May 1, 2023

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

The Honorable Lindsey Graham
Ranking Member
Senate Committee on the Judiciary
Washington, DC 20510

Re: Industry Concerns with S. 1207

Dear Chair Durbin and Ranking Member Graham:

Child sexual exploitation and the creation and distribution of child sexual abuse material (CSAM) are among the most painful and damaging harms that children face. We appreciate your work to protect victims and hold perpetrators responsible. The technology industry takes seriously the shared responsibility to ensure that CSAM is detected and removed from their services and our companies have worked extensively to proactively block and report CSAM and to respond to requests from law enforcement for information pertaining to this criminal activity. online.[1]

The 11 undersigned organizations have serious concerns that the recently reintroduced S. 1207, the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act, would hinder law enforcement's efforts against online child exploitation, disincentivize companies to continue to detect and block CSAM, impair lawful speech and conduct, limit technological innovation, and threaten companies' ability to provide end-to-end encryption, in turn threatening the privacy of millions of law-abiding citizens. We repeatedly shared similar concerns about prior versions of the bill in past sessions of Congress, and our concerns have not been addressed.[2]

---

[1] 18 U.S.C. § 2258A.

[2] Industry expressed these and a variety of other concerns in letters in previous sessions of Congress when the bill was introduced and in advance of the markup, and opposed it being brought to the floor. *See* Letter from CCIA, CTA, IA, i2Coalition, and NetChoice, Re: Concerns with Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (Mar. 5, 2020), *available at* https://www.ccianet.org/wp-content/uploads/2020/03/Tech-Assn-EARNIT-Letter.pdf; Letter from CCIA, CTA, i2Coalition, and NetChoice, Re: Requesting Delay of Markup of S. 3398 (July 1, 2020), *available at* https://www.ccianet.org/wp-content/uploads/2020/07/Tech-Assn-3398-Letter.pdf; Letter from CCIA, CTA, Engine, IA, i2Coalition, and NetChoice, Re: Industry Concerns with S. 3398 (Sept. 18, 2020), *available at* https://www.ccianet.org/wp-content/uploads/2020/09/2020-09-18-Industry-Letter-on-S.-3398.pdf; Letter from CCIA, ACT, Chamber of Progress, CTA, Developers Alliance, Engine, i2Coalition, Mailfence, NetChoice, SIIA, and Tor Project, Re: Industry Concerns with S. 3538 (Feb. 9, 2022), *available at* https://ccianet.org/wp-content/uploads/2022/02/Industry-Joint-Letter-on-S.-3538.pdf.

Technology companies continue to invest significant resources in combating CSAM including through the development of cutting-edge technology and tools that identify CSAM.[3] Companies have also established voluntary industry organizations that work to set industry standards and share best practices throughout the sector with the goal to make the internet as safe as possible.[4] While industry makes tens of millions of CSAM reports to authorities every year, fewer than 1500 prosecutions have occurred annually.[5] Instead of indiscriminate scanning of millions of devices, increased resources for law enforcement are needed to ensure more cases are prosecuted and more perpetrators are stopped.

Technology companies have built and deployed significant new tools that more effectively detect CSAM. Unfortunately, these same companies may be disincentivized to continue such innovation because of this legislation's reliance on enforcement through an unpredictable patchwork of state laws with various reduced and untested scienter requirements. As a result, companies would lose legal certainty in their efforts to combat CSAM because the more proactive and advanced steps a company takes, the more it might subject them to increased potential liability under varying state knowledge standards. This may lead to services not introducing new features or shutting down entirely due to uncertainty over liability risks.[6]

This legislation also raises serious concerns as it jeopardizes the ability of American companies to provide secure end-to-end encrypted communications to consumers worldwide. S. 1207 leaves open the possibility that the provision of encryption services can be used against companies as a negative factor in determining liability. Furthermore, S. 1207 specifies that courts will be able to consider whether a provider utilizes end-to-end encryption as evidence in cases brought under this Act — meaning courts could consider the use of end-to-end encryption as evidence to find a provider as complicit in all CSAM crimes across their service. Companies that provide secure tools that enable encryption would face overwhelming litigation risks and the ability of Americans to privately communicate would be harmed.

Additionally, the bill would threaten the ability of internet services from hosting user-created content due to increased and uncertain liability risks. Some companies would respond by excessively filtering user-generated content, thereby significantly limiting the scope and diversity of free speech online.

---

[3] For example, companies proactively detect and report CSAM to NCMEC's CyberTipline and have developed tools like CSAI Match (video hash matching), PDQ and TMK+PDQF (open-source photo and video matching), and PhotoDNA (photo hash matching). Companies are also part of initiatives like the Technology Coalition and the WeProtect Global Alliance. *See, e.g.*, The Technology Coalition Annual Report (Aug. 2021), https://www.technologycoalition.org/annualreport/; WeProtect Global Alliance and the Technology Coalition, Survey of technology companies (Oct. 2021), https://www.weprotect.org/survey-of-tech-companies/.

[4] Margaret Harding McGill, *Tech giants list principles for handling harmful content*, Axios (Feb. 18, 2021), https://www.axios.com/2021/02/18/tech-giants-list-principles-for-handling-harmful-content.

[5] *See* Table D-2—U.S. District Courts–Criminal Federal Judicial Caseload Statistics (Mar. 31, 2022), https://www.uscourts.gov/statistics/table/d-2/federal-judicial-caseload-statistics/2022/03/31.

[6] Aja Romano, *A new law intended to curb sex trafficking threatens the future of the internet as we know it*, Vox (July 2, 2018), https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom; Samantha Cole, *Craigslist Just Nuked Its Personal Ads Section Because of a Sex-Trafficking Bill*, Vice (Mar. 23, 2018), https://www.vice.com/en_us/article/wj75ab/craigslist-personal-ads-sesta-fosta.

Lastly, we are concerned that the bill would encourage more state legislatures to enact new laws restricting the ability of services to design and implement features that protect the privacy and security of users. These state laws could have the effect of compelling services to conduct searches for CSAM content, raising potential "state actor" problems under the Fourth Amendment, which would make prosecuting criminal activity more difficult.

While we have concerns about S. 1207, we are committed to combating online child exploitation, and look forward to working with members of the Committee on these serious issues.

Sincerely,

ACT | The App Association
Chamber of Progress
Computer & Communications Industry Association
Consumer Technology Association
Developers Alliance
Engine
Internet Infrastructure Coalition
NetChoice
Patreon
Software & Information Industry Association
TechNet

Cc: Members of the Senate Judiciary Committee