to preservation of freedom of association.”<sup>1</sup> The privacy offered by end-to-end encryption services is essential to preserving this freedom of association in the modern world. Dangerous provisions in STOP CSAM threaten the freedom and safety of people of color and other vulnerable communities online and offline by placing our most valuable rights in the hands of Big Tech executives and likely the government, without meaningful judicial oversight.

**Private, Secure Communications Are Essential to Protect Our Rights, Especially in this Crucial Moment.**

Today, private, secure messaging online is made possible by encryption and is essential for activists to organize and vulnerable communities to find spaces online to speak openly without being subjected to hate, harassment, or persecution. Encryption is crucial for those who have the most to

---

<sup>1</sup> *NAACP v. Alabama*, 357 U.S. 449, 462 (1958).

lose by having their privacy violated, including racial justice activists who are routinely targeted for surveillance and abuse by law enforcement<sup>22</sup> and LGBTQ+ individuals who may suffer harm from being outed. Encrypted messages are a frontline tool used to organize and defend our civil rights. Within such a backdrop, end-to-end encrypted services are a lifeline for immigrant communities fearful of government surveillance or for those seeking reproductive and gender-affirming healthcare.

Consider the current context in which this bill is being considered. The current administration has detained hundreds of people overseas without due process based on wartime authorities and has been found to be in violation or contempt of multiple court orders.<sup>3</sup> It has undertaken a massive social media monitoring program, increased its collection of biometrics and genetic data, and begun building a massive, unprecedented database of ordinary U.S. citizens — all aimed at attacking dissidents, protestors, students, and marginalized groups.<sup>4</sup> The recent reconciliation package has pumped billions of dollars into surveillance technology.<sup>5</sup> Hundreds of legal challenges to these actions have been filed since January,<sup>6</sup> and nationwide protests have challenged the administration's aggressive and warrantless raids and detentions, including illegal detentions of American citizens.<sup>7</sup>

In the face of a massive expansion of government surveillance and lawless activity by authorities, the STOP CSAM Act of 2025 would add fuel to a burning fire. It imposes a dangerous standard of liability for end-to-end encrypted messaging services, increasing the probability that providers will undermine or even stop offering encrypted services altogether.

---

<sup>2</sup> Russell Brandom, *How Police Laid Down a Dragnet for Kenosha Protestors*, THE VERGE (Aug. 30, 2021), <https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake>.

<sup>3</sup> Lindsay Whitehurst et al., *'Unquestionably in violation': Judge Says US government didn't follow court order on deportations*, ASSOC. PRESS (May 21, 2025), <https://www.ap.org/news-highlights/spotlights/2025/unquestionably-in-violation-judge-says-us-government-didnt-follow-court-order-on-deportations/>; *Judge finds 'probable cause' to hold U.S. in contempt over deportations*, NAT'L. PUB. RADIO, <https://www.npr.org/2025/04/16/g-s1-60696/judge-contempt-alien-enemies-act> (last updated Apr. 16, 2025).

<sup>4</sup> Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 90 Fed. Reg. 49062 (Nov. 3, 2025); Privacy Act of 1974; System of Records 90 Fed. Reg. 48948 (Oct. 31, 2025); Agency Information Collection Activities; New Collection: Generic Clearance for the Collection of Social Media Identifier(s) on Immigration Forms, 90 Fed. Reg. 44693 (Sept. 16, 2025).

<sup>5</sup> H.R. 1, 119th Cong. (2025); *What's in the 2025 House Reconciliation Bill? Immigration and Border Security Highlights*, AM. IMMIGR. COUNCIL (May 14, 2025), <https://www.americanimmigrationcouncil.org/research/house-reconciliation-bill-immigration-border-security>.

<sup>6</sup> *Litigation Tracker: Legal Challenges to Trump Administration Actions*, JUST SEC., <https://www.justsecurity.org/107087/tracker-litigation-legal-challenges-trump-administration/> (last updated May 23, 2025).

<sup>7</sup> Patrick Smith et al., *Anti-ICE protests held coast to coast after L.A. unrest as national movement grows*, NBC NEWS (June 10, 2025), <https://www.nbcnews.com/news/us-news/anti-ice-protests-held-coast-coast-l-unrest-national-movement-grows-rcna-211980>; *Federal Court Rules in Favor of U.S. Citizen Illegally Detained for Deportation by Florida Sheriff*, AM. CIV. LIBERTIES UNION (May 30, 2025), <https://www.aclu.org/press-releases/federal-court-rules-in-favor-of-u-s-citizen-illegally-detained-for-deportation-by-florida-sheriff>.

## **STOP CSAM Would Dis-Incentivize Encryption Services and Expand Surveillance of Vulnerable Communities.**

The STOP CSAM Act of 2025 creates liability for *reckless* “promotion,” “aiding and abetting,” “hosting,” or “storing” of prohibited materials, meaning that services like cloud storage or one-to-one messaging apps may be liable for their users’ actions, even when the service or platform has no knowledge that users are sending prohibited materials in their private communications. Imposing liability on platforms for users’ private documents and communication does one thing: it fuels Big Tech’s surveillance of us all.

