July 1, 2020

The Honorable Lindsey Graham
Chairman, Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Dianne Feinstein
Ranking Member, Senate Committee on the Judiciary
331 Hart Senate Office Building
Washington, DC 20510

Re: S. 3398 – EARN IT Act – OPPOSE

Dear Chairman Graham, Ranking Member Feinstein, and Members of the Committee:

The Electronic Frontier Foundation (EFF) writes to oppose S. 3398, the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT Act), both in its original form as introduced and if it were to be amended with the proposed Manager's Amendment.

EFF is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 members. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law to technology.

The EARN IT Act aims to protect children from online sexual exploitation—an important and laudable goal – but it does so by threatening free speech online, as well as the privacy and security of digital communications.

In its original form, the EARN IT Act violates the First and Fourth Amendments**.** The bill's broad categories of "best practices" for online service providers amount to an impermissible regulation of editorial activity protected by the First Amendment.[1] [2]The EARN IT Act, as introduced, also violates the Fourth Amendment by turning online platforms into government actors that search users' accounts without a warrant based on probable cause.[3] The introduced bill threatens end-to-end encrypted communications by

[1] Miami Hearld Pub. Co. v. Tornillo (1974), https://supreme.justia.com/cases/federal/us/418/241/#tab-opinion-1950903.
[2] La'tiejira v. Facebook, inc. (2017), https://scholar.google.com/scholar_case?case=16203454798300551523&q=La%E2%80%99Tiejira+v.+Facebook,+Inc.,+272+F.+Supp.+3d+981&hl=en&as_sdt=2006&as_vis=1.
[3] For a longer constitutional analysis of the introduced bill, see EFF's blog post: *The EARN IT Act Violates the Constitution* (March 31, 2020), https://www.eff.org/deeplinks/2020/03/earn-it-act-violates-constitution.

broadly empowering a commission to write "best practices" for platforms that could prohibit encryption.[4]

The proposed Manager's Amendment does not remedy these problems. It creates a new, wholesale exception to online service provider immunity for user-generated content, which would be codified in Section 230(e)(6) (47 U.S.C. § 230). Online platforms would no longer have a defense against federal civil claims related to CSAM, as well similar state civil claims and criminal prosecutions.

Just like the introduced bill, the Manager's Amendment threatens encrypted communications, even though the amendment does not use the word "encryption" in its text. The threat to encryption, however, no longer sits directly with one federal commission, but with the over 50 jurisdictions that are free to amend their CSAM laws to compel online service providers to break encryption, or be exposed to potentially crushing civil and criminal liability based on the actions of their users. These companies would no longer have the federal statute (Section 230) to shield them from such state law-based liability.

Additionally, while the commission would no longer have the force of law behind it, the "best practices" it proposes for online platforms and how they manage user-generated content may become the standard that states looks to. In particular, states may amend their CSAM laws to formally incorporate the commission's rules. Thus, the Manager's Amendment simply shifts enforcement of the "best practices" to state prosecutors and private lawyers filing civil lawsuits.

Moreover, as online platforms face increased legal exposure by their loss of Section 230 immunity for user-generated content, they may take drastic measures to mitigate their exposure, which would harm the free speech of users across the Internet. To mitigate their own legal liability, companies may cave to bogus claims that a particular users is posting CSAM without doing a proper investigation. We have seen time and again in the copyright space how such a notice-and-takedown system improperly removes legal content, and has been used to harass innocent users.[5] That is, false accusations and censorship abound. Additionally, platforms may severely curtail the services or features they offer. A small online forum, for example, may also provide a private messaging feature for its community. The operators may decide that the risk of liability for CSAM generated by users is too great, and they may cease to offer messaging at all as a result.

In short, the Manager's Amendment forces online service providers to make an impossible choice: cave to government pressure regarding their editorial decisions or face significant new criminal and civil liability.

---

[4] *The EARN IT Bill Is the Government's Plan to Scan Every Message Online* (March 12, 2020), https://www.eff.org/deeplinks/2020/03/earn-it-bill-governments-not-so-secret-plan-scan-every-message-online.

[5] For a list of bogus copyright takedowns, see EFF's takedowns page, https://www.eff.org/takedowns.

Finally, the amended bill creates a practical problem: by exposing online service providers to potential liability for user-generated content in over 50 jurisdictions, operators of these platforms would have to contend with following dozens of varying state mandates about how to run something as simple as a comments section.

As it is currently written, Section 230 allows the prosecution of platforms under federal criminal law. If Congress feels that the federal government is not adequately pursuing and mitigating CSAM cases, that is something that should be addressed directly. Deputizing states and private entities to do the federal government's work for them will not solve the intended problem. What will result, however, is a confusing legal landscape where services like iMessage, WhatsApp, and Signal could all be forced to either allow law enforcement access to all users' messages or over-censor users, or risk sweeping liability across many jurisdictions.

Sincerely,

India McKinney
Director of Federal Affairs
india@eff.org