February 8, 2022

The Honorable Richard J. Durbin
Chair, Senate Judiciary Committee
United States Senate
711 Hart Senate Building
Washington, DC 20510

The Honorable Chuck Grassley
Ranking Member, Chair, Senate Judiciary Committee
United States Senate
135 Hart Senate Building
Washington, DC 20510

cc: Members of the Senate Committee on the Judiciary

Re: Committee Markup of S. 3538, The EARN IT Act (February 10, 2022)

Dear Chairman Durbin, Ranking Member Grassley, and Members of the Committee:

We write to express our deep concerns about S. 3538, the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022 (EARN IT Act). We raised these concerns when the bill was first introduced in the previous Congress,[1] and again when amendments to that bill failed to adequately resolve those concerns.[2] Unfortunately, the reintroduced EARN IT Act fails once more to address the serious harms posed by the bill; indeed, it is worse than the 2020 version.

We share your Committee's goal of combating the twin evils of child sexual exploitation (CSE) and child sexual abuse material (CSAM). We supported—and indeed helped to craft—the tougher criminal provisions in the second House version of the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA) before that bill was married with the unworkable civil liability contained in the Senate bill (SESTA).[3] We have long supported increased funding for enforcement of CSAM and CSE laws, increased funding for victims of abuse, and empowering state, territorial and tribal prosecutors in the fight against CSAM and CSE—but have also explained that EARN IT is not necessary for any of these things.[4]

[1] Letter from TechFreedom to Sen. Lindsey Graham on The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (the "EARN IT Act") (Mar. 5, 2020), https://techfreedom.org/wp-content/uploads/2020/03/TechFreedom-Letter-re-EARN-IT-Act-3.5.2020.pdf.
[2] Letter from TechFreedom to Congress on The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT Act) (sept. 30, 2020), https://techfreedom.org/wp-content/uploads/2020/09/EARN-IT-Coalition-Letter-9.30.2020.pdf.
[3] Letter from TechFreedom to Chairman Bob Goodlatte (Dec. 11, 2017), https://techfreedom.org/wp-content/uploads/2017/12/TechFreedom-Letter-FOSTA-Markup-12.11.17-1.pdf.
[4] *See EARN IT Act Could Hurt Kids and Undermine Privacy of All Americans* at 10-11, TechFreedom (Mar. 5, 2020), https://techfreedom.org/earn-it-act-could-hurt-kids-and-undermine-privacy-of-all-americans/.

In fact, as drafted, EARN IT will undermine criminal prosecution of the most vile crimes against children. It will simultaneously undermine the privacy, security and safety of law-abiding users. Despite claims by the bill's sponsors, the bill will have the overall effect of coercing communications providers not to use "strong" end-to-end encryption (E2EE)—technology that is needed at home and abroad to keep private communications safe from thieves, repressive or hostile foreign governments, wayward government agencies, and other malicious actors. By creating vast new liability for not doing enough to stop CSE and CSAM, the bill will, for the first time, compel private companies to monitor their users' communications. This may sound like an improvement, but it will convert the voluntary efforts of companies into state action subject to the Fourth Amendment's warrant requirement. Because private companies do not, and cannot, obtain warrants before conducting such monitoring, any evidence they obtain will be tainted, and courts will have no choice but to toss out any criminal prosecutions based on such evidence.

Fortunately, there are ways to amend the bill to better effectuate its goals while simultaneously mitigating the risks to the privacy and security of online services. We propose five amendments that we believe would improve EARN IT. But we encourage your committee to hold further hearings on this topic to explore other ways to address concerns about CSAM and CSE, such as updating the reporting requirements established in 18 U.S.C. § 2258A.

Recommendation #1: Restore the Leahy Amendment

In 2020, Sen. Leahy's amendment to EARN IT, accepted at markup, attempted to address concerns that companies could face liability for their decision to offer end-to-end encrypted services.[5] This amendment is critical not only to protect the privacy and security of law-abiding citizens, but also to ensure that those who perpetrate CSAM and CSE crimes do not walk free.

