September 30, 2020

Re: The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT Act)

Dear Member of Congress:

We write to oppose the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (S.3398, H.R.___) (EARN IT) in its current form for three essential reasons. First, rather than stopping the scourges of child sexual exploitation (CSE) and child sexual abuse material (CSAM), the bill would risk having criminal prosecutions of those who sexually exploit children invalidated on Fourth Amendment grounds. Second, despite an amendment intended to protect encryption, the bill may still compromise the security of encrypted communications tools used by most Americans. Finally, the bill will interfere with the First Amendment rights of adults to use Internet services anonymously and to communicate with minors online, including their relatives.

All three of these problems were greatly amplified by the manager's amendment substitute version adopted by the Senate Judiciary Committee in early July — which has been introduced in the House as a companion bill. While addressing some of our longstanding constitutional and practical concerns, the substitute did not change the essentially coercive nature of the bill.[1] Instead, the substitute version opened the door to state civil and criminal liability far beyond even what the original bill would have allowed under federal law. The Committee did not vote on amendments proposed by Sen. Mike Lee that would have partially harmonized state and federal law. But even with full harmonization, the bill would still create sufficiently broad liability to produce the three effects noted above.

The Bill May Still Compromise Online Security. A further amendment offered by Sen. Patrick Leahy, and accepted at markup, aimed to address concerns that the EARN IT Act could expose

[1] The "best practices" have always been of secondary importance: under the original version, a provider would only have needed their protection to the extent it feared expanded liability.

tech companies to liability simply for offering end-to-end encryption. Ironically, the amendment creates a perverse incentive to encrypt all communications — at least, for those companies whose technology and business model makes that possible. And yet, the Leahy amendment is not the panacea that EARN IT's sponsors have claimed: It remains possible that companies may be sued or prosecuted for deciding not to compromise the security of their apps — *e.g.*, by building in backdoors for law enforcement as "ghost users,"[2] or by adding the capacity for client-side scanning of user communications before or after they are decrypted (so the user can view or hear them) and reporting certain content to centralized servers. Such capabilities might identify some CSE/CSAM, but once added, there is no way to prevent bad actors from using such features for other purposes, including surveillance by the very repressive governments that the U.S. government had in mind when it funded the development of end-to-end encryption.[3] End-to-end encryption cannot protect users if their apps betray them.

First Amendment Violation #1: Restricting Anonymous Speech. The Leahy amendment did nothing to address two related First Amendment problems: First, facing broad liability (both civil and criminal), tech companies may have no choice, as explained below, but to age-verify their users, especially users of encrypted services — *i.e.*, require them to prove their age by providing a credit card or other identification. Thus, EARN IT would do indirectly what the Child Online Protection Act (COPA) of 1998 mandated directly. Both COPA and the Communications Decency Act (CDA) — except for Section 230 — were struck down by the courts because they infringed on adults' right to access lawful content anonymously.[4] If anything, EARN IT raises even greater First Amendment concerns. At least the CDA and COPA focused on content deemed "harmful to minors." EARN IT would affect *all* users of private communications services *regardless* of the nature of the content they access or exchange: If a service is encrypted, the provider of an encrypted service has no way of knowing whether the messages being exchanged are bible verses or CSAM.

Critically, providers would face broad, vague liability not merely for failing to stop the distribution of visual CSAM, but also communications between those who "solicit" CSAM from minors or who "promote" it.[5] In practice, this means that all communications between adults and minors, regardless of the apparent subject, could lead to lawsuits or prosecution. While keyword filtering can, to some extent, identify interactions (on unencrypted services) that might be used for "solicitation" or "promotion" of CSAM between adults and minors, there is no easy

---

[2] Jon Callas, *The 'Ghost User' Ploy to Break Encryption Won't Work* (July 23, 2019), https://bit.ly/36k35oy.

[3] Jeff Stone, *U.S. Government Funded The WhatsApp Encryption*, Vocativ (Apr. 8, 2016), https://bit.ly/33ev7zF.

