Internet Impact Brief

How the US EARN IT Act Threatens Security, Confidentiality, and Safety Online

Natalie Campbell, John Morris, Internet Society

Anna Higgins, J.D. Candidate, University of Southern California Gould School of Law

Greg Nojeim, Center for Democracy and Technology

Contributor: Internet Infrastructure Coalition

Version 1.0, 16 November 2022

Abstract

In February 2022, the U.S. Senate Judiciary Committee approved a bill that aims to limit the liability protection of service providers guaranteed by Section 230 of the Communications Act. Though a number of Senators expressed serious misgivings about the legislation, it passed unanimously out of committee and could be considered for a full Senate vote later this year. The EARN IT Act threatens a company's ability to use and offer end-to-end encryption by putting their liability immunity at risk if they do not proactively monitor and filter for illegal user content. In doing so, it threatens the security, privacy, and safety of billions of people in the U.S. and worldwide who rely on encryption as a foundation for security online. End-to-end encryption (E2EE) is the strongest digital security shield to keep communications and information confidential between the sender and intended receivers. When used correctly, no third party – including the service provider– has the keys to access or monitor content. If passed into law, the EARN IT Act will directly threaten online service providers and Internet intermediaries, which are entities who facilitate interactions on the Internet, that supply or support encrypted services. It will also create risks for Internet infrastructure intermediaries – such as Internet Service Providers and others – that have no direct involvement in providing encrypted services.

For service providers and intermediaries offering encrypted services, the EARN IT Act would have one of three outcomes. Such providers would be forced to either:

1. Weaken security by providing a backdoor or "exceptional access" to end-to-end encrypted content for governments.
2. Bypass end-to-end encryption entirely by getting access to and surveilling content before or after the encryption process, through methods such as client-side scanning or storing a copy of every message sent, or,
3. Not offer end-to-end encrypted services at all.

Beyond this direct threat to the use of encryption – and thus the foundation of security online – the EARN IT Act could also put infrastructure providers who do not themselves provide encryption into potentially untenable positions because of state laws aimed at illegal content. By potentially making such providers civilly liable for delivering illegal traffic even without any knowledge about the contents of the traffic, states could create significant liability risk and force Internet Service Providers to block a broad range of online communications.

This Internet Impact Brief demonstrates that by preventing service providers from using end-to-end encryption – and by creating significant risks even for Internet infrastructure providers that do not directly provide encrypted services – the EARN IT Act poses an existential threat to the Internet by interfering with four of the five critical properties the Internet needs to exist. Moreover, it would also undermine most enablers that the Internet needs to thrive as an open, globally connected, secure and trustworthy resource for all.

Ultimately, EARN IT is unlikely to achieve its aim of stopping illegal activity. Undermining use of encryption makes people and businesses more vulnerable to criminal activity, and indeed preventing minors from encrypting their communications would make them more at risk of harm, not less. That's because preventing companies from using E2EE and offering secure services would undermine security and confidentiality online. This would put millions of law-abiding people in the U.S. – including marginalized groups and children – and billions more worldwide, at greater risk of harm from those seeking to exploit private data for harm. Weakening security of the Internet's infrastructure also jeopardizes national security and virtually every sector of the U.S. economy that relies on a strong Internet. Furthermore, encryption technology is widely available even without the support of service providers. Nefarious actors can and will encrypt their communications on their own even if the communication service they use does not do it for them.

While this Internet Impact Brief focuses on the EARN IT Act, the concerns we are raising would pertain to other proposals in the U.S. and abroad that would condition liability protection of intermediaries dealing with encrypted content they carry or store, or that their users create, on the intermediary's ability to ascertain meaning of that content. Unfortunately, as documented through the Global Encryption Coalition, such proposals are being made in many countries and regions.[1]

[1] These countries and regions include the UK, India, the European Union, Turkey and the U.S. https://www.globalencryption.org/blog/.

Methodology

The Internet owes its strength and success to a foundation of critical properties that, when combined, represent the Internet Way of Networking (IWN). This includes: an accessible Infrastructure with a common protocol, a layered architecture of interoperable building blocks, decentralized management and distributed routing, a common global identifier system, and a technology neutral, general-purpose network.

To assess whether the present proposal has an impact on the Internet, this report will examine its impact on the IWN foundation the Internet needs to exist, and what it needs to thrive as an open, globally connected, secure and trustworthy resource.

Context and Interpretations

The EARN IT Act would pose considerable risks for the Internet, both by directly threatening the ability of service providers to offer support for secure, encrypted communications, and by creating untenable risks even for Internet intermediaries that do not themselves offer encrypted services. This analysis will consider both sets of risk.

Billions of people worldwide rely on encryption to secure their daily activities online – often without even knowing it. It is the best digital security tool available. It keeps almost all web browsing secure and confidential from eavesdropping. It reduces the risk that criminals will get access to bank accounts of people who do things like online shopping and banking. It lets people communicate with friends and family without fear that someone is intruding on their conversation. It helps prevent bad actors from interfering with the operation of connected cars and other connected devices.

In addition to the ubiquitous way encryption keeps ordinary people secure, it is also crucial to making sure there are safe spaces for marginalized communities and vulnerable populations – including children – online. It lets parents put video baby monitors in children's rooms with the comfort that criminals will not also be able to see and even record their children. It also ensures children can submit school assignments or communicate with loved ones without bad actors getting access to sensitive data like health information, location and more that would put them at greater risk of harm.

Despite encryption's crucial role in our lives both on and offline, a pending proposal in the U.S. Congress threatens the foundation of Internet security under the misleading guise of promoting child safety. In

early 2022, Sen. Lindsey Graham (R-SC) reintroduced[2] the "Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022" – more commonly known as the EARN IT Act. The bill aims to curb the spread of child sexual abuse material (CSAM) online.

This report will demonstrate how the EARN IT Act poses a significant threat to both the Internet and users worldwide by discouraging service providers from using strong encryption, with a focus on two main components of the EARN IT Act:

1) The legislation proposes to create a National Commission on Online Child Sexual Exploitation Prevention. The Commission's mandate would include developing a list of "best practices" that interactive computer services should adopt to eliminate CSAM on their platforms, including "preventing, identifying, disrupting, and reporting" CSAM. This list is likely to include content filtering.

