July 2, 2020

The Honorable Lindsey Graham
Chairman, Senate Judiciary Committee
United States Senate
Russell Senate Office Building 290
Washington, D.C. 20510

The Honorable Diane Feinstein
Ranking Member, Senate Judiciary Committee
United States Senate
Hart Senate Office Building 331
Washington D.C. 20510

cc: members of the Senate Judiciary Committee

RE: Senate Judiciary Committee Markup of the EARN IT Act of 2020 (S.3398)

Dear Chairman Graham and Ranking Member Feinstein:

We appreciate your Manager's Amendment to the EARN IT Act. We have never opposed convening an expert commission to study the scourge of Child Sexual Exploitation (CSE) and Child Sexual Abuse Material (CSAM). We have opposed granting such a commission the power to make what amount to legal requirements. Doing so would (a) risk converting tech companies into government agents subject to the Fourth Amendment's warrant requirement, which would actually frustrate the fight against CSE/CSAM; (b) infringe on the First Amendment rights of both users and service providers; and (c) raise other grave constitutional problems.[1]

Our primary concern has never been the "best practices" contemplated by the bill, but the vague liability the bill would create for how Internet services are designed and operated. The effect of that liability would be to coerce Internet services to fundamentally change how they operate — *e.g.*, compromising the security of their service (to provide a backdoor for law enforcement to access the content of communications in unencrypted form), age-verifying all users, and segmenting users by age to prevent adults from communicating with minors. If anything, the practical effects of the Manager's Amendment on lawful speech protected by the First Amendment are murkier than those of the bill itself.

These effects cannot be understood without further hearings. Completely rewriting this bill at a markup and simply sending it to the Senate floor would mean failing to vet legislation,

[1] *See, e.g.,* Berin Szóka, *The Unconstitutional, Unworkable EARN IT Act*, (June 2020), https://bit.ly/2YQ8hfz.

both for its real-world effects and its constitutionality. It would harm, rather than help, children while also burdening the lawful speech of adults.

How The Manager's Amendment Could Backfire. Any law tied to a scienter standard[2] risks backfiring by discouraging interactive computer service (ICS) providers from gaining knowledge of potentially unlawful content. All three proposed amendments to Section 230 risk re-creating the very "Moderator's Dilemma" that led Congress to enact Section 230 in the first place.[3] The proposed Subsections 230(e)(6)(B) and (C) set the bar for liability too low — at "recklessness" or even lower (as explained below). Like the bill itself, such liability would effectively ban end-to-end encryption and force a host of other changes, even without "best practices." But standing on its own, the "actual knowledge" standard of Subsection 230(e)(6)(A) could make ICS providers *more* likely to adopt strong encryption for private communications among users, because it means ICS providers will not be able to read the contents of users' communications. If adopted, the Manager's Amendment risks suffering the same fate as the Communications Decency Act (CDA), and the Children's Online Protection Act (COPA), both largely struck down by the courts on constitutional grounds.[4]

A Better Approach. Instead of creating multiple forms of scienter-based liability, the way to avoid such perverse results, and also to minimize effects on lawful speech, is to stop focusing on either "actual knowledge" or "recklessness" as triggers for civil liability (as existing *criminal* law necessarily must). Instead, lawmakers should focus on process-based standards for how to deal with notice of potentially unlawful conduct, as proposed below.

Subsections 230(e)(6)(B) and (C) are inherently unworkable and unnecessary, and should thus be dropped entirely. Because it remains focused on scienter, even the proposed Subsection 230(e)(6)(A) (authorizing suits under 2255's existing "actual knowledge" standard) raises difficult First Amendment questions — and could backfire badly.

Civil Suits under State Law. The bill allows CSE/CSAM victims to bring civil suits under 18 U.S.C. § 2255 under a "recklessness" standard rather than "actual knowledge." The Manager's Amendment drops this provision, but reintroduces it in another form: the proposed Subsection 230(e)(6)(C) would allow civil suits under state law without specifying a scienter standard — which creates even greater First Amendment problems (as discussed below), because the state law could apply not only a recklessness standard but even lower thresholds for liability, such as negligence or even strict liability (which do not require scienter).

---

[2] "Scienter" includes actual knowledge of particular content and recklessness, among other standards.

[3] "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).

[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) (striking down COPA).

Specifying an "actual knowledge" standard would not solve the problems discussed below. In any event, there is no need for state civil liability to diverge from federal law. There should not be a patchwork of state laws with different approaches to encryption, age verification or other aspects of how Internet services work.

State Criminal Prosecution. The proposed Section 230(e)(6)(B) creates a second, entirely new problem not found in the original bill: allowing state criminal prosecution for "the advertisement, promotion, presentation, distribution, or solicitation of [CSE/CSAM]" without specifying that such state laws must match existing federal law. In particular, this means that state laws could be based on a lower scienter requirement, such as recklessness. Since 1996, Section 230 has ensured that a single body of consistent federal criminal law governs all Internet services, regardless of who applies it — and this consistency would remain. Specifying an "actual knowledge" requirement will not entirely ensure consistency as there could be other differences between federal and state law. Regardless, there is no need for this provision: the Attorney General already has the power to deputize state, local and tribal prosecutors to enforce Sections 2252 and 2252A,[5] but, for reasons that remain unclear, has simply chosen not to exercise this power.

Effects on Lawful Speech. Section 230 has never protected ICS providers from federal criminal prosecution, but it does currently shield them from civil liability under Section 2255. Thus, the law has prevented a host of First Amendment chilling effects in ways that must be carefully considered before any change to Section 230 is made (let alone introduced at markup as a newly conceived amendment that has not been scrutinized in hearings). Scienter-based standards are inherently more problematic for civil liability than for criminal prosecution because the two involve radically different evidentiary standards: "preponderance of the evidence" versus "beyond a reasonable doubt."