[4] *Reno v. ACLU*, 521 U.S. 844, 867-68 (1997) (striking down the CDA except for Section 230); *ACLU v. Mukasey*, 534 F.3d 181 (3d Cir. 2008), cert. denied, 555 U.S. 1137 (2009) (upholding the trial court decision striking down COPA).

[5] The proposed Subsections 230(e)(6)(B) & (C) both mention "solicitation" and "promotion." The proposed 230(e)(6)(A) does so indirectly, by allowing civil suits filed under Section 2255, which, in turn, turns on "violations" of Section 2252A, which bars, *inter alia*, the "solicitation" and "promotion" of CSAM.

technological solution that will allow ICS providers to reliably distinguish unlawful "grooming" and "enticement" from ordinary communications. In general, such automated tools have a very bad track record dealing with nuance or context, especially when the true meaning of unlawful conversations are coded to avoid detection. Moreover, ICS providers have no reliable way of distinguishing minors from adult users. Every flirtatious conversation between two adults might also look like "solicitation" of CSAM — and, absent robust identity checks for every user, the site will have no reliable way of knowing that neither user is a minor.

This is why all providers of communications services would face strong pressure to age-verify their users. In practice, no reliable age verification mechanism has ever been developed. Even requiring users to provide credit card information does not actually verify that the person entering that information is not a minor.[6] While requiring credit card information was deemed inadequate to satisfy the age verification mandate in COPA,[7] it remains the only obvious way for websites to attempt to minimize liability under the EARN IT Act.

Absent the Lee amendments,[8] the substitute version would allow state laws to *explicitly* require age verification. But even with his amendments, the bill would create such sweeping liability that, for the first time since COPA, the government would effectively force adults to prove their identity before using digital services. This pressure to age-verify users will be even stronger for encrypted services, since monitoring communications will not be an option for them unless they build-in client-side monitoring. The Leahy amendment will not shield encrypted service providers from this liability.

First Amendment Violation #2: Restricting Adult/Minor Communication. Age-verification would be a necessary but not sufficient step to avoid liability under EARN IT. Once users have been identified as minors, social media services would have a strong incentive to prevent them from communicating with adults, and perhaps an even stronger incentive to prevent them from using encrypted communications services altogether. Both could complicate families' use of Internet services and remote learning. Tech companies, notably Zoom, have faced enormous pressure to encrypt their services to protect users' privacy and prevent security breaches. While not every tech company can ultimately do so for technical and business reasons, those that do are unlikely to bear the cost of offering two versions of their service: the encrypted one for adults and the unencrypted one for minors. Instead, they likely will simply attempt to exclude minors

---

[6] *See Mukasey*, 534 F.3d at 195 (3d Cir. 2008).

[7] To avoid liability for collecting personal information for children under the Children's Online Privacy Protection Act (COPPA), many general audience sites "age-gate" users by simply asking them for their birth date. This would not shield against the liability created by the EARN IT Act.

[8] Both amendments would authorize liability under state laws only "if the conduct underlying the [state] claim would constitute a violation of section 2252 or 2252A of title 18…"

from their service — just as the Children's Online Privacy Protection Act (COPPA) requires today of sites that might attract a "mixed" audience.[9] In short, kids will lose access to valuable services.

The Fourth Amendment Timebomb. If the government conducts "searches" without a warrant, criminal convictions based on that evidence may be tossed out. By the same token, "if a statute or regulation so strongly encourages a private party to conduct a search that the search is not 'primarily the result of private initiative,' then the Fourth Amendment applies."[10] The sponsors of the EARN IT Act have been quite explicit that the purpose of the bill is to coerce greater cooperation with law enforcement: "Companies must do more to combat this growing problem on their online platforms," said Sen. Dianne Feinstein upon introducing the bill in March.[11]

Today, 18 U.S.C. § 2258A(a) requires tech companies to report CSAM to the government, via a special semi-private clearinghouse, whenever they find it. Congress set up for this purpose, the National Center for Missing and Exploited Children (NCMEC). Several defendants prosecuted under the two federal statutes that criminalize the possession, distribution, viewing, etc. of CSE and CSAM (18 U.S.C. §§ 2252 & 2252A) have argued that tech companies are essentially "state actors." According to that argument, those companies would need to convince a judge to issue a warrant before they scanned images and videos uploaded by the defendants to identify matches with algorithmic "hashes" (digital "fingerprints") identified by NCMEC as CSAM.

