Insight

Unintended Consequences of the EARN IT Act

JEFFREY WESTLING | FEBRUARY 23, 2022

Executive Summary

- The Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2022 would amend Section 230 to put a greater onus on platforms to find and remove child sexual abuse material (CSAM) online and allow states to define the standards for addressing CSAM that platforms must adhere to.
- Despite the important goals of the bill, as currently drafted the EARN IT Act would have major consequences for both user privacy and the ability of law enforcement to use the information obtained by platforms against the perpetuators of CSAM.
- Threats of liability may force platforms to scan users' communications and take away tools for encrypting communications, meaning Americans will have less protection against privacy intrusions from industry and government alike.
- Coercion of platform monitoring also threatens to deputize platforms in the identification and reporting of CSAM, meaning evidence obtained by the searches would become state action and thus inadmissible in trials against criminals.

Introduction

The Senate may soon consider the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2022. On its surface, the bill would make a relatively small modification to the Section 230 of the Communications Decency Act, which is designed to put a greater onus on "Big Tech" to crack down on the spread of child sexual abuse material (CSAM). While a laudable goal, the bill's changes threaten critical privacy protections, such as end-to-end encryption (E2EE), or mandate firms scan user communications. In isolation, this privacy tradeoff could be worth making, or at least worth debating. But the bill as

currently structured would deputize platforms as partners in law enforcement in the identification and reporting of CSAM. This could make evidence obtained by the platforms inadmissible in court, as platforms would now be state actors and their searches unconstitutional under the Fourth Amendment—and thus make prosecution of CSAM criminals much more difficult.

Now that the Judiciary Committee has moved the bill out of Committee, the Senate will have the opportunity to fix the major issues still prevalent in the bill. This insight explains why the legislation's reforms risk significant harm to both user privacy and law enforcement agencies as they attempt to prosecute CSAM criminals. Members should carefully consider these concerns as they consider the bill.

EARN IT Act – What It Does

The EARN IT Act does two main things. First, it creates a commission with a variety of different stakeholders to develop recommended best practices for platforms to prevent, reduce, and respond to the online sexual exploitation of children. The commission's recommendations do not bind platforms to act in accordance with the best practices, and ideally would remain voluntary to guide platforms with the best steps to address CSAM. Courts may also use these guidelines in determining whether platforms adhered to necessary standards of care under relevant state laws on the issue.

Second, the bill would create an exemption to Section 230's protections for intermediary liability for claims relating to the advertisement, promotion, presentation, distribution, or solicitation of CSAM. Section 230 currently has an exemption for violations of federal criminal law, meaning existing law which makes it a federal crime to knowingly possess and share CSAM already applies to platforms such as Facebook and Twitter. For all state and federal civil claims, however, Section 230 precludes courts from treating platforms as the publisher or speaker of what users post. In practice, this means that states cannot enforce CSAM-related statutes that attempt to hold platforms as the speaker when CSAM is shared. EARN IT would extend the exemption for federal criminal enforcement to any state civil or criminal claims. Further, because EARN IT allows states to enforce their own laws, in practice it also allows states to change the legal standards for liability. This means that even if a platform doesn't know about CSAM on their service, they can be liable for users possessing and sharing the content if the state finds that a platform should have known, or even acted negligently, in identifying and reporting these materials.

Certainly, both Congress and platforms should strive to find better strategies to target the spread of CSAM. But while the EARN IT Act clearly aims to this goal, as drafted, it would have significant unintended consequences for both user privacy and the ability of law

enforcement to prosecute criminals.

EARN IT Act Threatens User Privacy

Since the original bill's introduction, many critics have worried that it would target user privacy features such as end-to-end encryption, which criminals can use to obtain and share CSAM without the risk of law enforcement gaining access to these communications. In the original bill, for example, adhering to the commission's recommendations would "earn" platforms Section 230 immunity. Attorney General Bill Barr, a noted critic of end-to-end encryption, would have had significant control over the commission and its participants. This threat led to significant outcry from public interest and privacy groups. In response to massive opposition to this approach, the drafters drastically changed the bill to its current structure and Senator Leahy introduced an amendment to alleviate concerns that offering E2EE would lead to liability.