If the government conducts "searches" without a warrant, criminal convictions based on that evidence will generally be tossed out. The same goes for searches conducted by private companies under governmental compulsion: "Even when a search is not required by law, … 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." *U.S. v. Stevenson*, 727 F.3d 826, 829 (8th Cir. 2013) (quoting *Skinner v. Railway Labor Executives' Assn*, 489 U.S. 602, 615 (1989)).

As originally introduced, the EARN IT Act provided just such "strong encouragement" by exposing tech companies to vast new liability for CSAM and CSE unless they complied with government-approved "best practices" for identifying and removing CSAM and referring specific users for criminal prosecution. The manager's amendment made the bill's "best practices" voluntary, and thus appeared to make the bill less coercive. In fact, the manager's amendment merely obscured the bill's coercive effects, which have always come from the liability created by the bill. The "best practices" have always been secondary. Exposing companies to broad liability under uncertain standards would have

[5] EARN IT Act of 2020, S. 3398, 116th Cong. Leahy Amend. (2020), https://www.judiciary.senate.gov/imo/media/doc/Leahy%20Amendment%20to%20S.%203398%20-%20OLL20683.pdf.

effectively compelled them to conduct searches of user communications—a result that would not have been "primarily the result of private initiative."

It would be technically difficult to monitor user communications for CSAM or CSE if a site used strong encryption, and thus, the bill would coerce private companies into abandoning strong encryption to facilitate warrantless searches. The Leahy amendment aimed to avoid triggering the Fourth Amendment by declaring that companies could not be held liable for their use of encryption, their inability to decrypt messages, or their refusal to build backdoors into their products. The new version of EARN IT replaces the Leahy Amendment with language from the 2020 House version of the bill. The two provisions may appear similar, because they involve the same list of three protected activities, but they work so differently that the new House language does the opposite of the Leahy language: rather than protecting encryption, it attacks it by ensuring that providers *will* face greater legal liability. Courts *could* consider their use of encryption, their inability to decrypt messages, or their refusal to build backdoors into their products as evidence to support other claims, so long as none of these is "an independent basis for liability."

As discussed below, the House language makes it easy to bring such claims under state laws, which could require a showing only of recklessness or negligence, rather than the actual knowledge required by federal law. If courts can find a company was "reckless" or "negligent" in transmitting CSAM or facilitating CSE because its use of strong encryption left it unable to detect and stop such messages, the net effect is nearly the same as permitting liability for encryption itself. Few, if any, companies will risk offering E2EE-encrypted services if such liability is possible. Not only will the privacy and security of all law-abiding users suffer, but it will also jeopardize the prosecutions of the very criminals the bill aims to thwart: courts will likely conclude that forcing providers to retain the ability to decrypt communications is tantamount to coercing them to conduct warrantless searches.

Recommendation #2: Expand the Leahy Amendment to Cover Monitoring

The Leahy Amendment should be restored. But this will not be enough to avoid triggering the Fourth Amendment. While it protected companies from liability for being unable to conduct searches, the amendment did not protect them from refusing to conduct such searches—the more direct Fourth Amendment problem. Specifically, a company could still face liability for choosing not to scan or monitor user communications for CSAM or CSE—or at all. Even a company that uses E2EE could be coerced into compromising the security of its devices by scanning user communications "client-side" (*i.e.*, on the device) prior to encrypting sent communications or after decrypting received communications.[6] This puts user privacy at risk: client-side scanning could be used to create an architecture of surveillance by which the devices of *all* users could spy on them, reporting to centralized servers when the device sends or receives certain kinds of communications.

[6] "Theoretically, a system that uses client-side scanning could still send messages encrypted end to end, and so the Leahy amendment would not offer any protection…" Hannah Quay-de la Vallee & Mana Azarmi, *The New EARN IT Act Still Threatens Encryption and Child Exploitation Prosecutions*, CDT (Aug. 25, 2020), https://cdt.org/insights/the-new-earn-it-act-still-threatens-encryption-and-child-exploitation-prosecutions/.