Courts have rejected these arguments. In *Stevenson*, the Eighth Circuit ruled that AOL had "developed its scanning program for its own purposes, without any prompting or input from the government. AOL began using the filtering process for business reasons: to detect files that threaten the operation of AOL's network, like malware and spam, as well as files containing what the affidavit describes as 'reputational' threats, like images depicting child pornography."[12]

By contrast, in *Ackerman,* the Tenth Circuit decided that NCMEC *is* a state actor, based on the *Skinner* decision.[13] Just as the Supreme Court ruled that the government had effectively required

---

[9] COPPA requires "mixed" audience sites merely to "age-gate" users (ask for age) and to block users that admit they are under 13. Under EARN IT, this will not suffice; websites will have to assume that *all* users might be minors under age 18 and thus require them all to identify themselves by providing a credit card, as COPA would have done.

[10] *United States v. Stevenson*, 727 F.3d 826, 829 (8th Cir. 2013) (quoting *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614-15 (1989)).

[11] *Graham, Blumenthal, Hawley, Feinstein Introduce EARN IT Act to Encourage Tech Industry to Take Online Child Sexual Exploitation Seriously*, Senate Committee on the Judiciary (Mar. 5, 2020), https://bit.ly/3n1utNZ.

[12] *Stevenson*, 727 F.3d at 830.

[13] *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016).

railroads to drug-test *all* employees (even though the regulations technically applied only to some employees),[14] then-Judge Neil Gorsuch wrote that:

> the government surely "encouraged and endorsed and participated" in NCMEC's putative search for the same reasons it "knew of and acquiesced in" that activity: Congress funded the Center, required AOL to cooperate with it, allowed it to review Mr. Ackerman's email by excepting it from various federal criminal laws, and statutorily mandated or authorized every bit of its challenged conduct."[15]

The Senate manager's amendment attempts to make the EARN IT Act less directly resemble the situation in *Ackerman* by removing provisions that would have allowed tech companies to "earn" back their Section 230 immunity by certifying their compliance with the "best practices" developed by a working group dominated by the Attorney General. But these provisions were always of secondary importance: the original bill aimed to coerce the adoption of such practices by exposing tech companies to broad legal liability. In that sense, the bill has become even *more* coercive, as it removes any specific safe harbor, leaving companies to guess how much "more" they must "do" to avoid liability — and under completely unspecified legal standards that could be even lower than the "recklessness" standard of the original bill. In any event, a company's being liable for how it designs and runs its service has the same effect as NCMEC's being "statutorily mandated or authorized" to act as an agent of the government: in each instance the putatively private entity is strongly "encourage[d]" to make choices that are not "primarily the result of private initiative." In this sense, EARN IT is readily distinguishable from the reporting requirement in 2258A, which, the Eighth Circuit has ruled, "does not so strongly encourage affirmative searches such that it is coercive."[16]

Furthermore, so long as ICS providers fear liability based on "recklessness" (or some lower scienter standard), any "best practices" issued under the bill *will* effectively compel changes to how services are designed: Plaintiffs will inevitably point to those standards in pleading their claims, and courts will necessarily weigh those standards in assessing what ICS providers *should* have done. Indeed, this may happen even under an actual knowledge standard for civil liability. Thus, the bill should be further amended to specify that the "best practices" developed by the Commission should not be considered by courts in assessing the liability of ICS providers. At a minimum, to minimize the risk that EARN IT will result in tech companies being considered government actors, the Commission should be required to consider and address the effects any "best practices" might have upon civil litigation.