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, what might constitute "actual knowledge" (under the preponderance of the evidence test of civil litigation) is less clear than it might seem.

With visual depictions, the challenge can, to some extent be managed at scale: while there are always hard edge cases, tech companies have developed an extensive catalog of hashes of known CSAM. This allows tech companies to automatically filter their content for such hashes, and report them to NCMEC — thus avoiding liability for content for which they might otherwise be said to have "actual knowledge." But all three proposed amendments to Section

[5] 28 U.S.C. § 543(a) ("The Attorney General may appoint attorneys to assist United States attorneys when the public interest so requires").

230 authorize legal actions (civil suits or prosecutions) not merely for those who traffic in visual imagery, but also those who "solicit" it from minors or who "promote" it.[6] In practice, this means that all communications (text messages and voice or video chats) between adults and minors about any subject would create litigation risks under the Manager's Amendment. While keyword filtering can, to some extent, identify interactions that might be used for "solicitation" or "promotion" of CSAM between adults and minors, there is no easy technological solution that will allow ICS providers to distinguish unlawful "grooming" and "enticement" from ordinary communications — both because such conversations are generally coded and because 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.

The Manager's Amendment's effects on lawful speech can be grouped into three categories:

Effect #1: Age Verification Mandates. The practical effect of holding ICS providers liable for communications between adults and minors would be essentially similar to those of the Communications Decency Act (CDA) of 1996 and the Child Online Protection Act (COPA) of 1998. Both laws failed in court for overly burdening the free speech rights of adults.[7] While the CDA created broad, vague liability for allowing minors to access "obscene or indecent" content, COPA explicitly required age verification of adults attempting to access content that might be deemed "harmful to minors." COPA was struck down for unconstitutionally infringing on adults' right to anonymous speech, since many would be unwilling to identify themselves (such as by providing a credit card) before accessing sensitive content. COPA also violated the First Amendment rights of ICS providers to reach such adults.

The Manager's Amendment, like the bill itself, raises similar constitutional problems: the broad liability it creates could force ICS providers to age-verify all users to determine which ones might be minors. But where COPA's age verification mandate was limited to a narrow class of content (primarily legal pornography), the Manager's Amendment could affect the rights of all adults to anonymously use any service, especially an encrypted service, that allows users to communicate with each other (because some *might* be minors), regardless of the nature of the content. It could also force age-segmentation in ways that COPA did not, which could complicate families' use of Internet services and remote learning.

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

---

[6] 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.

[7] *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) (striking down COPA).

(*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, but at least it would not affect ordinary lawful communications.

Effect #2: Heckler's Veto. Any scienter-based system for civil liability creates a second First Amendment problem: 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.[8]

Effect #3: Encryption & Takedowns. 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 — a further heckler's veto.

A Notice-Based Approach. Scienter-based civil liability inevitably creates a Moderator's Dilemma. The better way to distinguish between responsible operators and truly bad actors — and to encourage cooperation with law enforcement — would be a mechanism by which law enforcement (and potentially NCMEC) could, with proper safeguards, put ICS providers on notice about potential CSE/CSAM. A properly crafted notice system would avoid the problems inherent in scienter-based liability — *e.g.*, an email or a tweet directed to an ICS employee complaining about certain content might create "actual knowledge" of the nature of the content. Creating a clear channel for notification would ensure that ICS providers take appropriate action when they are properly notified of unlawful content on their service — *without* the need for vague, open-ended liability. When limited to responsible parties, and combined with opportunities for appeal by those wrongly accused (and sanctions for meritless complaints), formal notice mechanisms can greatly reduce the "heckler's veto" problem created by scienter-based liability regimes.

For example, when the Supreme Court struck down a state law banning all Internet use by convicted sex offenders as overly broad, it noted: "the First Amendment permits a State to enact specific, narrowly tailored laws that prohibit a sex offender from engaging in conduct that often presages a sexual crime, like contacting a minor or using a website to gather

---

[8] 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.

information about a minor."[9] Such a law could be enforced not only by penalties on sex offenders, but also by providing operators of encrypted messaging services with the names, IP addresses, and other potentially identifying information of convicted sex offenders. This would help ICS providers block sex offenders from using their services *without* forcing all users to identify themselves (as COPA did). Such a law would have a built-in judicial safeguard against abuse: valid criminal convictions of those involved.

Applying such a model in other circumstances may require other safeguards. Avoiding the failure of Section 512(f)'s flawed and ineffective regime for deterring baseless copyright notices, would require careful drafting — not a last-minute amendment.

Quasi-Regulatory Effects of "Best Practices." So long as ICS providers fear liability based on "recklessness" (or some lower scienter standard), any "best practices" issued under the bill will have *de facto* regulatory effect: 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 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, the Commission should be required to consider and address the effects any best practices it might issue could have upon civil litigation.

* * *

Section 230 has been called the law that made the Internet possible — and for good reason. The law has enabled a flourishing of services that enable free speech by users in unprecedented ways. But just as importantly, by avoiding the Moderator's Dilemma, the law has also ensured that the threat of legal liability does not discourage Internet services from acting responsibly. Any proposal to amend Section 230 must be considered with the greatest care. We urge you to postpone this markup and schedule a new hearing to consider the difficult legal and practical questions raised by the Manager's Amendment. We stand ready to assist your committee in this matter.

Sincerely,

TechFreedom

Americans for Prosperity

---

[9] *Packingham v. North Carolina*, 137 S. Ct. 1730, 1737 (2017).