Apple has recently proposed such a technology for client-side scanning, touting safeguards that limit use of the system to known CSAM to prevent the capability from being abused by foreign governments or rogue actors. Setting aside the complicated question of whether or not Apple's safeguards are adequate, it is essential that Apple's decision to experiment with client-side monitoring is truly voluntary. Otherwise, Apple would be deemed a state actor subject to the Fourth Amendment's warrant requirement. Because Apple is ineligible to seek to see a warrant, and thus any searches it conducts would necessarily be warrantless, courts would likely have to throw out evidence collected through client-side monitoring and, without that evidence, toss out indictments of any Apple users charged under the CSAM and CSE statutes. Some applauded Apple's move and want to see more companies do the same, despite the privacy risks for law-abiding users. But even they must understand that if EARN IT coerces adoption of such technologies, this could lead a court to declare this coercion makes these private companies, *pro tanto*, state actors.

Congress has been in precisely this situation before. In 2008, Congress overhauled the statutory scheme for CSAM reporting. For the first time, Congress created an explicit duty for providers to report CSAM and CSE to the National Center for Missing and Exploited Children, which, in turn, would refer that evidence to law enforcement for criminal prosecution. 18 U.S.C. § 2258A. But to protect prosecutions based on such reports, Congress needed to ensure that any searches for such material conducted by providers was voluntary and therefore did not require warrants. Thus, Congress included Subsection 2258A(f), which provides:

> (f) Protection of Privacy.—Nothing in this section shall be construed to require a provider to—
>
> (1) monitor any user, subscriber, or customer of that provider;
>
> (2) monitor the content of any communication of any person described in paragraph (1); or
>
> (3) affirmatively search, screen, or scan for facts or circumstances described in sections (a) and (b).

This provision has been crucial to courts in finding that tech services are not state actors subject to the Fourth Amendment. "The only [statutory provision] that bears on scanning makes clear that an electronic communication service provider is not required to monitor any user or communication, and need not affirmatively seek facts or circumstances demonstrating a violation that would trigger the reporting obligation of § 2258A(a). 18 U.S.C. § 2258A(f)." *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013).

Congress should combine the Leahy amendment with 2258A(f) in the following new Section 230(e)(7):

> (7) CYBERSECURITY ***AND PRIVACY*** PROTECTIONS DO NOT GIVE RISE TO LIABILITY.—Notwithstanding paragraph (6), a provider of an interactive computer service shall not be deemed to be in violation of section 2252 or 2252A of title 18, United States Code, for the purposes of subparagraph (A) of such paragraph (6), and

shall not otherwise be subject to any charge in a criminal prosecution under State law under subparagraph (B) of such paragraph (6), or any claim in a civil action under State law under subparagraph (C) of such paragraph (6), because the provider—

"(A) utilizes full end-to-end encrypted messaging services, device encryption, or other encryption services;

"(B) does not possess the information necessary to decrypt a communication; or

"(C) fails to:

> ***(1)*** take an action that would otherwise undermine the ability of the provider to offer full end-to-end encrypted messaging services, device encryption, or other encryption services***;***
>
> ***(2) monitor any user, subscriber, or customer of that provider;***
>
> ***(3) monitor the content of any communication of any person described in Section 2258A(a)(1)(A);***
>
> ***(4) affirmatively search, screen, or scan for facts or circumstances described in Section 2258A(a) and (b); or***
>
> ***(5) facilitate monitoring, or other access to communications, by a government entity.***

Subparagraphs (7)(C)(1)-(4) adapt 2258A(f). Simply replicating 2258A(f) as a stand-alone provision of Section 230(e) will not work. Congress wanted to avoid Section 2258A being interpreted as requiring monitoring, and thus declared that 2258A did not do so. Here, the concern is one step removed: not that state laws might explicitly "require a provider to monitor" user communications, but that, fearing liability under those laws for *not* monitoring, providers would feel compelled to do so. The Leahy Amendment's "fails to" language captures this dynamic appropriately; this merely needs to be supplemented with the three elements of 2258A(f). By contrast, simply declaring that "nothing in Section 230(e)(6) shall be construed to require a provider to [monitor users]" would allow plaintiffs and prosecutors to argue that, because the state laws under which they bring suit do not *explicitly* "require" searches, their enforcement is not preempted. In making such arguments, such plaintiffs and prosecutors would rely on fundamental canons of construction that, by using two different framings, Congress must have intended the Leahy Amendment to work differently from the 2258A(f) language. Our proposed amendment avoids these problems.