While the bill states that encryption may not be an “independent basis for liability,”<sup>8</sup> that protection is so narrow as to be meaningless, permitting liability so long as the use of encryption is paired with other evidence, no matter how attenuated. Additionally, provisions in the bill purport to exempt end-to-end encryption, but they are too narrow to provide meaningful protection, permitting the use of encryption to still be introduced as evidence against a provider.<sup>8</sup> Platforms that seek to defend their policies not to spy on users must offer a defense for that it would be “technologically impossible” to limit access to prohibited content “without compromising encryption technologies,”<sup>9</sup> a difficult standard for providers to meet and for courts to assess.

A previous version of the bill from last session held online operators liable only for “intentional or knowing” promotion, aiding and abetting, hosting, or storage of CSAM on their platforms and app stores.<sup>10</sup> This language would allow the bill to target bad actors without endangering services that offer encrypted messaging, storage, or services. There are of course other ways to achieve the same end of ensuring that the liability imposed by the bill does not deter companies from offering encrypted messaging services.

However, the current bill poses a real danger of destroying the ability for platforms to offer encrypted communication. Platforms will inevitably restrict such services to shield themselves from legal liability or to surveil and censor user inputs to comply with the mandates of this bill.

This is unacceptable. In seeking to mitigate and prevent the awful harms of CSAM, this bill risks opening a Pandora’s Box that could radically reshape the internet at the expense of vulnerable communities, protestors, and activists who rely on encryption and the safety of private communications to gather and share information freely. Companies will have a business incentive to surveil and access the private communications of their users, lest they be charged with being reckless in not knowing about the conduct of their users. That surveillance will in turn have grave consequences. Recent history clearly shows that platforms will make content moderation decisions

---

<sup>8</sup> STOP CSAM Act of 2025, S. 1829, 119th Cong. § 5(c) (2025), adding 18 U.S.C. § 2255A.(g)(1)-(2) (OLL25620).

<sup>9</sup> *Id.*

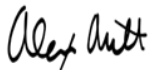
<sup>10</sup> S. Amdt. 2011 to S. Amdt. 1911 to H.R. 3935, 118th Cong. (2024) (proposed), <https://www.congress.gov/amendment/118th-congress/senate-amendment/2011/text>.

based primarily on their private financial interests<sup>11</sup> or political calculations,<sup>12</sup> rather than that of the greater public good. The criminal legal system has always disproportionately surveilled Black and Brown communities and prosecuted them more often and more harshly.<sup>13</sup> Additional surveillance by technology companies' collection, monitoring, and reporting requirements will likely be disproportionately targeted at people of color and other vulnerable communities due to algorithmic or human bias.<sup>14</sup> Creating new avenues to surveil private online activity will only create new online harms and make platforms less safe for vulnerable communities, protestors, and activists .

Privacy rights are civil rights, and encryption is a necessity for privacy in an always-online world. Civil rights cannot be collateral damage in the effort to improve online safety. The solution to preventing CSAM is not to place greater power in the hands of online platforms, disincentivize them from offering privacy protecting technologies, and then task them to moderate and interfere with private communications.

For the reasons summarized above, we urge you to oppose any version of the STOP CSAM Act of 2025 that would impede or discourage encryption on platforms by straying from a knowledge-based standard for private messages. Thank you for your consideration of this matter. For any questions or further discussion, please contact Cody Venzke at [cvenzke@aclu.org](mailto:cvenzke@aclu.org), Jina John at [jjohn@lawyerscommittee.org](mailto:jjohn@lawyerscommittee.org), or Alex Ault at [aault@lawyerscommittee.org](mailto:aault@lawyerscommittee.org).

Sincerely,



Alex Ault  
Policy Counsel  
Lawyers' Committee for Civil Rights Under Law



Christopher Anders  
Director, Democracy & Technology  
American Civil Liberties Union



Jina John  
Policy Counsel



Cody Venzke  
Senior Policy Counsel

---

<sup>11</sup> Yi Liu et al., *Implications of Revenue Models and Technology for Content Moderation Strategies*, UNIV. PA. WHARTON SCHOOL (Nov. 23, 2021), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3969938](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3969938).

<sup>12</sup> Kelvin Chan et al., *Meta eliminates fact-checking in latest bow to Trump*, ASSOC. PRESS (Jan. 7, 2025), <https://apnews.com/article/meta-facts-trump-musk-community-notes-413b8495939a058ff2d25fd23f2e0f43>.

<sup>13</sup> Susan Nembhard & Lily Robin, *Racial and Ethnic Disparities throughout the Criminal Legal System*, URB. INST. (Aug. 2021), <https://www.urban.org/sites/default/files/publication/104687/racial-and-ethnic-disparities-throughout-the-criminal-legal-system.pdf>.

<sup>14</sup> Ángel Díaz and Laura Hecht-Felella, *Double Standards in Social Media Content Moderation*, BRENNAN CTR. FOR JUST. (Aug. 4, 2021), <https://www.brennancenter.org/our-work/research-reports/double-standards-social-media-content-moderation>.