When EARN IT was reintroduced in 2022, lawmakers changed the language again. Now the encryption provision only states that offering E2EE cannot be used as evidence to support other claims, as long as it not be an "independent basis for liability." What does this mean in practice? If a claim against a platform alleges the service should have known about CSAM, plaintiffs and prosecutors could argue that offering E2EE could have contributed to the reckless behavior of the platform. The language would only protect platforms if they engaged in no other conduct that potentially supported the conclusion that the platform should have known about the CSAM.

This wouldn't be a major issue in isolation, as federal law requires actual knowledge of the content, so offering E2EE wouldn't necessarily give rise to liability. Nevertheless, the bill also allows for states to bring claims under state laws that could have different standards than the current federal regime, such as recklessness. While the actual legality of the practices will depend on the facts of the case, firms will likely feel pressure to eliminate these services, regardless of the privacy benefits they provide to users.

Worse, even a fully restored Leahy amendment that made clear offering E2EE could not be used as evidence against a platform wouldn't fully protect the privacy of users. E2EE only protects the communications in transit, and not the information on users' devices. Firms can employ client-side scanning to examine the contents of messages before the message is encrypted or decrypted. The Leahy amendment would only cover the encryption of messages in transit, and not on the device, itself. Again, this in isolation doesn't give rise to liability, but when states impose a lower standard than knowledge, ICS could be found liable for spreading CSAM if they do not use tools such as client-side scanning to ensure users do not share CSAM over the service.

With Congress' significant focus on online privacy, including that of the EARN IT Act's cosponsors, this threat to user privacy is somewhat surprising. Encryption protects users from a variety of potential harms. Victims of domestic abuse need secure and confidential communications to speak to loved ones and access support. Journalists use encryption to protect sources. And a lack of strong protections opens the door for hostile actors to target Americans. At the same time, pedophiles can also use encryption to evade law enforcement and continue to harm children.

If the EARN IT Act's changes simply meant a tradeoff between stopping CSAM and keeping privacy protections such as encryption, then Congress and the public could have that debate. Unfortunately, as drafted, the bill would both reduce privacy protections—and make it more difficult to prosecute CSAM criminals.

EARN IT Act Could Make Prosecution of Criminals More Difficult

Despite the best intentions of the bill's authors, by effectively deputizing platforms into searching for and reporting CSAM on behalf of law enforcement, the EARN IT Act could make information obtained by platforms inadmissible in court under the Fourth Amendment.

Currently, platforms employ a wide range of tools to find and eliminate CSAM. Under federal law, when the platforms learn of CSAM, they report to the National Center for Missing and Exploited Children (NCMEC) the details so that law enforcement can find and arrest the individuals involved. These voluntary actions then lead to prosecution of the individual. Yet this regime only works as long as the platforms provide information to law enforcement voluntarily.

The Fourth Amendment protects individuals against unreasonable searches and seizures, which means that law enforcement must normally obtain a warrant to search users' communications. Because platforms aren't state actors, their searches do not need the same protections, and prosecutors can use any information obtained from the platform to convict the perpetrators. If a state employs a recklessness or even negligence standard for platforms to find and remove CSAM, however, and platforms are essentially coerced into monitoring communications for CSAM, courts may determine that the influence from government actors essentially makes the platforms state actors.

If courts determine that platforms are state actors, then the evidence obtained from the platforms' monitoring efforts may be deemed unconstitutional. For example, an app can use a program such as PhotoDNA to automatically compare unencrypted information against a hash of material in an authoritative database. When there is a successful hit for CSAM, the app can report that to NCMEC and law enforcement can follow up to arrest the perpetrator.

But if the government forces the app to scan all the communications on the device to get around the Fourth Amendment, evidence obtained by the app would be inadmissible in the actual prosecution of the case.

It is critical that the enforcement regime remains voluntary so that evidence obtained will not be barred in courtrooms. While Congress should continue to work to target CSAM online, the bill's current approach would effectively coerce platforms into acting as the deputy of law enforcement and risks allowing criminals off the hook.

Conclusion

The EARN IT Act as currently drafted has significant problems that threaten the privacy of users and may make it more difficult to prosecute the criminals exploiting children online. While the goals of the bill are certainly laudable, Congress should consider amending the bill to both ensure important privacy features are protected and that platforms do not become state actors when they search for CSAM on their services.