2) The bill amends Section 230 to allow state criminal and civil lawsuits relating to CSAM, which could include state laws with lower standards of knowledge or intention of crime than existing federal law. This means a judge could determine that using encryption or failing to follow the commission's best practices is evidence that a service provider was reckless or negligent in identifying CSAM.

The EARN IT Act includes a section that purports to "carve out" and protect the ability of intermediaries to use encryption, but the asserted carveout does very little to prevent problematic state civil or criminal laws. Technical experts and civil society organizations are thus skeptical and view this proposal as another in a long line of proposals – advanced by directors of the U.S. FBI and U.S. attorneys general over the past 15 years – that seek to prevent encrypted communications or to require the creation of insecure "backdoors" to access the plain text of encrypted communications. Although these proposals have been made by Attorneys General on both sides of the U.S. political aisle, they have always failed in the face of overwhelming technical evidence that encryption is key to security and "backdoors" cannot be made to be secure. In response to some of these proposals, the Global Encryption Coalition was formed and civil society and technical expert members raised public concern about the significant security risks posed by the previous version of EARN IT Act initially introduced in 2020.

EARN IT Act and Section 230

The 2022 EARN IT Act would remove liability protections provided to a broad range of Internet intermediaries and services by what is called "Section 230." Section 230 of the Communications Act has been fundamental to the Internet's success. Passed in 1996, the U.S. law has allowed Internet intermediaries – which are service providers that facilitate interactions on the Internet – to focus on

[2] Sen. Graham originally introduced the EARN IT Act in March 2020 during the 116th Congress. The bill passed the Senate Judiciary Committee and went to the Senate in July 2020. However, the full Senate did not consider the bill and it died when the 116th Congress ended in January 2021. https://www.congress.gov/bill/116th-congress/senate-bill/3398

offering specific services (Internet access, content hosting, search, etc.) without the risk of liability for what individual users or other third parties share or publish online. Section 230's liability protection has helped fuel innovation online, allowing many new types of Internet intermediaries to emerge over the last 26 years. This includes new platforms, Internet service providers (ISPs), and much more. Section 230's protections are crucial to the viability and operation of a vast array of large and small companies, non-profits, political parties, publications, and individuals who provide content or services online – far beyond the very large platforms about which Congress has expressed concern in the area of CSAM transmission.

The EARN IT Act proposes to change the liability landscape for Internet intermediaries by increasing the risk of liability that all "interactive computer services"[3] face when their users distribute CSAM via their services. Internet intermediaries are already liable for violations of federal criminal law, including federal bans on possessing and distributing CSAM[4]. However, Section 230 shields intermediaries from most civil lawsuits and state criminal law charges that are based on the intermediary's role in hosting or transmitting third-party content[5]. The EARN IT Act would weaken this liability protection by exposing intermediaries to federal civil law claims as well as criminal charges and civil claims under state laws addressing the "advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material."[6] The proposal is especially problematic for liability protection because there is nothing in the EARN IT Act that would require state law claims to meet the same knowledge standard as existing federal criminal law. As such, intermediaries could be subject to state-to-state variations in law and could face prosecution and civil lawsuits for CSAM being distributed on their services without their knowledge.

As Stanford Internet Observatory research scholar Riana Pfefferkorn said in a 2020 blog post: "Providers could reasonably fear that the liability threat would encompass a wide range of their services. Any service that gives users the ability to talk to each other (think social media, chat rooms, messaging apps, video conferencing services, voice calling apps); the ability to post online ads seeking to buy or sell stuff (think Craigslist); the ability to post images (think Tumblr); the ability to share files (think Dropbox) – all of these could be misused by users, rendering the provider liable under one or more laws."

---

[3] This term is defined in Section 230 as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." As detailed below, this includes well known services ranging from Internet Service Providers, to web hosting, to online content and social media platforms, and also includes less well known services such as domain name providers and content distribution networks, among others.

4 E.g. 47 U.S.C. § 2252 and 2252A.

[5] 47 U.S.C. § 230(c)

[6] EARN IT Act Sec. 5.

EARN IT Act and Encryption

Encryption is a technology that helps keep information and communications private and secure for all people, including the most vulnerable ones. It keeps data confidential by scrambling messages so that they can only be read by someone who has the "key" to unscramble the information. End-to-end encryption is the strongest form of communications encryption. It preserves confidentiality even where the sender and receiver must rely on an intermediary to deliver their messages, because only the sender and intended receiver(s) have the keys to decrypt their messages. No third party – not even the communications service provider – can decrypt end-to-end encrypted communications.

The EARN IT Act would make it possible for a court to determine that a service provider's adoption of end-to-end encryption for its users is evidence of wrongdoing. This would effectively make the service provider liable for content they cannot see.

The EARN IT Act lists circumstances and conduct related to encryption that cannot be an "independent basis" for liability:

1. "The provider utilizes full end-to-end encrypted messaging services, device encryption, or other encryption services."
2. "The provider does not possess the information necessary to decrypt a communication."
3. "The provider fails to take an action that would otherwise undermine the ability of the provider to offer full end-to-end encrypted messaging services, device encryption, or other encryption services."

When read literally, this language is meaningless. Under current law, none of these circumstances and conduct create an independent basis for liability because they are not elements of a CSAM crime. Enacting a law saying that they cannot be an independent basis for liability does not change that. However, courts are unlikely to read the language literally and are likely to struggle to find the Congressional intent for including it.

While offering end-to-end encryption in itself is not a crime, the EARN IT Act makes it possible for a court to use encryption as evidence to find a service provider liable in cases related to CSAM. If a user disseminates CSAM and violates Title 18 sections 2252, 2252a, or 2256(8) using an encrypted service, a court could determine the service provider's offering of encryption makes it liable for negligently or recklessly distributing CSAM because the encryption prevented the service provider from detecting and then blocking CSAM sent by its users – even if the service provider had no knowledge of particular CSAM being transmitted.

