The Effect of International Proposals for Monitoring Obligations on End-to-End Encryption

By Kir Nuthi | November 14, 2022

European and American policymakers have proposed imposing monitoring obligations on Internet intermediaries in order to improve online safety. Despite their best efforts, these proposals risk undermining users' privacy by eliminating the use of end-to-end encryption. Therefore, policymakers should not pursue them.

INTRODUCTION

In 2022, three separate government bodies published draft legislative proposals with the same goal: to protect members of their nation's public while they are online. First, the U.S. Senate Judiciary Committee published the EARN IT (Eliminating Abusive and Rampant Neglect of Interactive Technologies) Act of 2022 in January, a bill targeting child predation and criminal activity related to child sexual abuse material (CSAM) online.[1] In March, the United Kingdom government introduced the Online Safety Bill, which requires search engines, social media firms, and other user-created content services to seek and potentially remove a variety of online content through compelled monitoring obligations.[2] And in May, the European Commission followed with its legislative proposal, focusing on protecting children from criminal activity and exploitation online.[3]

The EARN IT Act, the Online Safety Bill, and the EU scanning proposal create monitoring obligations for online services to scan all content, including photos, private messages, and cloud files. While these bills have noble goals, each proposal would pressure Internet companies to prohibit end-to-end encryption (E2EE), a process that maximizes users' privacy, free expression, and security online.

Rather than impose monitoring obligations on online services, policymakers should instead:

- exclude encrypted services from monitoring obligations,
- increase resources for national law enforcement agencies to find and prosecute criminal activity related to CSAM, and
- improve reporting from and coordination with online services to better enable national law enforcement agencies to track, remove, and prosecute illegal activity in a timelier fashion.

In 2021, online services in the United States issued 29.1 million CyberTipline reports of apparent CSAM to the National Center for Missing and Exploited Children.[4] Reports such as these ensure that enforcement entities can find perpetrators and shield individuals from harm, and online services can identify and remove illegal content online. Law enforcement legislation that predates the rise and evolution of social media—such as the European Union's Child Sexual Abuse Directive—could not predict or properly encompass how online crime and illegal activity has evolved. For that reason, future legislation needs to make it easier to find and prosecute bad actors and keep people safe, but any method of doing so cannot risk the online safety E2EE provides.

THE IMPORTANCE OF END-TO-END ENCRYPTION

Encrypted information has existed since before the Internet age. From the cipher method used by Julius Caesar to the Enigma machine in World War II, individuals have been using encryption to protect confidential communications, trade secrets, and national security information.[5]

Design of Encryption

At the heart of any encryption scheme are the following:

- **The Message**: the desired communication and text or file
- **The Ciphertext**: the jumbled and indecipherable form of the message
- **The Key**: the solution to the puzzle, which turns the ciphertext back into the message

Box 1: Basic Caesar Cipher Encryption Scheme Diagram

```
Message: Hi there!

Ciphertext: Lm xlivi!

Key : e f g h i j k l m n o p q r s t u v w x y z a b c d

      a b c d e f g h i j k l m n o p q r s t u v w x y z
```

A Caesar cipher involves a fixed substitution of letters. If "a" becomes "e," then "c" should become "g."[6] And Enigma used electromagnetic rotors and plug boards to change alphanumerical characters on multiple levels.[7]

But encryption in the digital age is much more complex than were its mechanical predecessors. Modern E2EE uses complex algorithms to encrypt the ciphertext in transit, at rest, and until the end user uses its key to decrypt it.[8] These algorithms can be either symmetric or asymmetric. Symmetric encryption has both the encrypter and the decrypter use the same key. In contrast, asymmetric encryption has a public key used by the encrypter to encode the message that only the decrypter's private key can decode.[9] A key is a fancy term for the solution string used by encryption algorithms to encrypt or decrypt information. It's like the solution to a large, sometimes exponentially long math problem.

Box 2: Simplified Symmetric Versus Asymmetric Encryption

Matthew and Anna discuss their dog Maya on an encrypted service.

Symmetric Encryption: Both Matthew and Anna use the same password to unencrypt their messages.

Matthew sends message: "Maya is sick, taking her to the vet today."

Matthew uses password: Wo0fWo0f32!

Message is encrypted.

Anna receives message.

Anna uses password: Wo0fWo0f32!

Message is decrypted as: "Maya is sick, taking her to the vet today."

Asymmetric Encryption: Matthew and Anna use different passwords to unencrypt messages.

Matthew sends message: "Maya is sick, taking her to the vet today."

Matthew uses password: Wo0fWo0f32!

Message is encrypted.

Anna receives message.

Anna uses password: Parr0tsEatC@ts

Message is decrypted as: "Maya is sick, taking her to the vet today."

Third parties would be unable to decrypt these messages without the password.

Encryption provides important features to users, including:

- **Authenticity**: the ability to verify a message's origin
- **Confidentiality**: the ability to completely scramble messages and maintain the private nature of the contents until decrypted
- **Integrity**: the ability to prove that the message has not been manipulated, tampered with, or otherwise changed[10]

Purpose of End-To-End Encryption

E2EE protects the confidentiality, authenticity, and integrity of user data even when it is held by a third-party online service.[11] If using or providing E2EE, the online service does not have the decryption key required to access a user's communications or contents.[12] While it is sometimes possible for third parties to identify where users are holding, sending, or receiving messages, third parties cannot decrypt them. E2EE has many applications, including the following:

- **Messaging:** Messaging apps such as Wire, Signal, and WhatsApp use E2EE to make sure only the participants directly messaging each other can consensually access their information, photographs, and videos.[13]
- **Email:** Email platforms such as Protonmail use E2EE to protect email messages from third-party access.[14]
- **Videoconferencing and Chatbots:** Videoconferencing software, chatbots, and other communication channels can use E2EE to protect sensitive data.[15]
- **Home Security:** Ring—the home security system owned by Amazon—allows users to use E2EE to protect against unauthorized access to their security and home footage.[16]
- **Commercial Use:** Microsoft is rolling out E2EE support for commercial customers to protect users during Team Calls so that sensitive data discussed in one-on-one conversations is safeguarded.[17]

Online services use E2EE to protect consumer privacy. The more parties who can access a user's data, the greater the risk of data breaches. Using E2EE ensures that these services do not have access to unencrypted user data, thereby mitigating the risk of data breaches from insider attacks, negligence, incompetence, or bad actors.

