March 6, 2020

The Honorable Lindsey Graham
Chairman, Senate Committee on the Judiciary

The Honorable Richard Blumenthal
Senate Committee on the Judiciary

Dear Senators Graham and Blumenthal:

The undersigned organizations write to express our strong opposition to the *Eliminating Abusive and Rampant Neglect of Interactive Technologies Act* (EARN IT Act). We fully support the goal of curbing child exploitation online. We are concerned, however, that the bill's language as drafted currently is seriously flawed in several important respects, and could in fact make it more difficult for law enforcement to protect children.

First, the bill would fall far short of the goal of protecting children, while at the same time making all Americans less safe and less secure by potentially exposing everyone in society to substantially higher risk from malicious cyber actors, including hostile nation-states. We all must work together to better protect children from abuse and exploitation, but unfortunately, the bill would not be effective in addressing the crisis of child exploitation material online. It would, however, threaten the widespread adoption of strong encryption, which is essential for protecting the national security of the United States and the confidentiality, integrity, and availability of important data for all persons, corporations, and other organizations, including governmental actors.

Second, the text of the bill raises several serious constitutional questions. The bill may violate the First Amendment and creates the risk of turning private actors into agents of the government under the Fourth Amendment, potentially putting at risk any future criminal prosecutions of producers, distributors, and consumers of online child sexual abuse material. We explain our concerns about the bill in more detail below.

What the EARN IT Act Does

The EARN IT Act would create a National Commission on Online Child Exploitation Prevention ("Commission"), headed by the Attorney General and tasked with establishing "best practices" to detect child sexual abuse material (CSAM) on their services as well as to combat "child sexual exploitation," a term that has an unclear scope as used in this bill. The bill provides a procedure for Congress to enact these best practices into law. If found not to comply with these practices, interactive computer services would be stripped of important protections under Section 230 of the Communications Decency Act.

The EARN IT Act also lowers the intent standard applicable in civil child exploitation laws. Current law requires that service providers have actual knowledge that people using their services are distributing CSAM in order for them to have liability. Under the EARN IT Act, providers would face lawsuits if they allegedly have acted "recklessly," a much lower standard. The burden would then be on the provider to show that they followed the best practices or otherwise implemented reasonable measures. To be clear: the threat of such increased legal liability would, in effect, make the best practices mandatory requirements. The bill also criminalizes making a false statement in a certification of best practices and carries a 2-year prison sentence, a penalty that is redundant with existing law (which already criminalizes making a false statement to the federal government in a wide variety of contexts, carrying a penalty of a 5-year prison term).

First and Fourth Amendment Concerns

As noted above, the EARN IT Act raises several serious constitutional questions. The proposed bill may not comport with the First Amendment, as numerous categories listed as matters to be addressed in the best practices are written in an overly broad fashion, without clear definitions. For example, the recommended best practices must include measures meant to address the problem of "child sexual exploitation." This term will likely be interpreted in an overly broad manner that would lead to best practices that incentivize impermissible censorship of protected speech alongside efforts to restrict CSAM. This would present service providers of all sizes with a "choice" to either follow government-issued best practices, or face liability—thereby violating the First Amendment's protections for free expression.

Additionally, the bill raises serious questions under the Fourth Amendment, jeopardizing the admissibility of evidence in CSAM cases. If the EARN IT Act led to establishment of a "best practice" essentially requiring companies to search private communications and data for CSAM and report to law enforcement when they find it—on pain of potentially losing Section 230 protections if they do not—a court could find that such private companies were acting as "agents of the government." The actions of companies that are deemed agents of the government would have to comport with the requirements of the Fourth Amendment, including the requirement to obtain a warrant based on a judicial finding of probable cause in order to search communications content for evidence of crime. But the bill does not contemplate warrants or any judicial finding of probable cause, and it is not clear that any recognized exception to the warrant clause would apply. The structure set up by the EARN IT Act therefore creates a risk that any evidence obtained pursuant to the EARN IT Act could be suppressed, ultimately making it more difficult for prosecutors to hold predators accountable.