A service provider offering E2EE is not aware of and does not have access to the content or communications shared or published online. As such, a court might consider this use of E2EE to

determine whether the provider was in reckless disregard of CSAM distributed on its platform or was negligent in permitting its dissemination. Indeed, under the EARN IT Act, a state law could explicitly say that offering an encrypted service could be viewed as evidence of negligence or willful ignorance of CSAM transmission (without ever running afoul of the asserted "carveout" included in the EARN IT Act).

Another example of an intermediary that can have a decision-making factor in whether a user uses encryption is cloud backup services. Cloud backups can be a critical part of business and individual cybersecurity strategies, and many cloud storage companies offer a 'zero-knowledge' feature where those users can encrypt their data before it is stored. The users are the only ones with the key to decrypt the content. These services could become tools of distributors of CSAM, and thus cloud services could be at risk for knowingly offering a feature that enables user-controlled encryption – even though the cloud service providers have no knowledge of the content stored on their systems.

The impact of making Internet intermediaries at risk of liability for using E2EE will discourage its use (or encourage the adoption of backdoors, like client-side scanning, or other mechanisms to bypass the encryption). This would fundamentally weaken security online, making users and service providers more vulnerable to criminal activity.

Encryption is further threatened by the fact that the EARN IT Act's proposed amendments to Section 230 sweep in all intermediaries, including the many intermediaries who do not themselves provide encryption services to end users. Under the EARN IT Act, an infrastructure intermediary could lose its Section 230 protection for a user publishing or distributing illegal content that the intermediary did not even decide to encrypt.

As one example of how encryption could be impacted by the EARN IT Act's amendments to Section 230, consider the case of traffic between websites and their users. This traffic is encrypted with HTTPS, a protocol that uses Transport Layer Security Version 1.3 (TLS 1.3) to encrypt the connection between a browser and a server. As of February 2022, nearly 93 percent of web pages loaded by U.S. users on the Firefox web browser was with HTTPS.[7] Consider as well that many websites, including U.S. government websites, pay to use content delivery networks' (CDNs) global network of servers and data centers to better meet user demand and improve performance for activities like downloading media files, streaming video, and using social media platforms. Both CDNs and ISPs are considered "interactive computer services" under the definition in Section 230, and thus under the EARN IT Act, these intermediaries could lose their Section 230 liability protection if an end user is found to be distributing CSAM online.

[7] Let's Encrypt, Percentage of Web Pages Loaded by Firefox Using HTTPS, https://letsencrypt.org/stats/#percent-pageloads

However, CDNs and ISPs were never meant to moderate content as it flows between an end user and a website. When websites use HTTPS to secure the connection "pipe" between a user and a website server, a CDN may be used to facilitate the communication and would be aware of content at each end of the pipe. However, its role was never meant to moderate the content it helps to deliver. Taking on this task would increase the complexity of the CDN's role within the Internet's infrastructure exponentially. And yet, the EARN IT Act could put its liability at risk if it failed to do so. On the other hand, network operators like Internet Service Providers that connect end users to the Internet also would not even be able to know what information is flowing through the HTTPS traffic.

Once one court in the U.S., applying the EARN IT Act, decides an intermediary can lose their Section 230 liability protection if someone disseminates CSAM using the intermediary's service, a dangerous precedent will be set. Such a decision could influence all kinds of intermediaries to try to reduce their liability risk by weakening or avoiding encryption, or by taking disproportionate surveillance measures to ensure third party content does not contain CSAM. In some cases, this type of risk reduction would require fundamental and far-reaching changes to the service offerings (i.e. the introduction of encryption "back doors") due to the essential nature of the encrypted transport protocols used, and those changes could lead to unexpected technical problems and cybersecurity risks.

The negative consequences of forcing intermediaries, including infrastructure services, to weaken security to scan and identify content would be detrimental to the safety, security, and livelihood of users, businesses, and governments worldwide. It would also lead to severe negative financial impacts on many businesses due to the loss of trust that would result. Preventing people from locking the doors to their house makes the owner more vulnerable to criminals and intruders. If a content intermediary weakens or bypasses encryption, it is like preventing every user from locking the doors to their house to prevent criminals from getting access to their private and sensitive data and communications online. If infrastructure intermediaries are forced to do the same, it creates even more backdoors and holes into the home's foundation, giving criminals even more insidious pathways to get access.

EARN IT Act's Harmful Impact on Infrastructure Intermediaries Beyond Encryption

Looking beyond threats to encryption technology discussed above, elimination of Section 230 protections for Internet intermediaries that carry CSAM would have another profound impact on Internet infrastructure intermediaries. If the EARN IT Act becomes law, a state could, for example, enact legislation that requires ISP's, CDNs and other Internet infrastructure providers to take problematic steps to keep CSAM off their services, and make those intermediaries civilly and criminally liable if they fail to block such traffic. These service providers could face significant risk of civil litigation actions brought by individuals under such legislation. This could both disrupt secure Internet operations and lead to the blocking of lawful content as well.

While limiting the spread of CSAM is an appropriate goal for a state, allowing 50 different state legislatures to impose various (and likely differing) obligations on the operation of the Internet and the provision of Internet services – to combat a global problem – creates enormous risks of unintended and unlawful consequences. Past state-level efforts to combat CSAM on the Internet – while well intended – have caused significant problems[8], and future efforts enabled by the EARN IT Act would carry similar risks. Enabling states to legislate to address a global problem on a highly technical infrastructure is likely to lead to unpredictable future problems.

Similarly, the Commission that the EARN IT Act creates may recommend "best practices" that result in the blocking by intermediaries of not only CSAM, but of perfectly lawful content as well. It is difficult to establish best practices that are tailored to the operation of networks with differing topologies. As with authorizing 50 states to legislate their own approaches to CSAM, the Commission creates risk and uncertainty across the many intermediaries on which the Internet operates.

How the EARN IT Act Would Impact the Internet

What the Internet Needs to Exist

The Internet owes its success not only to the technology that makes it work, but to the unique way it operates and evolves. The Internet Way of Networking describes a foundation of critical properties that, all together, are what the Internet needs to exist and work for everyone. The Internet's unprecedented growth and success is a direct result of people and organizations committed to protecting this foundation as the Internet has expanded worldwide. This section examines how the EARN IT Act would impact certain critical properties that the Internet requires to exist and function.

