The EARN IT Act: Concerns & Responses

The EARN IT Act creates new incentives for the tech industry to take online child sexual exploitation seriously. The Act amends section 230 of the Communications Decency Act (CDA) to require companies to "earn" their liability protection for violations of laws related to the trafficking of child sexual abuse material. The EARN IT Act has three components: establishing a broadly representative National Commission on Online Child Sexual Exploitation Prevention, laying out best practices for companies to detect and prevent Child Sexual Abuse Material (CSAM) and other forms of online child sexual exploitation, and bolstering enforcement if companies choose not to follow best practices or take reasonable measures.

CONCERN:

- This bill opens up tech companies to unforeseeable and unmitigable liability that necessitated CDA 230's unqualified immunities two decades ago.

RESPONSE:

- The EARN IT Act differentiates those companies that are doing the right thing to protect against online child sexual exploitation, and companies that have no interest in taking basic steps to stop CSAM. The liability opened up under the EARN IT Act is targeted against specific, illegal conduct, and the process of earning immunity is designed to promote best practices to stop child abuse, rather than merely punish companies.

- EARN IT **only** opens up an interactive computer service to civil liability and state criminal liability when:

    1. the service has elected not to self-certify that it follows best practices issued by the Commission and has failed to implement its own reasonable practices for preventing online child sexual exploitation;

    2. CSAM is found on the platform; **and**

    3. The service was either recklessly (for civil claims) or knowingly (for criminal claims) transmitting CSAM.

CONCERN:

- CDA 230's blanket immunity, applicable to all tech companies regardless of size or business model, is necessary to promote startups, and opening up liability for criminal conduct will be good for Big Tech.

RESPONSE:

- The Commission established by the EARN IT Act is required to establish multiple sets of best practices, designed to take into account the size, type of product, and business model of companies. Small businesses will have direct representation on the Commission, equal to that of large companies.
- Startups and small businesses still have a critical role in the fight against online CSAM. Smaller social media sites and messaging applications, such as Kik Messenger, are routinely

used by abusers.[1] While alternative best practices will account for the cost and time required of smaller actors, there are still simple steps that can be taken by any tech company. Through providing flexible and responsive best practices, the EARN IT Act will ensure that abusers do not flock to small platforms to evade the protections and accountability put in place on larger platforms.

CONCERN:

- CDA 230 already exempts child sexual exploitation crimes – there isn't an enforcement issue.

RESPONSE:

- CDA 230 only allows criminal enforcement actions brought by the federal Department of Justice, blocking states and survivors from their well-established role in enforcing the nation's laws. Bad actors know that even if they flagrantly violate the law the Justice Department is unlikely to have the resources to prosecute every violation, or anything close.
- Underenforcement fails victims. The EARN IT Act would ensure that there is more than one cop on the beat by enabling states and civil litigants to seek justice against those who enable child sexual exploitation.
- Finally, the EARN IT Act provides survivors an opportunity to enforce the law themselves, giving them a chance to secure compensation from the companies that facilitated and profited off their exploitation.

CONCERN:

- This is just an attempt to ban encryption.

RESPONSE:

- The EARN IT Act is not an encryption bill and does not ban encryption or otherwise impose obligations related to lawful access to data. To the contrary, the Commission is required to consider user privacy when developing best practices, and it is required to include members who are expert in cybersecurity – and to receive sign off from the Department of Homeland Security and the Chair of the Federal Trade Commission – to ensure that cybersecurity generally and consumer privacy specifically are protected.

- Tech companies say that they can deploy strong encryption and still help to reduce and remove CSAM on their servers. The Commission can help them achieve that goal.

- Best practices will require real buy-in from tech experts and companies. The Commission's structure and approval process ensures that the best practices reflect a broad consensus on what is technologically feasible and how to respect values such as data security, primarily through:

    - requiring that at least 14 out of the 19 members of the Commission (which includes four companies, two computer scientists, and two civil libertarians or constitutional law scholars) must agree on the best practices;

    - requiring that the best practices be approved by **three agency heads** with specific interests in data security, privacy, and law enforcements matters (DOJ, FTC, DHS); **and**

[1] https://www.justice.gov/usao-me/pr/westbrook-man-pleads-guilty-child-sexual-exploitation-offense

then

- requiring Congress to approve the Commission's best practices within 90 days of issuance.

CONCERN:

- If the EARN IT Act passed, tech companies would be considered government actors, because they would be acting based on a government mandate to search for illegal content. As a result, nothing the companies find on their servers would be admissible in court.

RESPONSE:

- Nobody has claimed that passage of the EARN IT Act would turn tech companies into government agents for Fourth Amendment purposes. At most, critics have claimed that if the Commission chose to require tech companies to search for CSAM then tech companies responding to that mandate could be considered government actors. In other words, the EARN IT Act raises Fourth Amendment issues only if the Commission chooses to adopt problematic best practices. There is no reason to think a Commission made up of tech companies, law enforcement, survivors, and other experts would promulgate best practices that undermine the ability of tech companies and law enforcement to stop CSAM.

- The case law in this area is extremely under-developed. It is entirely possible that courts will hold that the Commission can make searching for CSAM a best practice without raising any Fourth Amendment issue. For example, courts might determine that stripping immunity for companies that refuse to search for illegal content is not the same thing as requiring them to do so. Similarly, courts might find that just as DWI checkpoints or dog-sniff tests are reasonable under the Fourth Amendment, so is a requirement that companies utilize non-invasive technological mechanisms for identifying the most heinous criminal content.

- In the *Ackerman* opinion cited by tech companies as raising Fourth Amendment concerns, Gorsuch suggested that the **third-party doctrine** will protect evidence of CSAM found by a company that privately searched. When a company has terms and conditions that enable it to privately search, there is no Fourth Amendment violation because users lose their reasonable expectation of privacy. Gorsuch stated that "The [Supreme] Court has, after all, suggested that **individuals lack any reasonable expectation of privacy and so forfeit any Fourth Amendment protections in materials they choose to share with third parties.**"

- Even if the courts hold that the Commission cannot issue a best practice that requires tech companies to search for content, the Commission can do much good. It could simply require tech companies – if they choose to search for CSAM – to turn illicit materials over to NCMEC in a more format that is more helpful to law enforcement. Or it could create a better system for categorizing CSAM and providing law enforcement with information that allows them to catch perpetrators and liberate victims. The Commission could dramatically reduce the prevalence of CSAM without even coming close to areas that raise Fourth Amendment questions.

CONCERN:

- EARN IT violates the First Amendment.

RESPONSE:

- Child sexual abuse materials are not protected speech. Mere possession of child sexual abuse materials is a criminal violation, and there is no defensible claim that the First Amendment protects child sexual abuse material.

- Further, there is no risk that targeting child sexual abuse materials will chill protected speech. Tech companies already have free and inexpensive tools to identify and remove child sexual abuse materials without any meaningful risk of false positives – ensuring that CSAM comes down while protected speech stays up.