Threats to Encryption, Privacy, and Security

The Department of Justice has made no pretense about its desire to force online platforms to eliminate strong encryption technologies. The bill affords so much law enforcement control over the guidelines the Commission would produce, that it would provide officials a mechanism for pressuring small and large online service providers to eliminate strong encryption under threat of losing Section 230 protections.

By setting the stage for adoption of best practices that, whether directly or indirectly, require companies to avoid offering strong device encryption or end-to-end encrypted messaging services, the bill could create encryption backdoors. Backdoors to encryption make everyone in society more vulnerable to privacy, cybersecurity, and other risks.

Strong encryption is vital for national security, the economy, individual liberty, and free expression. Encryption is one of the most effective technologies available to protect safety, security, and privacy. Individuals, businesses, and governments who use encrypted services can be confident that the content of their communications will be protected against outside efforts to surveil or corrupt them. This confidence allows individuals to freely express themselves, to exchange personal and other sensitive information, and to protect their data. This includes active duty military personnel stationed overseas, scientists, doctors and patients, journalists and human rights workers abroad, corporate executives, and victims of domestic abuse and other marginalized populations. For these reasons, encryption services are also vital to the U.S. economy—large sectors including online banking, e-commerce, and R&D rely upon trusted encryption services. Removing encryption would threaten our economy and sacrifice all users' security and privacy, leaving their data and communications susceptible to misuse by bad actors of many sorts, including the military and intelligence services of hostile nation-states, organized criminals, terrorist groups, and malicious hackers. A backdoor for law enforcement is unfortunately a backdoor for all of these bad actors as well. Accordingly, undermining encryption in this way is inconsistent with the prior efforts of the Committee and its members to protect the security and privacy of all Americans.

Conclusion

While we applaud Congress' desire to address the sexual exploitation of children online, a more effective way to address that crisis would be to better equip law enforcement agencies to investigate it by adding staffing and funding to more effectively use their current lawful investigative tools. Americans should not be forced to compromise their own security in order to compensate for the failure of governmental actors to provide law enforcement agencies with the lawful and appropriate means to achieve their mission. Law enforcement agencies in the United States at all levels—federal, state, local, and tribal—do not have sufficient personnel or technical resources to investigate and prosecute all of the cases that internet service providers currently refer to the National Center for Missing and Exploited Children (NCMEC). Indeed, we understand that U.S. law enforcement prosecutes only a small fraction of the cases that NCMEC refers to them.

The bill as drafted would not fulfill its purported goal of catching criminals responsible for child exploitation online. Rather, eliminating or undermining encryption on some online platforms will likely achieve the opposite, and make law enforcement's job harder by simply pushing criminals to other communications options. In other words, EARN IT would harm ordinary users who rely on encrypted messaging, but would not stop bad actors.

Amending Section 230 through the EARN IT Act ultimately would provide no significant benefit to law enforcement and would not be effective in addressing the crisis of production and distribution of child sexual abuse material online. Instead, it would sacrifice the security and privacy of all Americans and leave them susceptible to online dangers. Therefore, we strongly oppose this bill.

Sincerely,

Access Now
Americans for Prosperity
Center for Democracy & Technology
Constitutional Alliance
Defending Rights & Dissent
Demand Progress
Digital Liberty
The Due Process Institute
Electronic Frontier Foundation
Fight for the Future
Free Press Action
FreedomWorks
Internet Society
LGBT Tech
Media Alliance
National Association of Criminal Defense Lawyers
National Coalition Against Censorship
New America's Open Technology Institute
Oakland Privacy
Restore the Fourth
R Street Institute
Surveillance Technology Oversight Project
TechFreedom
Wikimedia Foundation
X-Lab

cc: Senate Judiciary Committee Members and House Judiciary Committee Members