Critical Property 1: An Accessible Infrastructure with a Common Protocol

It's easy for a network to access the Internet because the only essential condition is to adopt its common protocol - IP. This 'permissionless' feature of the Internet's design –using the lowest possible technical barrier to access– is what has led to its rapid growth and reach worldwide.

By eliminating Section 230 protections for infrastructure intermediaries in situations involving CSAM, the EARN IT Act would allow states to impose blocking requirements on intermediaries or create new civil claims for damages arising out of any transmission of CSAM, with no requirement that civil liability be based on actual knowledge of the presence of CSAM. This would put Internet service providers and other infrastructure services at risk of civil liability for unknowingly facilitating the delivery of CSAM

8 See, e.g, CDT v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004) (overturning state law aimed at blocking access to CSAM sites because law ended up blocking access to more than a million lawful websites).

content. This could lead to court-ordered or state-imposed mandates on carriers and ISPs to intercept traffic through DNS or IP blocking, which carry a significant risk of preventing access to lawful content. Content blocking to pre-emptively interfere with the movement of data that is not illegal undermines the permissionless model of the Internet by creating significant barriers to access to the global Internet's open and accessible infrastructure.

Critical Property 2: An Open Architecture of Interoperable and Reusable Building Blocks that are Openly Defined and Voluntarily Adopted by a User Community

Section 230's liability protections cover many different types of intermediaries on the Internet, including infrastructure providers such as ISPs and CDNs, which play a role in the Internet ecosystem that differs from the role that content service providers play. They know they are carrying, storing, or otherwise facilitating the flow of communications content. However, they do not know the substance or meaning of those communications, nor were they designed for this purpose. This has allowed infrastructure providers to focus on simple functions to facilitate the flow of traffic across networks without having to know what the content is.

The EARN IT Act hinders the ability of intermediaries to use a critical community-adopted building block for Internet security: encryption. It does so by creating liability risk to the intermediary that cannot monitor content users share, store, or publish online. State laws could seek to impose civil liability on every party involved in the creation, carriage, or storage of communications, including ISPs, web hosting providers, cloud backup services, and encrypted communications services like WhatsApp.

The EARN IT Act's broad scope is especially problematic for infrastructure intermediaries. Their primary role in the Internet ecosystem is to transfer data without needing to monitor what content lies within that data. The proposal, however, coerces these intermediaries to undermine E2EE and create processes to monitor the data that flows through their pipes. These intermediaries are not appropriate vehicles to monitor content because their infrastructural designs are not meant to do so.

Furthermore, in the face of civil liability for damages under state laws permitted by the EARN IT Act, network operators could decide to stop carrying encrypted traffic or take other actions to block such traffic to avoid the risk of liability. Doing so would make them less interoperable with networks carrying E2EE traffic. Without interoperability, Internet users may experience slower and less secure web browsing.

As the Internet Society wrote in a 2020 paper on intermediary liability, changes to a regime "could affect the interoperability of building blocks and applications across networks, undermining the so-called end-to-end principle where the networks are agnostic to the data they pass along. This would make innovation more difficult, since applications would need to consider additional network functionality, or make complex arrangements with the network."

Critical Property 4: Common Global Identifiers

IP addresses are what ensure that any two systems on the Internet can find each other. Likewise, the Domain Name System (DNS) is an identifier space, and one of its functions is providing a consistent map of IP addresses to domain names. Making sure common global identifiers like the IP and domain name addressing systems are intact is crucial to the Internet.

The EARNIT Act could lead to infrastructure services pre-emptively blocking or filtering traffic, either in response to a direct state mandate or to reduce risk of civil liability.

Content filtering that uses IP-based blocking places barriers in a network that block all traffic to or from a set of IP addresses. Blocking whole ranges of IP numbers 'over-blocks' wide swathes of the Internet, blocking many more than the intended sites or services. Over-blocking using the DNS causes similar 'collateral damage' when an entire website is blocked in order to cut access to specific pages or types of content on it. All these practices fragment the global identifier systems and damage the critical property that makes the Internet consistently accessible.

Critical Property 5: A Technology-Neutral, General-Purpose Network that is Simple and Adaptable

Under the EARN IT Act, an infrastructure provider with a decision-making role in the use of strong encryption would be at risk of losing Section 230 immunity if a user uses the service to transmit CSAM (knowingly or not). The intermediary's offering of encryption could be used as evidence of negligence for unknowingly transmitting CSAM over its networks – even if it was never meant to be aware of content in the first place. Infrastructure intermediaries are not designed to scan content, which is what allows them to be general-purpose and focused on data transmission and storage. Furthermore, taking on this role would likely significantly increase the cost of Internet connectivity. Similarly, state law imposing civil liability would be unbounded in the realm of CSAM, and states have in the past enacted well-intended but highly problematic civil statutes.[9]

The Internet would no longer be able to function as a general-purpose network if infrastructure intermediaries had to scan every piece of data that runs through their systems. Under the EARN IT Act, states would be free to impose a range of obligations on infrastructure providers, possibly to scan content or filter certain data. The Internet works because it provides the opportunity for all kinds of data and platforms to flourish and shows no favoritism towards certain content. Asking infrastructure

[9] See, e.g, CDT v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004) (overturning state law aimed at blocking access to CSAM sites because law ended up blocking access to more than a million lawful websites).

providers to filter data would be like asking an electricity company to only supply power to user televisions if they watch the shows the company approves.

The general-purpose nature of the Internet is what allows new entrants to have a chance to succeed. These new entrants include platforms, businesses, and online services. Without the technology-neutral, general-purpose approach, the digital economy and innovation would suffer. The economic impact of weakened encryption is discussed below in the section on "Data confidentiality of information, devices, and applications."

What the Internet Needs to Thrive

In addition to the critical properties the Internet needs to exist, there are additional characteristics, or "enablers," that it needs to thrive. The Enablers of an Open, Globally Connected, Secure and Trustworthy Internet can help us get closer to the kind of Internet we want, and that many countries and organizations worldwide have committed to supporting, now and in the future. The following section analyzes how the EARN IT Act would impact these enablers, preventing the Internet and everyone that uses it from benefiting from its full potential.

