



*January 30, 2024*

The Honorable Dick Durbin  
Chairman, Senate Judiciary Committee  
U.S. Senate  
Washington, D.C. 20510

The Honorable Lindsay Graham  
Ranking Member, Senate Judiciary Committee  
U.S. Senate  
Washington, D.C. 20510

CC: Members of the Senate Judiciary Committee

**Re: Senate Judiciary Committee’s January 31, 2024, Hearing on “[Big Tech and the Online Child Sexual Exploitation Crisis](#)”**

Dear Chairman Durbin, Ranking Member Graham, and Members of the Committee,

The undersigned organizations write to urge Committee members to focus their questions at tomorrow’s hearing on child safety on ensuring the technology companies represented at the hearing are appropriately investing in identifying threats to young internet users and developing content-neutral tools to mitigate these threats including tools that empower young people to protect themselves and their privacy and to refrain from advancing legislation that, as currently drafted, undermines their rights.

We strongly agree with Committee members that ensuring young people are safe online is essential. The goal of ensuring safety is not and should not be at odds with supporting young people’s autonomy to access information, use secure communication channels, and make decisions about their online experiences. Compromising the latter goals to achieve an illusory sense of safety will undermine young people’s well-being as well as their fundamental rights. As many of [our organizations have highlighted](#), some of the legislative proposals before the Senate bear this risk and threaten to jeopardize all internet users’ access to information and privacy.

**Access to online services is essential for young people’s development**

Young people rely on online services to stay in touch with friends and family, find and nurture interests, and develop their sense of self. Research has repeatedly shown that in today’s world, social media and secure messaging services are integral for young people and their well-being.

A poll conducted by [Pew Research Center in April 2023](#) found that the 80% of teens report that access to social media helps them feel more connected to their friends' lives, 71% of teens feel like social media is a place where they can be creative, and 67% of teens use social media to support them when they are going through tough times. In particular, marginalized youth such as LGBTQ+ teens and teenagers of color rely on online spaces to nurture their identity, find community, and exchange resources. LGBTQ+ teens use encrypted messaging services and disappearing messaging features offered by social media companies to confide in friends and trusted adults, especially when facing unsupportive or abusive situations at home.

Black-and-white assertions about the role social media plays in young people's lives risks obscuring the real ways young people use and rely on these services. The Surgeon General's [advisory guidance](#) on youth mental health says that social media offers both benefits and drawbacks for young people and that their benefits may be especially salient for marginalized youth. As youth advocate Sarah Philips wrote in [Teen Vogue](#), "the most under-cited part of the [Surgeon General's] report is actually the most important... LGBTQ+ youth actually have better outcomes when they have access to social media and secure online communities."

### **Legislation being reviewed by this Committee could undermine young people's access to critical information and in turn, their well-being**

Proposed legislation before this and other Committees could jeopardize young people's access to information and privacy, and potentially impact their well-being. Bills like the most recent public version of the Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act (STOP CSAM Act), the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2023 (EARN IT Act), and the version of the Kids Online Safety Act (KOSA) that passed through the Senate Commerce Committee in July 2023, contain strong incentives to use content filtering tools and/or eliminate end-to-end-encryption guarantees by weakening or introducing new liability standards for platforms that host user-generated content, some of it that is perceived to be harmful to children.

Creating or increasing the risk of liability that platforms face for hosting certain categories of content will inevitably lead reasonably risk-averse platforms to institute compliance measures, including filtering tools, that sweep far more broadly than those categories. Unclear liability standards such as a "duty of care" which requires companies to prevent a set of harms caused by the design of the platform may result in similar effects with companies developing and deploying aggressive content filters to reduce the visibility of lawful content that platforms fear enforcers may interpret as harmful. The use of these tools is likely to result in over-moderation of First Amendment-protected and developmentally-important speech, including [about gender identity, sexual orientation, and reproductive health](#). The passage of SESTA-FOSTA is one

example where a broadly scoped carve-out of intermediary liability protections [chilled speech](#), particularly by the [LGBTQ+ community](#).