Subparagraphs (7)(C)(5) is our attempt to deal with one additional obvious shortcoming of the Leahy amendment: it does not clearly protect websites from liability for refusing to facilitate government monitoring.[7] For example, two British cybersecurity experts have proposed including the

[7] See Riana Pfefferkorn, *The EARN IT Act Threatens our Online Freedoms. New Amendments Don't Fix It.*, Center for Internet and Society at Stanford Law School, Jul. 6, 2020,

government as a "ghost user" in every encrypted conversation, claiming this would not result in "weakening encryption or defeating the end-to-end nature of the service."[8] Likewise, in 2016, the Federal Bureau of Investigation sought a court order compelling Apple to facilitate access to communications stored on the iPhone of the alleged San Bernardino shooter by creating a custom version of iOS that Apple would push to the phone as if it were a regular software update.[9] These are just two examples and there is no way to predict what more government entities might demand in the future—or what measures companies might feel pressured to implement as a way of limiting their liability. This is why it is more important to limit the scope of that liability, as proposed below, than to try to make the Leahy amendment cover every conceivable circumstance. Nonetheless, it is worth trying to improve the Leahy amendment. We are not confident that our proposed language would be adequate; such questions of legislative drafting are precisely why the Committee needs to hold hearings on this bill. And we recognize that our amendment may raise difficult questions about the intersection of such language with the technical assistance provisions of other potentially applicable statutes.[10] But these are precisely the questions your Committee should be considering, and if the only opportunity to discuss them is at a markup, our proposed amendment will at least force *some* of that conversation.

Recommendation #3: Better Harmonize State Criminal Claims & Federal Law

Besides the Leahy amendment, the most significant amendment offered at the 2020 markup was that proposed by Sen. Mike Lee.[11] He proposed to harmonize the state laws under which claims could be brought, both civil and criminal, with federal law. He withdrew these amendments on the understanding that the bill's sponsors would work with him to address his concerns on the Senate floor before any final vote. No such changes were made when the bill was reintroduced January 31. Lee proposed to amend the new Subsection 230(e)(6)(B) as follows:

> (B) any charge in a criminal prosecution brought against a provider of an interactive computer service under State law ~~regarding the advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material, as defined in section 2256(8)~~ ***if the conduct underlying the charge would constitute a violation of section 2252 or 2252A*** of title 18, United States Code.

---

https://cyberlaw.stanford.edu/blog/2020/07/earn-it-act-threatens-our-online-freedoms-new-amendments-don%E2%80%99t-fix-it.

[8] See Ian Levy & Crispin Robinson, *Principles for a More Informed Exceptional Access Debate*, Lawfare, Nov. 29, 2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate; but see Jon Callas, *The Ghost User Ploy to Break Encryption Won't Work*, ACLU, Jul. 23, 2019. https://www.aclu.org/blog/privacy-technology/ghost-user-ploy-break-encryption-wont-work?redirect=blog/ghost-user-ploy-break-encryption-wont-work.

[9] Timothy B. Lee, *Apple's battle with the FBI over iPhone security, explained*, Vox, Feb. 17, 2016, https://www.vox.com/2016/2/17/11037748/fbi-apple-san-bernardino.

[10] *See, e.g.*,The Pen Register Act 18 U.S.C. § 3121 et seq., The Wiretap Act: 18 U.S.C. § 2511 et seq.

[11] EARN IT Act of 2020, S. 3398, 116th Cong. Lee Amend. (2020), https://www.judiciary.senate.gov/imo/media/doc/Lee%20Amendment%20to%20S.%203398%20-OLL20673.pdf.

This amendment would solve two problems. First, states would otherwise be free to define each of the five grounds for liability differently. Of these terms, Section 2252 currently includes only "distribution," and while Section 2252 contains three more of these terms, it does not include "presentation"—a term found nowhere in existing CSAM or CSE law.

State courts, confronting such ambiguities, may well dramatically broaden the scope of proposed Section 230(e)(6)(B) far past existing law. Their inclination to do so is vividly illustrated by a recent decision of the Supreme Court of Texas,[12] which held that state law analogues to federal sex-trafficking claims are not immunized by Section 230, despite the statute's clear carveout of only claims under specific federal statutes. As written, the proposed Section 230(e)(6)(B) magnifies this risk exponentially, exposing companies to unbounded and unpredictable liability based on the whims of local prosecutors and courts.