Easy and Unrestricted Access

"It is easy to become part of the Internet, for networks and users alike. Network operators can easily add themselves to the Internet's infrastructure without unnecessary regulatory or commercial barriers. Responsive Internet infrastructure creates an Internet that is affordable for users and that has accessible services, empowering users to connect and use the Internet with minimal barriers."[10]

One of the greatest benefits of the Internet is its ability to generate innovative new companies, services, and products. However, the EARN IT Act will pose a significant barrier to entry for U.S. startups and small companies, causing innovation to suffer while giving the big tech companies an even stronger advantage against smaller competitors.

If the EARN IT Act is implemented in its current form, it could force service providers to choose between removing end-to-end encryption or weakening it by attempting the impossible task of creating a secure backdoor to end-to-end encrypted communication. In addition, the Act could lead to an unpredictable and detrimental array of state law obligations.

If a service provider chooses to create a backdoor to access the content it carries, it would no longer be able to use end-to-end encryption or offer it to its users. Not only would this significantly weaken

[10] The first paragraph of this and subsequent sections are quoted from the Enablers of an Open, Globally Connected, Secure, and Trustworthy Internet, Internet Society, 2021, https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

security, but it would also be a costly process that especially hurts smaller service providers. The cost of creating and managing backdoors would be expensive. Platforms would need encryption engineers on constant standby to respond to inevitable attacks on the backdoor. And history has shown that it is impossible to restrict the backdoors to only authorized users. They will certainly be leaked or independently discovered and used by people with bad intent.

The only companies that could afford the costs of running large-scale surveillance systems are the largest interactive computer services. Therefore, under the EARN IT Act, companies would have to decide between a business model that sacrifices privacy and security for their users, or not enter the market at all. Alternatively, providers could attempt to create a separate, non-end-to-end encrypted product for the U.S. market while maintaining an end-to-end encrypted service elsewhere. However, creating multiple product lines is expensive and resource intensive, even for large companies. Smaller providers would not be able to flourish under this scenario, especially because they would likely be closed out of non-U.S. markets that do not limit the use of encryption. Given the global nature of the Internet and its users, this is generally not a viable option for the vast majority of service providers.

By creating a barrier to entry for service providers and users, the EARN IT Act will harm the open Internet. The companies that can afford to create and maintain backdoors to encrypted services will be the ones that decide what (less secure) services and products users can find online. As a result, users will have fewer options of services that they can use on the Internet. And, very crucially, there are numerous strong encryption options available that are outside the jurisdiction and control of the U.S. government and its allies. The net result is that this would create a significant harm to most of the general population of the U.S., with no hope of achieving its stated goal of countering CSAM.

Unrestricted Use and Deployment of Internet Technologies

"The Internet's technologies and standards are available for adoption without restriction. This enabler extends to end-points: the technologies used to connect to and use the Internet do not require permission from a third party, OS vendor, or network provider. The Internet's infrastructure is available as a resource to anyone who wishes to use it in a responsible and equitable way. Existing technologies can be mixed in and used to create new products and services that extend the Internet's capabilities."

Encryption is an Internet technology that revolutionized security online. It is what has allowed the Internet to foster a digital economy where users can do things like shop and bank online.

If enacted, the EARN IT Act would restrict how innovators can use end-to-end encryption with other technologies to create new products and services, significantly restricting the U.S.'s advantage as a powerhouse for technology and innovation. It would also hinder the ability of service providers to develop and use new secure cryptographic protocols to keep themselves and users secure among an ever-evolving threat landscape.

For example, encryption is an important building block for cloud backup and storage providers. Some cloud storage providers offer a "zero-knowledge" security architecture. This architecture ensures that only the customer has the key that unlocks the stored data, which is encrypted. The cloud storage provider has no access to the key and cannot decrypt it. Zero-knowledge security architectures provide the highest assurance that only customers have access to the data. Not even a data breach at the provider would disclose the customer's data. These services are used by a range of entities that hold particularly sensitive data, including news media, legal aid and law firms, academic institutions, health care providers, financial services firms, and many more. In fact, this is a critical service for industries bound by regulations (such as finance, legal and health) that require them to use the highest level of data privacy. Similarly, any commercial entity with valuable trade secrets would insist that cloud storage providers provide zero-knowledge encrypted storage. Under EARN IT, however, these cloud storage providers would face risk of civil liability if a user is found to use the service for CSAM on the theory that providing zero-knowledge storage was negligent because it prevented the storage provider from detecting the CSAM. Potential liability for damages under state laws – which would be permitted if the EARN IT Act becomes law – would discourage or prevent cloud storage providers from offering a zero-knowledge security architecture.

In restricting the use of encryption, the EARN IT Act promotes an Internet that is less open by limiting service providers from using all available technologies.

Unrestricted Reachability

"Internet users have access to all resources and technologies made available on the Internet and are able to make resources available themselves, contributing to the Internet's role as a resource of global knowledge production. Once a resource has been made available in some way by its owner, there is no blocking of use and access to that resource by third parties."

The Internet is made of more than 70,000 independent networks that work together by using the same common language or "protocol." They make their own decisions on how to route traffic to one another, which allows them to 'route around failure' and operate at utmost efficiency to meet local requirements and the needs of users.

As noted above, infrastructure intermediaries are a critical part of the Internet's plumbing that aren't meant to monitor the content that flows through their pipes. And yet, the EARN IT Act makes it possible for them to lose their liability protection if they don't do so. Under the EARN IT Act, states could impose content blocking obligations for CSAM, or impose civil liability on intermediaries for carrying CSAM traffic, even if the intermediaries were unaware that the traffic they carried included CSAM. This risk could force infrastructure intermediaries to adopt new and disruptive ways of operating, including by content blocking or attempting to gain access to communications content (e.g., through deep packet inspection) so they can make sure it does not include CSAM.

Coercing these service providers to have to block or monitor content is inconsistent with the role of infrastructure providers, which are agnostic to the content they carry. It also risks over-blocking and would slow down the flow of the data that they carry. Even if an infrastructure intermediary were to attempt to take on this role, it would not be possible without the cooperation of major service providers that make up the Internet's ecosystem. This is highly unlikely since enabling encryption "back doors" involves a significant redesign of their systems and the resulting loss of trust puts their core business at major risk. Furthermore, since only image based CSAM is detectable via content scanning, it is simply not practical for video. This expectation that infrastructure providers must scan content for CSAM could hinder their ability to be resilient, cost efficient, and work in a way that optimizes traffic flows.