---

[14] *Id*. at 615 (refusing "to accept petitioners' submission that tests conducted by private railroads in reliance on [these regulations] will be primarily the result of private initiative.").

[15] *Ackerman*, 831 F.3d at 1302.

[16] *United States v. Ringland*, 966 F.3d 731, 736 (8th Cir. 2020), *available at* https://bit.ly/2S7vF44.

Critical to *Stevenson*'s conclusion that AOL was not a government actor was 2258A(f)'s declaration that providers have no legal duty to search for CSAM or to monitor content on their services. The original version of EARN IT contained a similar proviso, but the Senate manager's amendment removed it. Thus, nothing will prevent the bill's vast, ambiguous legal liability from causing tech companies to collect more information about their users and share that with the government. As such, the bill creates a serious risk that today's system of voluntary cooperation between tech companies and law enforcement (necessarily voluntary to avoid triggering the Fourth Amendment's warrant requirement) will come crashing down. This would only help those who sexually exploit children to escape justice.

Sen. Lee's Amendments. At the July markup, Sen. Mike Lee offered two amendments, but withdrew them on the understanding that the bill's sponsors would work with him to address his concerns on the Senate floor before any final vote. His amendments attempt to harmonize the state liability authorized by the manager's amendment version (which creates new exceptions to Section 230's immunity shield) with federal law. The intention behind both is sound, but neither amendment remedies serious problems created by the substitute bill.

Sen. Lee's Criminal Amendment. Lee's amendment to the proposed Subsection 230(e)(6)(B) requires that the conduct at issue in the state criminal charge also "constitute a violation of section 2252 or 2252A." While this *would* harmonize the grounds for liability, it would not require state laws to conform with federal law in penalties and process. As such, the threat of state criminal prosecution could still coerce radical changes to how communications services are designed — raising the First and Fourth Amendment concerns discussed above.

Since 1996, Section 230 has ensured that a single body of consistent federal criminal law governs all Internet services, regardless of who applies it. As the Internet remains an inherently interstate medium, the need for consistency remains as great as ever. There is simply no need to authorize new state laws: the Attorney General already has the power to deputize state, local and tribal prosecutors to enforce Sections 2252 and 2252A,[17] but has simply chosen not to exercise this power. If Congress wants to authorize states to act without waiting for such deputization, it should directly authorize states to enforce federal law — or ensure that state laws mirror federal criminal law in *all* respects.

Sen. Lee's Civil Amendment. Sen. Lee's other amendment would ensure that the proposed Subsection 230(e)(6)(C) would tie state law civil liability to violations of Sections 2252 or 2252A — just as the manager's amendment's proposed Subsection 230(e)(6)(A) would authorize suits under Section 2255 for the same conduct. Both would be a significant improvement compared to the EARN IT Act as introduced, which would have lowered the scienter requirement for suits based on Section 2255 from "actual knowledge" to "recklessness." But even with his amendment,

[17] 28 U.S.C. § 543(a) ("The Attorney General may appoint attorneys to assist United States attorneys when the public interest so requires").

the proposed Subsections 230(e)(6)(A) and (C) would nonetheless mark a significant expansion in liability — raising the Fourth and First Amendment concerns discussed above, while also potentially producing perverse results.

Section 230 has never shielded Internet services from federal criminal law. Thus, they have always been liable for prosecution under Sections 2252 and 2252A if they have actual knowledge of CSE or CSAM. In general, actual knowledge of criminal content is most likely to arise in circumstances where the Internet service is complicit, at least in part, in the creation or development of the illegal content. In those situations, Section 230 would not provide a shield from civil liability under Section 2255 for conduct that would violate either criminal provision. Thus, the shield Section 230 provides from civil liability in this context is limited to cases in which the Internet service ought not to be liable for others' criminality.