Second, absent the Lee amendment, states would be free to apply whatever *mens rea* requirement they wanted for such laws: instead of requiring actual knowledge, states could require only negligence or recklessness. Existing state laws already impose lower standards.[13]

The Lee amendment would not, however, fully harmonize state and federal laws: not only could penalties and prosecutorial processes, so could relevant generally applicable doctrines such as "willful blindness."[14] Creating alternative bodies of state law is antithetical to the fundamental goal of Section 230: maintaining a uniform body of federal criminal law for the entire Internet. If that criminal law is inadequate, it should be changed, as it was when Congress enacted FOSTA in 2017,[15] but still remain uniform. If the federal prosecutorial resources have proven inadequate, there are easier ways to enlist state, local and tribal prosecutors in the fight against CSAM and CSE than by amending Section 230 to allow the enforcement of a patchwork of state laws. 28 U.S.C. § 543 already allows the deputization of state, local or tribal prosecutors as "special attorneys" empowered to prosecute federal law. Strangely, DOJ has not, to date, taken advantage of this authority.

If there is some compelling reason why Section 230 must be amended to enable prosecutions by non-federal prosecutors, the cleanest way to accomplish that would be to empower state prosecutors to directly enforce federal law. That could be accomplished in two steps, first by adding the following as Section 2252(b)(3) and 2252A(b)(4) to authorize such prosecutions, as follows:

---

[12] In Re Facebook, Inc., 625 S.W.3d 80 (Tex. 2021).

[13] *See, e.g.* ARK. CODE § 5-27-604 (2010); MD. CODE § 11-208 (2020); FLA. STAT. § 847.0137 (2021); GA. CODE § 16-12-100.1 (2010). *See also EARN IT's State-law Exemption Would Create Bewildering Set of Conflicting Standards for Online Speech*, CDT (Aug. 11, 2020), https://cdt.org/insights/earn-its-state-law-exemption-would-create-bewildering-set-of-conflicting-standards-for-online-speech/.

[14] In general, in federal criminal law, defendants "cannot escape the reach of these statutes by deliberately shielding themselves from clear evidence of critical facts that are strongly suggested by the circumstances." Global-Tech Appliances, Inc. v. SEB S.A., 131 S. Ct. 2060, 2068-69 (2011). As the Court noted, "persons who know enough to blind themselves to direct proof of critical facts in effect have actual knowledge of those facts." *Id*. at 2069.

[15] H.R.1865, 115th Cong. (2018).

> The Attorney General of a State shall have the same power to prosecute violations of subsection (a) as the Attorney General of the United States.

And second by the new 230(e)(6)(B) as follows:

> (B) any charge in a criminal prosecution brought against a provider of an interactive computer service under ~~State law regarding the advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material, as defined in section 2256(8)~~ ***Sections 2252(b)(3) and 2252A(b)(4)*** of title 18, United States Code; or

While it is common for federal law to authorize state officers to enforce civil remedies, we could find no current example of a federal law authorizing prosecutions of federal law. This reflects a longstanding, general trend towards the dominance of federal law enforcement. It may also reflect the fact that the Attorney General already has the power to appoint state officers as special prosecutors capable of enforcing federal law.[16] Since *Printz v. United States*, 521 U.S. 898 (1997), Congress has been careful to avoid anything that might look like commandeering state officers. In that case, federal law violated the Tenth Amendment by *requiring* state and local officials to perform background checks on people buying guns. Our proposal involves no such requirement: it would merely give state officers the option of prosecuting federal crimes—exactly like 28 U.S.C. § 543, except authorizing all state attorneys general across the board instead of one by one.