The EARN IT Act's changes to Section 230 could impose significant new requirements on companies that would require a significant re-architecture of their systems and could change network topology. The resulting loss of trust by their customers would likely be followed by significant negative impacts to their businesses. This also interferes with the decentralized nature of the Internet by restricting the autonomy and agility of networks to collaborate with each other. Not only would this significantly restrict and fragment a user's experience of the Internet, it would also pose significant economic disadvantages and hinder the resilience and performance of the Internet at large.

Furthermore, if the EARN IT Act essentially forces secure communications tools out of the U.S. market, U.S. users will either be excluded from accessing and contributing information and technologies on the Internet, or they will choose to use secure non-U.S. products offered in countries that promote strong Internet security.

Many Internet users cannot or will not access or share resources on the Internet without services that use strong end-to-end encryption to guarantee privacy and security online. The Global Encryption Coalition, civil society organizations and Internet experts worldwide maintain that end-to-end encryption is critical to the personal and national security of people and countries. For instance, victims of domestic violence often rely on encrypted communications as a confidential lifeline to get themselves and their families to safety. Likewise, many journalists rely on encryption when working on sensitive stories, especially in authoritarian countries, to submit their stories and keep themselves and sources out of harm's way. And ordinary Internet users will hesitate to share and communicate online if they feel unsafe. Excluding users from accessing and sharing resources by jeopardizing their privacy, security and safety online significantly hinders knowledge sharing, collaboration, innovation, and a range of other benefits enjoyed on the Internet.

With many service providers based in the U.S. also operating in other countries, the EARN IT Act will have significant extraterritorial impact. If people cannot communicate or share sensitive content with the security of and confidentiality assured by end-to-end encryption, they may choose not to communicate it at all. As a result, the EARN IT Act could decrease the flow of data and resources

worldwide. Meanwhile, criminals who distribute CSAM – who are often sophisticated Internet users – will easily find ways to encrypt illegal material to hide their activity in less secure distribution channels.

By limiting end-to-end encryption technologies, the EARN IT Act will significantly impact user and service provider behavior to the detriment of a globally connected Internet.

Available Capacity

"The capacity of the Internet is sufficient to meet user demand. No one expects the capacity of the Internet to be infinite, but there is enough connection capacity – ports, bandwidth, services – to meet the demands of the users."

The EARN IT Act could compel larger service providers to use client-side scanning to avoid risking losing intermediary liability protections. Client-side scanning (CSS) refers to a system that can scan the content of a message before it is sent to another user. It would work by comparing content - text, images, files - against a database of known objectionable content. To circumvent encryption, the analysis is done either on the user's device or on a cloud server before content is encrypted.

In 2021 Apple proposed an approach to client-side scanning, which was criticized by more than 90 civil society groups worldwide because oppressive governments could abuse it and it endangered youth online. Apple has since scrapped its plans.

In addition to the significant danger to device security, CSS in practice would significantly decrease available capacity for networks and users in underserved communities.

The resources and bandwidth required to scan, monitor, and keep databases updated would hinder the performance and efficiency of some intermediaries. For ISPs, latency could increase. For CDNs, websites could load much more slowly, which could hinder large transactions, the synchronization of clocks on computers, and other matters that rely on mere seconds. Users would also be affected, as they would experience increased data costs and latency. This would disproportionately affect millions of Americans in underserved communities who already lack fast, affordable, and reliable Internet access.

It would be impossible for interactive computer services to scan and monitor content without their services running less efficiently. Internet users would ultimately face worse services in this case, including Internet access.

Data Confidentiality of Information, Devices, and Applications

"Data confidentiality, usually accomplished with tools such as encryption, allows end users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating. Allowing the transfer of sensitive information helps create a secure Internet. Data confidentiality also extends to data-at-rest in applications. (N.B., "confidentiality" also contributes to privacy, which is part of a trustworthy Internet)."

End-to-end encryption ensures what people share and say to each other online stays confidential between the sender and receiver(s). By preventing service providers from using end-to-end encryption, or breaking it with backdoors, the EARN IT Act will jeopardize the safety and security of people and businesses in the U.S. and worldwide.

Data confidentiality is crucial for businesses that handle financial transactions, exchange confidential information, or have important trade secrets. If criminals get access to this data, it can be disastrous for businesses that handle large amounts of money and private information of clients and users. Policies that weaken data confidentiality can have a significant impact on an economy. A recent study of the economic impact of laws that weaken encryption found Australia's TOLA Act to have a significant impact on local industry. One company told researchers that "they had experienced a direct adverse economic impact and estimated the effect as being to the order of AU$ 1 billion" – over $700 million in U.S. dollars. Extrapolating this impact to reflect the scale of the U.S. tech industry would be significant.

The EARN IT Act will also discourage businesses from using zero knowledge, end-to-end security architectures (see above) to secure user data, which would make companies and individuals much more vulnerable to large-scale data breaches and eavesdropping attacks. These kinds of breaches not only inflict reputational and financial loss on the companies concerned. They also could have severe consequences for American consumers including financial loss, disclosure of healthcare data, exposure to identity fraud, and much more. It would be unfortunate if the Internet we have now (which can securely handle our most sensitive personal and financial information) became instead an Internet where we could only share information we were comfortable shouting from the rooftops to everyone.

There are many reasons law abiding humans need confidentiality online. End-to-end encryption is also a valuable tool for vulnerable communities that rely on it for safety. For members of the LGBTQ+ community, encrypted technologies create a safe space for individuals to come out, find resources, and connect with others who understand their situations. For survivors of domestic violence, encryption is a life-saving tool. Encrypted communications allow for survivors to plan and execute escape from abusive situations, protect their whereabouts from abusers, and find safe living situations. Taking confidential communication away from vulnerable individuals would rob them of a crucial lifeline and put them at greater risk.