Imposing civil liability under any *scienter* standard, even "actual knowledge," creates two distinct problems. First, tying civil liability to knowledge re-creates the very "Moderator's Dilemma" that led Congress to enact Section 230 in the first place:[18] it creates a perverse incentive for websites to avoid gaining knowledge that could lead to liability, such as through monitoring or moderating user communications. Again, ironically, websites would be *more* likely to adopt strong encryption for private communications among users — so that they would not be able to read the contents of users' communications. (Presumably, this is why the original bill relied on a recklessness standard — and why the substitute version allows civil liability under state laws not only for recklessness but, by failing to specify any minimum standard for state laws, also for mere negligence, or even strict liability.)

Second, any scienter-based standard for civil liability — *even an actual knowledge standard* — will be necessarily overbroad (and yet also potentially perverse) in its effects when applied at the scale and speed of Internet services. With billions of pieces of content being posted every day across social media, and hundreds of millions of users accessing such services daily, "actual knowledge" is simply not a workable standard for civil liability.

The existing actual knowledge standard for federal *criminal* liability has allowed prosecution of truly bad actors without creating perverse effects because the evidentiary burden in criminal cases is high: proof beyond a reasonable doubt. But when an actual knowledge standard is combined with the much lower evidentiary bar for civil liability ("preponderance of the evidence"), companies risk being sued based, for example, on allegations that a single employee was told of content on their service by email or tweet. Again, this creates a perverse incentive *not* to monitor or moderate to protect children. But it also means that any time a company is notified of potentially unlawful content or conduct on their service, that notice could be deemed

[18] "CompuServe, as a news distributor, may not be held liable if it neither knew nor had reason to know of the allegedly defamatory … statements." *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135, 141 (S.D.N.Y. 1991).

to create actual knowledge — which, in turn, creates a strong incentive to take down content upon complaint.

If it is too easy to put ICS providers on "notice" of potentially unlawful content, the fear of liability will create a "heckler's veto" that could be used to take down specific content or disable particular accounts. Research consistently shows that platforms exposed to such liability receive numerous false accusations, and often follow the path of least resistance by simply removing lawful speech.[19] Such requests could easily be weaponized by a small group of ideologues to force the takedown of content or users they dislike — making it deeply ironic if Congressional Republicans should embrace the EARN IT Act even as they decry political bias in content moderation.

The dilemma could be particularly acute for services that use strong encryption: if someone alleges that a particular user is distributing CSAM over an encrypted service, and the ICS provider cannot view the contents of that user's communications, it will have no way to resolve the complaint. But leaving the account up risks later being accused of having "actual knowledge" of CSAM distribution. This risk may discourage some sites from offering strong encryption altogether, but it may also simply lead to overzealous takedowns of user accounts.

To some extent, such overly broad effects on protected speech could be avoided by focusing liability on the distribution (*etc.*) of visual depictions, not communications between users (*i.e.*, solicitation and promotion). The bill would still raise hard questions about distinguishing true CSAM from family photos, cartoons, and artworks protected by the First Amendment,[20] but at least it would directly not affect ordinary lawful communications.

—

In short, the Senate Judiciary Committee simply has not finished fixing a bill that is deeply constitutionally flawed. A fundamentally different approach is needed to protect children — an approach that can do so *without* violating either the First or Fourth Amendments, or denying Americans the security and privacy protections that only strong encryption can provide. Most importantly, any new civil liability should be tied not to inherently unworkable *scienter* standards but rather to whether a provider has properly responded to clear, specific notices of CSAM/CSE on their services provided through designated channels. At a minimum, the issues we have raised here require further hearings before any legislation should be considered on the Senate floor and before the House Judiciary Committee marks up this exceptionally complicated bill.

---

[19] Daphne Keller, *Empirical Evidence of "Over-Removal" by Internet Companies Under Intermediary Liability Laws* (Oct. 12, 2015), http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws.

[20] "Constitutionally protected expression . . . is often separated from obscenity only by a dim and uncertain line." *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963).

Sincerely,

TechFreedom

Americans for Prosperity

NetChoice

The Copia Institute

Woodhull Freedom Foundation

Daphne Keller, Director of Program
on Platform Regulation, Stanford
Cyber Policy Center