Our proposal is consistent with the practice of the early republic, in which Congress relied on state officers to enforce federal criminal laws.[17] Some scholars have suggested that such practice might have, somehow unbeknownst to the earliest Congresses, violated the Appointments Clause's requirement that the President appoint, and the Senate confirm, "Officers of the United States."[18] They have invoked Justice Scalia's solitary dissent in *Morrison v. Olson,* which argued that the Ethics in Government Act of 1978 violated the Appointments Clause by authorizing the appointment of an independent counsel outside the control of the President.[19] But the most thorough academic study of the question concluded that:

> significant law enforcement responsibilities have at times been discharged by state officials immune from close executive branch supervision. State officials have wielded influence in determining when to arrest individuals suspected of violating federal

---

[16] Harold J. Krent, *Executive Control Over Criminal Law Enforcement: Some Lessons From History*, 38 Am. U. L. Rev. 275, 303-12 (1989), https://scholarship.kentlaw.iit.edu/fac_schol/323.

[17] "The first Congresses feared that exclusive reliance upon federal law enforcement machinery would not suffice to enforce the penal laws of the nation. In addition to affording individuals significant enforcement responsibility, Congress vested jurisdiction in state courts over actions seeking penalties and forfeitures, granted concurrent
jurisdiction to state courts over some criminal actions, and assigned state officials auxiliary law enforcement tasks." *Id.* at 303.

[18] *See* Margaret H. Lemos, *State enforcement of Federal Law*, 86 N.Y. L. Rev. 698, 712 n 64 (2011); *see generally* Evan Caminker, *The Unitary Executive and State Administration of Federal Law*, 45 U. KAN. L. Rev. 1075 (1997) (analyzing state administration of federal law under unitary executive theory).

[19] Morrison v. Olson, 108 S. Ct. 2597, 2625-31 (1988) (Scalia, J., dissenting).

> laws, when to recommend mitigation of a punishment otherwise due under federal law, and even when to prosecute. The historical examples suggest that some responsibility to enforce the Ethics in Government Act, whether through direct criminal actions or suits in equity, could be vested in the state judicial system, outside the direct control of the Executive.[20]

Congress could, of course, avoid these questions *and* also ensure uniformity of the law governing CSAM and CSE online simply by encouraging the Attorney General to make use of his existing power to appoint special prosecutors. We know of no reason why the Attorney General could not appoint all state and territorial attorneys general to that role.

Recommendation #4: Remove Civil Liability Provisions

As originally introduced, the EARN IT Act would have lowered the scienter requirement for civil suits brought under Section 2255 (and based on Sections 2252 or 2252A) from "actual knowledge" to "recklessness."[21] As reintroduced, EARN IT drops this language—yet accomplishes precisely the same thing indirectly. The new Section 230(e)(6)(A) would authorize federal civil suits under Section 2255 without changing the actual knowledge standard contained in both 2252 and 2252A. Yet, just as with state criminal prosecutions, the new Section 230(e)(6)(C) would authorize a staggering array of state-level civil actions far beyond those contemplated by Sections 2252 and 2252A; states would be free to invent their own scienter requirements.

The best, cleanest solution would be to delete both Section 230(e)(6)(A) and (C). In conjunction with Senator Lee's amendment to Section 230(e)(6)(B), this would focus the bill and permit state authorities to provide much-needed assistance in the enforcement of a uniform body of federal criminal law. Federal and state prosecutors would be free to explore prosecutions of truly bad actors—such as Backpage.com—under theories such as willful blindness, which is applicable to criminal, but not civil law.[22]

Recommendation #5: Harmonize State Civil Claims with Federal Law

Less effective in mitigating these concerns — but nonetheless a considerable improvement over EARN IT as introduced — would be Sen. Lee's amendment to Section 230(e)(6)(C). This amendment limited state civil actions to circumstances where "the conduct underlying the claim constitutes a violation of section 2252 or section 2252A." Adopting this amendment would at least limit the scope of potential liability to violations of federal law, including the actual knowledge requirement, thus

---

[20] Harold J. Krent, *A Symposium On Morrison v. Olson: Addressing The Constitutionality Of The Independent Counsel Statute: Executive Control Over Criminal Law Enforcement: Some Lessons From History*, 38 Am. U.L. Rev. 275, 309 (1989).

[21] EARN IT Act of 2020, S. 3398, 116th Cong. § 6(b)(3).