Integrity of Information, Applications, and Services

"Strong encryption helps ensure that the integrity of data sent over the Internet, and stored in applications, is not compromised. Critical underlying Internet services, such as DNS and the routing system, cannot be manipulated or compromised by malicious actors. Data stored in applications cannot be manipulated or compromised by third parties."

Encryption is critical to data integrity online. The EARN IT Act jeopardizes this by encouraging service providers to either create encryption backdoors or remove end-to-end encryption. Backdoors to

encryption are a vulnerability that puts service providers and users at significant risk of malicious attacks. As discussed in earlier sections, there is no way to create a backdoor that can only be used for law enforcement purposes. Anyone seeking access to a backdoor to encryption, including criminals and hostile actors, could exploit the vulnerability to access and manipulate sensitive information.

Furthermore, the EARN IT Act could prompt the largest interactive computer services to create large scale surveillance systems. These kinds of systems are impossible to run securely and in a way that only allows access for law enforcement. The existence of backdoors breaks end-to-end encryption and opens a vulnerability for bad actors.

Small or medium size interactive computer services would likely not be able to manage to maintain a backdoor while also monitoring and responding to all security threats to it. Even the large interactive computer services that have enough money to spend on a backdoor would likely not be able to manage it securely due to the large volume of data that interactive computer services use and the inevitability of human error.

Virtually every sector in the United States relies on the security of strong end-to-end encryption. Businesses rely on it to protect sensitive financial data and user information. Utilities, government agencies, service providers, and other infrastructure services also rely on strong encryption to keep their systems secure from manipulation by attackers.

Furthermore, services that are encompassed by the term “interactive computer service” vary widely and may use different encryption standards. Inconsistent encryption standards could cause systemic complexities along the supply chain between the service provider and the user. This could lead to more machine-in-the-middle attacks (MITM), where a third party intercepts a communication between users. It could also make devices more vulnerable to manipulation. For instance, in February 2022 a teen found a vulnerability in a third-party app installed in some Teslas which allowed him to unlock doors and control the music and headlights.

By restricting the use of strong encryption, the EARN IT Act significantly jeopardizes the integrity of information, applications, and services on the Internet, placing business, individuals, and national infrastructure at greater risk of harm. This would result in a less secure Internet for everyone.

Reliability, Resilience, and Availability

"The Internet is reliable when technology and processes are in place that permit the delivery of services as promised. If, for example, an Internet service’s availability is unpredictable, then users will observe this as unreliable. This can reduce trust not just in one single service, but in the Internet itself. Resilience is related to reliability: a resilient Internet maintains an acceptable level of service even in the face of errors, malicious behavior, and other challenges to its normal operations."

When people use end-to-end encrypted services, they expect their communications and the data they share to remain private. The EARN IT Act would erode this expectation and damage trust online by encouraging service providers to remove or weaken encryption. Weakening encryption puts people, businesses, and national security at risk. It also creates a major disconnect between the level of Internet security expected from the service and what is actually delivered. This will deteriorate users' perception of reliability of both encryption and the Internet.

If users cannot rely on the privacy and security of service providers who weaken encryption, users will be less likely to rely on these services and the Internet itself. Billions of users need the privacy that the Internet affords for everyday activities like protecting personal information, health information, finances, and more. Users may avoid sharing sensitive information on the Internet if they believe their personal details can be exposed.

Likewise, government officials and military personnel also depend upon the reliability of end-to-end encryption for national security and rescue missions. For instance, many service members and veterans relied on encrypted communications – namely the messaging app Signal – to help rescue former Afghan colleagues after the United States pulled out of Afghanistan in August 2021. In this case both parties relied on end-to-end encryption to keep communications private. Those rescued might not otherwise have been able to communicate, for fear of having their identities and location discovered, and hence exposing themselves to imprisonment or death.

More recently, encrypted services have been essential to users living in Ukraine during the Russian invasion and occupation. Apps like Telegram (which has the option for end-to-end encrypted messages), Zello, and Signal saw increased downloads during the beginning of the Russian invasion in February 2022. These services protect Ukrainians from Russian surveillance and can aid them in reaching safety.

If the EARN IT Act is implemented as written, it will significantly impact the reliability of encrypted services online, reducing the trustworthiness of the Internet and services delivered over it.

Accountability

"Accountability on the Internet gives users the assurance that organizations and institutions they interact with are directly or indirectly acting in a transparent and fair way. In an accountable Internet, entities, services, and information can be identified and the organizations involved will be held responsible for their actions."

Service providers have certain responsibilities to be careful with user data under data privacy laws. The trend for data privacy laws is to protect consumers more, as seen with the California Consumer Privacy Act and the General Data Protection Regulation (GDPR) in the European Union. To help meet their responsibilities for user data privacy under data privacy legislation, providers often employ strong

encryption to protect consumers. The EARN IT Act jeopardizes this accountability for data privacy by threatening end-to-end encryption.

There is no way for platforms to provide the highest level of data protection using a weakened form of encryption or none at all. The EARN IT Act will force platforms to choose between retaining their Section 230 liability protection or using a digital security tool that is critical to privacy, personal safety, and national security. Because Section 230 protections are essential for sites that invite user content, platforms may choose to weaken users' privacy and security so they can continue to operate with Section 230 protections. Given the trend in U.S. data privacy laws, platforms that choose to do so would become less accountable to their users.

The EARN IT Act reduces providers' ability to offer the most private and secure forms of communications, and thus would foster loss of data security. As such, the EARN IT Act significantly reduces accountability on the Internet and reduces trustworthiness.

Privacy

"Privacy on the Internet is the ability of individuals and groups to understand what information about them is being collected and how, and to control how this is used and shared. Privacy often includes anonymity."

When users seek out end-to-end encrypted services, they expect that their information and communications will be kept private and secure. The EARN IT Act would significantly reduce privacy online by incenting companies to weaken or remove end-to-end encryption. As such, EARN IT significantly jeopardizes the personal safety of everyone online. Even if encryption exists with backdoors, bad actors like abusers and criminals can access their victims' information and communications.

By restricting the use of end-to-end encryption, the EARN IT Act would decrease the amount of control that users have over who can access, share, and store their data. This would have significant negative privacy consequences for individuals, businesses, and governments seeking to protect national security.

