NetChoice

May 2, 2023

Chairman Dick Durbin
Committee on the Judiciary
United States Senate
711 Hart Senate Building
Washington, D.C. 20510

Ranking Member Lindsey Graham
Committee on the Judiciary
United States Senate
211 Russell Senate Office Building
Washington, D.C. 20510

Re: Opposition to the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2023 (EARN IT Act)

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

Congress is properly focused on combating child exploitation. But the EARN IT Act remains fraught with problems that would, if passed, threaten Americans' privacy and undermine the bill's stated aim to protect children from sexual exploitation and predation. Because the EARN IT Act continues to suffer from these defects, we ask that you **oppose** the bill.

EARN IT Would Frustrate Law Enforcement Prosecution of Child Exploitation

Under current federal law, certain internet communication service providers ("Providers") can voluntarily file reports of Child Sexual Abuse Material (CSAM) on their platforms. Those reports are sent to the National Center for Missing and Exploited Children (NCMEC), which coordinates with law enforcement to prosecute these CSAM peddlers.[1]

Although no provider is required to search its platform for CSAM, the most popular websites and platforms voluntarily choose to do so.[2] In fact, in 2022 alone providers submitted over 32 million reports of CSAM to NCMEC.[3] That's because providers have an independent motivation to search for CSAM: they don't want CSAM on their platforms.

[1] 18 U.S.C. 2258A
[2] *Id.* at (f).
[3] National Center for Missing and Exploited Children, CyberTipline Data, https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

This independent motivation and lack of government encouragement, control, or direction has been *the* key to enabling successful prosecutions of CSAM peddlers.

That's because current law does not trigger the Fourth Amendment's protection. By contrast, the EARN IT Act would trigger the Fourth Amendment by deputizing providers and, thereby, turn otherwise private attempts to ferret out CSAM into government searches.

The Fourth Amendment protects against unreasonable searches and seizures conducted by the government without a warrant.[4] Truly private searches, by contrast, do not trigger Fourth Amendment protection.[5] The Fourth Amendment will apply, however, when a private search, or the actions of a private party, can be fairly attributed to the government.[6]

The Supreme Court has clearly held that when the government becomes involved in a search by encouraging, directing, or overseeing the search then it will be considered a search *by the government* even where the physical action was taken by a private entity.[7]

For a private search to remain private, and therefore to avoid the Fourth Amendment's warrant requirements, the actions of the private searcher must be *entirely voluntary*. Voluntarily undertaking a search is crucial here. The Fourth Amendment is concerned with the voluntariness of the *initial search*. After a search has been voluntarily performed, the Fourth Amendment will not be implicated by a requirement to report the findings of a search–even when that reporting requirement mandates disclosure directly to the government.[8]

Indeed, even when particular convictions have been challenged, no court has ever ruled that the current CSAM reporting requirement transformed a private search into state action. When the current regime is challenged, that the initial searches are private is a given.[9] The only point of dispute among the courts is whether the government has *exceeded the scope* of the initial, private search.[10] Where the government exceeds the scope of a private search, without first obtaining a warrant, it violates the Fourth Amendment.[11]

---

[4] U.S. Const. Amend. IV.
[5] *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921).
[6] *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 614 (1989) ("Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government.").
[7] *See id.* ("Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the government's participation in the private parties activities[.]" (citing *Lustig v. United States*, 338 U.S. 74, 78-79 (1949) (plurality opinion))).
[8] *See e.g., United States v. Miller*, 982 F.3d 412, 424 (6th Cir. 2020) (Google's private search for CSAM was not compelled and, therefore, does not implicate the Fourth Amendment).
[9] *United States v. Sykes*, No. 21-6067 (6th Cir.2023) (Slip Op. at 3).
[10] *United States v. Ackerman*, 831 F.3d 1292, 1305-07 (10th Cir. 2016) (Gorsuch, J.); *United States v. Wilson*, 13 F.4th 961, 971-74 (9th Cir. 2021).
[11] *United States v. Jacobsen*, 466 U.S. 109, 117-18 (1984).

The EARN IT Act, however, seeks to increase reporting of CSAM material by eliminating a provider's ability to opt out of the reporting requirement. And, while increasing CSAM reports may sound appealing, the *reports* are not the end goal. The end goal is to *secure convictions* of CSAM peddlers. Yet, EARN IT would make convictions more difficult to secure.

Indeed, the EARN IT Act would trigger the Fourth Amendment's warrant requirement by transforming providers into state actors.

A private actor becomes a state actor when the action it takes can be fairly attributed to the government.[12] Private action requires private initiative. Where the government has placed its thumb on the scale, private initiative disappears. Private initiative can be displaced directly—through compulsion—or indirectly—by offering both positive and negative repercussions to incentivize compliance.[13]

The EARN IT Act does both. It would require providers to search for CSAM and make reports to NCMEC *and* it attempts to "incentivize" providers to comply by conditioning the continued protection under 47 U.S.C. § 230 on that compliance.[14] As though it were deliberately designed to eliminate any colorable claim of private initiative, EARN IT also establishes so-called "best practices" for providers to follow for identifying, disrupting, and reporting CSAM.[15]

By overpowering the private incentive to search for CSAM and replacing it with government incentives, the EARN IT Act necessarily implicates the Fourth Amendment in any and all CSAM searches done by providers. Therefore, any search undertaken by a provider without a warrant would result in that evidence being suppressed at trial.

Accordingly, EARN IT undermines the goal of securing CSAM convictions by making the very evidence used to support a conviction subject to suppression.

EARN IT Would Undermine American Privacy

At a time when threats of cyber attacks are all too real, the EARN IT Act would gut Americans' online privacy and cripple data security. Encryption is an essential security tool that turns readable data into an unreadable code so that, if it were to be intercepted by nefarious actors, it would be unreadable. The data breaches in the last few years have showcased the increased need to encrypt data in order to keep Americans safe.

---

[12] *See id.* at 113-114 (quoting *Walther v. United States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting).
[13] *Skinner* at 615.
[14] *Id.* at § 5.
[15] S. ___ § 3(b), 4(a)(1)

American companies are mindful of the data they guard. In an effort to be good stewards of our data, more companies have employed encryption technology as a safeguard against bad actors. Yet, rather than praise this innovative attitude and promote data security, the EARN IT Act would penalize and create disincentives to continue protecting our most sensitive information.

On its face, the EARN IT Act could mislead some to think that it does not penalize encryption. After all, it does say that encryption shall not be "an independent basis for liability."[16] But this is nothing more than false consolation. By making encryption a "dependent" rather than "independent" basis for liability, the EARN IT Act permits the use of crucial security measures to be used as evidence of wrongdoing. If encryption may be wielded against providers so casually, the incentives to use that tool will be severely diminished.

American innovation is our greatest protection against the world's bad actors. Our data is under threat, so providers employ encryption to keep us safe. CSAM is distributed online so providers develop sophisticated tools to ferret out the material and ensure it makes its way to law enforcement. These innovations have made the internet safer and more secure for Americans. Because the EARN IT Act would undermine these advances, Congress should oppose this bill.

Sincerely,

Carl Szabo
Vice President and General Counsel, NetChoice

[16] *Id*. at § 5.