[22] *See* EARN IT Act of 2020, S. 3398, 116th Cong. Lee Amend. (2020), https://www.judiciary.senate.gov/imo/media/doc/Lee%20Amendment%20to%20S.%203398%20-OLL20673.pdf.

eliminating the risk of a patchwork of 56 state and territorial laws and liability standards (and state attorneys general motivated by political considerations) that would be nearly impossible to navigate.

Even then, imposing *any* scienter-based civil liability on Internet companies under these circumstances, including the liability carved out for claims under Section 2255 by proposed Section 230(e)(6)(A), is unworkable for multiple reasons. Indeed, it will likely do the *opposite* of what the bill's sponsors said: *discourage* moderation and *encourage* the use of strong encryption.

First, tying civil liability to knowledge recreates the very "Moderator's Dilemma" that led Congress to enact Section 230 in the first place: it creates a perverse incentive for websites to avoid gaining knowledge that could lead to liability, such as through monitoring or moderating communications. Again, ironically, websites would be *more* likely to adopt strong encryption for private communications among users and *less* likely to implement client-side scanning—if they cannot read the contents of users' communications, they can largely avoid "knowledge" of unlawful activity.

Largely avoid, but not *entirely* avoid. Knowledge standards are unworkable for civil liability in this context because even unsubstantiated complaints about unlawful material may, in some circumstances, suffice to establish "knowledge." Consider copyright law. The Digital Millennium Copyright Act (DCMA) requires a service provider to remove, or disable access to, material upon obtaining "actual knowledge that the material or an activity using the material on the system or network is infringing."[23] It is not sufficient to show that a service provider has "general knowledge that one's services could be used to share infringing material."[24] Instead, a service provider must have "knowledge or awareness of specific infringing activity."[25] As that appeals court explained, "the nature of the removal obligation itself contemplates knowledge or awareness of specific infringing material, because expeditious removal is possible only if the service provider knows with particularity which items to remove."[26] The DMCA determines what constitutes "knowledge" by prescribing what notifications of infringement must entail and to whom they must be delivered; only by complying with such "notice" requirements can a rightsholder trigger the "takedown" obligations of the statute—and if a service provider complies with its takedown obligations upon receipt of statutorily compliant notices, it is immune from liability.[27]

Here, service providers would face a perverse incentive to make it more difficult for users to flag objectionable content. But they could not avoid such complaints entirely. If someone complains that a particular account is using the service to transmit CSAM or to engage in CSE (*e.g.*, grooming or solicitation), does this allegation give the provider "knowledge or awareness of specific infringing activity?" What kind of allegation would suffice? An email to any employee? Which employees? A Twitter direct message—or a Twitter @mention? What information must be provided to put a company on notice: the user's legal name, user ID, or something else? Unlike the DMCA, EARN IT provides no basis for assessing whether a complaint has provided it with sufficient knowledge that

[23] 17 U.S.C. § 512(c)(1)(A)(i), (iii).
[24] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1022 (9th Cir. 2013).
[25] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 26 (2d Cir. 2012).
[26] *Id*. at 30.
[27] 17 U.S.C. § 512(c)-(d).

it must take down that content or disable an account. For the first time, the courts would have to wrestle with such questions in the uniquely complicated context of the Internet. It is not clear to what extent decisions involving the DMCA's actual knowledge standard would apply.

But the experience of the DMCA does strongly suggest what will the practical result will be: "Twenty years of experience with these laws in the United States and elsewhere tells us," Stanford's Daphne Keller notes, "that when platforms face legal risk for user speech, they routinely err on the side of caution and take it down."[28] This would be even more likely under EARN IT, which opens the door to stiff *criminal* penalties, than it is under copyright law, where criminal prosecutions are relatively uncommon.[29]

If the courts make it too easy to put a company 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.[30] Such requests could easily be weaponized by a small group of ideologues to force the takedown of content or users they dislike. Such requests could be weaponized for political purposes and EARN IT provides no mechanism for deterring false reports, unlike the DMCA.[31]

Providers of services utilizing E2EE would face a quandary: if someone alleges that a particular user is distributing CSAM or engaging in CSE over an encrypted service, but the ICS provider cannot view the contents of that user's communications, it will have no way to assess the merits of specific complaints, and thus no sure way of identifying serial abusers of the complaint process.

