EARN IT Act Does Not Do Enough to Protect Encryption or Competition

Senators Lindsey Graham (R-SC), Richard Blumenthal (D-CT), and others have introduced the "EARN IT Act." This bill conditions Section 230 of the Communications Decency Act, with respect to material that sexually exploits children, to platforms that follow a Congressionally-appointed Committee's recommended best practices. This process could harm user security and privacy by disincentivizing the use of privacy-protecting technologies such as encryption.

While Public Knowledge acknowledges that platforms should do more to prevent the exploitation of children on their services, Public Knowledge cannot support a bill that could discourage the use of privacy-promoting technologies like end-to-end encryption. Additionally, a process that allows online platforms to regain a liability shield is likely to mostly benefit larger and more dominant platforms that have the resources to certify their compliance. The EARN IT Act in its current form does not address these concerns, which are far from the only criticisms that could be levied at this bill. Below is additional feedback:

- EARN IT sets up a "certification" process that is likely to be mostly taken advantage of by larger, more well-resourced companies that can afford the compliance costs.
- The issue of fair representation between large and small platforms on the Committee created by this bill is not one of representation but capability. The cost of defending one of these lawsuits is greater than the cost of seed funding for a startup. EARN IT Act does not, by creating equal representation on the Committee, make up for the disparity in resources between large platforms like Google (~$300 billion in revenue) and Signal (non-profit). New internet regulations should not further solidify the market position of dominant platforms.
- Members who sponsor EARN IT and also Attorney General Barr along with other federal law enforcement agencies have long railed against the use of encryption. For example, Senator Lindsey Graham has been outspoken in his opposition to the use of encryption by tech companies, warning them that they would need to design systems to allow for law enforcement access or "we will impose our will on you." It is not unreasonable to suspect that one of the primary purposes of this bill is to create a mechanism to limit the use of encryption generally, through a vehicle that seems to address a legitimate social harm.
- End-to-end encryption is one of the best technological tools to protect user privacy. It ensures that no one except the sender of a communication and its recipient or recipients can read it. No technology solves every privacy and security problem -- devices themselves still need to be secure, and communications providers can still see who is talking to whom, even if they don't know what they're saying. But end-to-end encryption protects users from hackers, from malicious or compromised network operators, and from other cybersecurity threats. End-to-end encryption is a tool used not just by journalists, executives, and civil rights advocates, but also by armed service members who use it to communicate securely overseas.

- The bill lacks any savings language that explicitly protects encryption, nor is there any requirement for the Committee to include language or recommendations that protect encryption. The only requirement is that the Committee *consider* issues of user privacy and security, not give them determinative weight.
- The structure of the Committee is weighted against issues of security and privacy. For example, there is no requirement that any experts in encryption or data security be members of the Committee (those are merely optional areas of expertise).

Instead, Public Knowledge urges Congress to support bills that don't sacrifice encryption or advantage large, dominant platforms over others. For example:

- Congress could require that platforms assist law enforcement in developing and funding the expertise necessary to prosecute Child Sexually Abusive Material (CSAM) cases. Many currently referred cases are not even investigated due to a lack of necessary law enforcement personnel and skills.
- Congress could mandate best practices for platforms regarding how platforms report violations to the National Center for Missing & Exploited Children. Best practices might include ways for platforms to uniformly report violations that best assist law enforcement in tracking those responsible for proliferating CSAM material.

New rules for dominant internet platforms regarding the spread of CSAM and other unlawful materials should be carefully considered by Congress, and may be warranted. But such rules should not discourage technologies that, on balance, promote privacy and security, and they should not advantage dominant platforms over smaller ones.

For general inquiries email: pk@publicknowledge.org