Websites focused on sex education and LGBTQ+ issues have been regularly swept up in attempts to block sexual content due to the imprecise nature of content filtering tools. A study conducted by [Top10VPN](#) in 2021 found that 92% of child-safety apps on Google Play were wrongly blocking at least one LGBTQ or sex-education website including the Trevor Project and It Gets Better as “adult content.” An [EFF analysis](#) of a popular student monitoring tool, GoGuardian, found that a vast majority of sample websites were inaccurately flagged as potentially dangerous just for mentioning information about LGBTQ issues —even when those sites were merely educational or informative. A [WIRED](#) investigation in 2023 into commercial child-safety content filtering tools found that these tools also blocked access to essential information a young person may seek as part of their education and development including websites of Human Rights Watch and Amnesty International, artistic interpretations of The Hobbit, and even press coverage of school shootings. Widespread use of these tools to avoid the risk of liability resulting from legislation like the STOP CSAM Act will only lead to more censorship of essential and lawful speech affecting all internet users’ fundamental rights.

**Proposed legislation would have an outsized impact on all internet users, removing all users’ access to secure communications channels**

Some of the companies represented at the hearing offer secure end-to-end encrypted group messaging services, which according to a recent study by the [Center for Democracy & Technology](#), young people aged 14 to 21 use to stay in touch with friends and family. Ensuring these group chats cannot be intercepted by malicious actors is paramount to the safety of young people, and all internet users. Yet, legislation, including STOP CSAM, EARN IT and KOSA, would incentivize providers not to offer encrypted services or to weaken encryption in order to facilitate additional surveillance of content. This surveillance will be done in the name of protecting child safety, but will instead undermine their [right to privacy](#) and that of all other internet users. Weakening or eliminating access to encrypted platforms would harm all internet users’ right to private communications and in particular harm LGBTQ+ youth who depend on encrypted messages to confide in trusted adults and counselors, journalists who use encrypted messages to contact their sources, doctors who use it to speak with patients, domestic violence victims who rely on completely private communications to escape dangerous situations at home, and businesses discussing finances with clients.

Weakening encryption would also equip law enforcement with easier access to more information on our private communications and social ties, enabling increased government surveillance. For example, a woman in the UK received a 28-month sentence for taking abortion

pills based on her internet searches and [private messages](#). All of us, including children, need to be able to communicate in the digital age without our conversations being spied on.

### **Young people want tools to empower themselves and to keep themselves safe**

Young people have regularly called on technology companies to give them the ability to shape their own healthy, online experiences. What a healthy online experience looks like to one group of young people is likely to be different from another. When CDT researcher Michal Luria spoke with over 30+ young people as part of a study to understand the nature of unwanted encounters young people receive on direct messaging services, many told her that they relied on reporting, blocking, and privacy features to keep themselves safe. Many respondents asked for dynamic tools such as the ability to block certain words in their comments or receive notices when an individual outside of their network is trying to send a message. These tools, the participants aged 14 to 21 argued, helped them shape their online environment and keep themselves safe.

This autonomy is critical for young people's development according to child psychologists. In a separate paper published by the [Journal of Pediatrics](#) in 2023, researchers say that early independence amongst young people is critical for emotional development, future decision-making skills, and can even have better mental health outcomes. Policymakers can bolster this call from young people by asking the technology companies represented at the hearing about how their teams build user tools to promote teenage independence.

Passing legislation that imposes strong incentives for companies to create a one-size-fits-all approach to child safety and remove access to secure communication channels will do more harm than good for marginalized youth and all internet users.

If you have any questions, please do not hesitate to contact Aliya Bhatia, CDT ([abhatia@cdt.org](mailto:abhatia@cdt.org)) or Jenna Leventoff, ACLU ([jleventoff@aclu.org](mailto:jleventoff@aclu.org)).

Sincerely,  
Signatories  
American Civil Liberties Union  
Center for Democracy & Technology  
Electronic Frontier Foundation  
Fight for the Future