Such perverse results have not resulted from enforcement of existing federal *criminal* laws (Sections 2252 & 2252A) because the evidentiary burden in criminal cases is high: proof beyond a reasonable doubt. But combining the actual knowledge standard of those statutes with the much lower burden of proof for civil liability ("preponderance of the evidence") found in Section 2255 could produce radically different, and more perverse results—which Section 230 has, thus far, prevented.

One way to avoid such concerns, at least in part, is by amending the bill to require not only that state civil claims be based on violation of Sections 2252 or 2252A (as in the Lee amendment), but also that *any* civil claim, whether federal (230(e)(6)(A)) or state (230(e)(6)(C)) be proven not by a preponderance of the evidence, but rather by "clear and convincing evidence." We proposed modifying the Lee amendment as follows:

---

[28] Daphne Keller, *Internet platforms: Observations on Speech, Danger, and Money*, *in* Hoover Institution's Working Group on National Security, Technology, and Law at 2 (2018), https://cyberlaw.stanford.edu/files/publication/files/381732092-internet-platforms-observations-on-speech-danger-and-money.pdf.

[29] *See Are FBI Anti-Piracy Warnings More Bark Than Bite?*, JOLT (Mar. 19, 2018), https://jolt.richmond.edu/2018/03/19/are-fbi-anti-piracy-warnings-more-bark-than-bite/.

[30] *See* Keller, *supra* note 28, at 18.

[31] The DMCA's sanctions mechanism has been widely criticized as inadequate, *see* Michael P. Murtagh, *The FCC, the DMCA, and Why Takedown Notices Are Not Enough*, 61 Hastings L.J. 234 (2009), illustrating just how thorny the problem of dealing with abuse of takedown notifications is.

(A) any claim in a civil action brought against a provider of an interactive computer service under section 2255 of title 18, United States Code, if the conduct underlying the claim constitutes a violation of section 2252 or section 2252A of that title ***and such conduct is proven by clear and convincing evidence***;

[...]

(C) any claim in a civil action brought against a provider of an interactive computer service under State law ~~regarding the advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material, as defined in section 2256(8) of title 18, United States Code.~~ ***if the conduct underlying the claim would constitute a violation of section 2252 or 2252A of title 18, United States Code, and such conduct is required by State law to be proven by clear and convincing evidence.***

The "clear and convincing evidence" standard is not the norm in civil litigation, but it *is* generally imposed in cases involving allegations of quasi-criminal conduct implicating moral turpitude, where, in addition to mere monetary damages, reputational stakes are high. Civil fraud, which also contains a scienter requirement, is a classic example.[32] That is precisely the case here: a successful civil suit would hinge on proof that a provider had committed criminal behavior of the most shocking nature. Moreover, these claims will not be against those directly engaged in CSAM or CSE, but the providers used by those criminals—presumably in violation of a company's terms of service. It is sound policy to ensure that such claims are proven by a standard that accounts for the nature of the claims and the relative position of the defendants contemplated by these provisions.

Of course, merely imposing a heightened burden of proof would not resolve the fundamental underlying issue that it is entirely unclear whether a company might be held liable under an actual knowledge standard if it uses strong encryption and lacks the ability to assess the merits of purported notice of offending content. As such, it is vital that Congress restore the Leahy amendment and adopt a version of the Section 2258A(f) language as discussed above.

—

Thank you for your attention. We would be happy to assist your Committee in working to revise the EARN IT Act to ensure that it facilitates, rather than frustrating, the enforcement of CSAM and CSE laws, and that it does not harm the privacy, security and safety of law-abiding users.

Sincerely,

Berin Szóka
President, TechFreedom
bszoka@techfreedom.org

Ari Cohn
Free Speech Counsel, TechFreedom
acohn@techfreedom.org

[32] *See* Addington v. Texas, 441 U.S. 418, 424 (1979) ("One typical use of the [clear and convincing evidence] standard is in civil cases involving allegations of fraud or some other quasi-criminal wrongdoing by the defendant. The interests at stake in those cases are deemed to be more substantial than mere loss of money, and some jurisdictions accordingly reduce the risk to the defendant of having his reputation tarnished erroneously by increasing the plaintiff's burden of proof.").