Summary and Recommendations

Working to promote the safety of children online and in real life is an important goal. However, it is critical to find solutions that do not make people, including children, more vulnerable in their personal, family, financial, and business lives. Encryption is our strongest digital security tool to promote security, safety, and privacy online. It is a crucial means to secure the information carried or stored by intermediaries that operate core parts of the Internet's infrastructure, and important to companies that offer communications and content services online.

This Internet impact brief has demonstrated how the EARN IT Act poses an existential threat to Internet security by coercing intermediaries of all kinds to weaken or drop end-to-end encryption and monitor their traffic to retain liability protection. In doing so, the EARN IT Act threatens four of the critical properties the Internet needs to exist: an accessible infrastructure with a common protocol; an open architecture of interoperable and reusable building blocks; common global identifiers; and a technology-neutral, general-purpose network. The legislative proposal also jeopardizes several elements the Internet needs to thrive as an open, globally connected, secure, and trustworthy resource for all. With so many facets of society, economy, and national security relying on a strong Internet, the impact of weakening encryption would be disastrous to the security, privacy, and safety of people - including children - and businesses in the U.S. and worldwide. The EARN IT Act would likely put them at greater risk of harm by threatening their strongest digital security shield that helps them protect themselves and their information from bad actors.

To mitigate harm to what the Internet needs to exist and thrive, and protect the security, privacy, and safety of people in the United States and worldwide, this brief offers four observations:

1. The EARN IT Act coerces interactive computer services, including Internet infrastructure intermediaries, to break end-to-end encryption, not use encryption at all, or block traffic that is not encrypted. The encryption "carveout" in the legislation does not remedy these problems. If adopted, this bill would lead to an Internet that is less open, globally connected, secure and trustworthy. In turn, it would significantly jeopardize the personal safety of law-abiding people worldwide.
2. No legislation should remove, weaken, or reduce the incentives to use end-to-end encryption through backdoors and/or government access.
3. The EARN IT Act would also authorize states across the country to adopt their own unique mandates and liabilities, which would further damage the ability of Internet intermediaries to operate as part of the global Internet (and would harm the ability of all but the largest companies to offer services at all).
4. Congress should establish a process through which it can conduct Internet impact assessments to give more careful consideration to the potential impact of legislation on what the Internet needs to exists and thrive before members vote on such legislation.

Appendix A – Tables – How EARN IT Act would Impact What the Internet Needs to Exist and Thrive

What the Internet Needs to Exist: Critical Properties of the Internet Way of Networking

The EARN IT Act would have a negative impact on four of the five critical properties of the Internet Way of Networking.

Critical Property	Effect of the EARN IT Act
1. An Accessible Infrastructure with a Common Protocol	Negative: Court-ordered or state-imposed CSAM blocking mandates on ISPs and other infrastructure providers can result in over-blocking, thereby compromising the open and accessible infrastructure of the global Internet and creating significant barriers to access.
2. An Open Architecture of Interoperable and Reusable Building Blocks	Negative: Coercing infrastructure intermediaries to have the ability to monitor content and/or block encrypted traffic would prevent them from using encryption, a community-adopted security building block and best practice and would therefore hinder interoperability.
4. Common Global Identifiers	Negative: Content filtering that uses IP based blocking places barriers in a network that block all traffic to or from a set of IP addresses. Blocking whole ranges of IP numbers 'over-blocks' wide swathes of the Internet, blocking many more than the intended sites or services. Over-blocking using the DNS causes similar 'collateral damage' when an entire website is blocked to cut access to specific pages or types of content on it. Each of these practices fragment the global identifier systems and damage the critical property that makes the Internet consistently accessible.
5. A Technology-Neutral, General-Purpose Network	Negative: Requiring infrastructure intermediaries to scan for content can force infrastructure intermediaries to specialize and design their services to accommodate specific types of content.

What the Internet Needs to Thrive: Enablers of an Open, Globally Connected, Secure and Trustworthy Internet

Internet Goal	Enabler	Effect of the EARN IT Act
Open	Easy and Unrestricted Access	Negative: Forcing service providers to create "backdoors" to encryption, such as complex content monitoring systems, creates a barrier to entry for new market entrants.
	Collaborative Development, Management, and Governance	Negative: By forcing the development of services and apps that must meet locally imposed technical standards, start-up companies lose the ability to compete for business outside of their local markets.
	Unrestricted Use and Deployment of Internet Technologies	Negative: Restricting use of encryption limits service provider use and development of widely available and robustly tested security technologies.
Globally Connected	Unrestricted Reachability	Negative: To minimize liability risk under EARN IT Act and ensuing state civil and criminal laws, network operators, CDNs and cloud storage providers could be forced to adopt new requirements that hinder reachability and result in over-blocking. Furthermore, users who can't

		use services that guarantee privacy will be excluded from accessing and sharing resources on the Internet, reducing flow of information and collaboration online. Users who do use services that undermine privacy will suffer privacy-related harms such as identity theft, account takeovers, etc.
	Available Capacity	Negative: Implementing a large-scale surveillance system will hinder the performance for some of the intermediaries, resulting in lower capacity to serve content. This will also increase latency for Internet Service Providers, disproportionately affecting millions of Americans who lack fast, affordable, and reliable Internet access.
Secure	Data Confidentiality of Information, Services, and Applications	Negative: Restricting end-to-end encryption will reduce data confidentiality for people and businesses, and governments in the U.S. and globally, ultimately resulting in a less secure Internet for everyone.
	Integrity of Information, Applications, and Services	Negative: Weakening or removing encryption from services makes them more vulnerable to attacks that would reduce the integrity, such as eavesdropping attacks; different encryption standards cause systemic complexity in the supply chain to the user.
Trustworthy	Reliability, Resilience, and Availability	Negative: The unreliable nature of weak encryption erodes user trust in encryption technology and the Internet itself.
	Accountability	Negative: The EARN IT Act would create a new Commission to create "best practices" for service providers to adhere to, but it fails to describe accountability or reporting measures, or how those "best practices" would be tested for security or reliability.
	Privacy	Negative: Weakening or removing encryption reduces privacy, and the ability for people to control who can access, share, and store their data.