E2EE services have been historically used by dissidents to protect themselves from authoritarian regimes, activists to organize protests against institutional injustice, individuals from marginalized communities to protect

their identity and sensitive information from being outed without their consent, reporters to communicate with whistle-blowers and other confidential sources, grassroots politicians to protect themselves from repressive government control, and abuse survivors to stay safe from threats of persecution or violence.[18] Each of these communities can use E2EE to restrict who can access their secure data and communications, reducing the risk of government interference, political suppression, or potential incarceration or other loss of bodily autonomy. In the wake of George Floyd, police brutality protesters turned to Signal to stay anonymous, with 135,000 new first-time users joining the E2EE communications platform the first week of June 2020.[19] Any weakening of E2EE or encrypted protections will negatively affect users' ability to protect themselves online.

GENERAL MONITORING OBLIGATIONS DE FACTO COMPEL SCANNING OF ALL CONTENT

From a content moderation perspective, the purpose of monitoring obligations is to ensure online services thoroughly screen user-created content to prevent the spread of harmful content, misinformation, and illegal activity. General monitoring obligations do so by explicitly holding the online service strictly liable for user-created content on their platform. In contrast, intermediary liability frameworks that do not have general monitoring obligations either do not hold online services liable for user-generated content or only hold them liable when they have actual knowledge of illegal content.[20] Intermediary liability frameworks that use a broad immunity model—such as the EU's e-Commerce Directive or the United States' Section 230 of the Communications Decency Act—place the burden of liability on the creators of content rather than online services, while holding online services liable for removing illegal content known to be on their sites.[21] While broad immunity models leave it up to the online services to design the specifics of their content moderation practices, monitoring obligations narrow services' ability to self-moderate by delineating what content services must prevent and how they will be held strictly liable if they do not.

What Monitoring Obligations Broadly Mean for End-To-End Encryption

Monitoring obligations tend to lead to over-moderation of content because online services face potentially significant penalties for false negatives (i.e., unintentionally allowing prohibited content) and little to no penalties for false positives (i.e., unintentionally removing permissible content). When monitoring obligations are limited to public-facing user-created content, they do not actually affect a user's privacy (i.e., the secrecy of communications).[22] It is only when a monitoring obligation compels the scanning of all content, including private content, that it infringes upon a user's privacy.

When monitoring obligations require scanning of encrypted channels, these obligations become fundamentally incompatible with E2EE. From a confidentiality perspective, monitoring obligations will de facto compel online services to look through their users' messages, something that runs contrary to keeping messages private until decrypted. And from an integrity perspective, monitoring obligations that force online services to weaken their encrypted protections or create backdoors create security vulnerabilities that can be exploited by foreign adversaries or other bad actors—something that would make it impossible to prove messages have not been potentially manipulated, tampered with, or otherwise changed. In short, monitoring obligations intrude into the lives of hundreds of millions of adults and children, who have a right to have their private life, personal data, and personal integrity online respected.[23]

PROPOSALS TO CIRCUMVENT END-TO-END ENCRYPTION

Law enforcement and espionage agencies in a variety of nations—including Australia, the United Kingdom, the United States, China, Russia, and Saudi Arabia—have called for circumventing E2EE, especially to protect national security.[24] But these proposals would harm online privacy and security and are ripe for abuse.

Backdoors

A backdoor is a catch-all term for a built-in method that allows someone to bypass security measures. With regard to E2EE, backdoors enable third parties to access encrypted data without the user's key.[25] If tech companies were to create backdoors to encryption, by their own will or by government fiat, they would open their users' encrypted information to heightened vulnerabilities. Famously, Tim Cook, the CEO of Apple, said that, with regards to encryption backdoors, "the reality is if you put a back door in, that back door's for everybody, for good guys and bad guys."[26]

Weak Encryption Protocols

One type of backdoor is introducing a vulnerability in an encryption protocol.[27] For example, an online service could implement an encryption protocol with a known vulnerability to allow third parties that know of this weakness to break the encryption.[28] Anyone who knows about, or discovers, this vulnerability can exploit it. Indeed, the National Security Agency (NSA) has allegedly used this tactic to create a faulty random number generator standard that serves as a backdoor in widely used encryption protocols.[29]

Key Escrow

Another type of backdoor is key escrow—a system that maintains copies of private keys that allow a third party to recover access to encrypted data.[30] In the 1990s, NSA created the Clipper Chip—a device that provided encrypted

protections for messages sent through the devices it was installed on and also used key escrow to give law enforcement access to the encrypted messages. The Clipper Chip was meant to help law enforcement work around the Data Encryption Standard—a symmetric encryption algorithm developed in the 1970s and ultimately replaced by the Advanced Encryption Standard in the 2000s.[31]

The purpose of modern encryption protocols is to provide mathematically provable security. Key escrow systems undermine this security because the security of encrypted data no longer depends on the strength of the encryption protocol but rather on the degree to which a third party protects keys in its key escrow system.[32]

Client-Side Scanning

An alternative to backdoors is client-side scanning. Also known as endpoint filtering or local processing, client-side scanning scans the content of messages (e.g., images and videos) before they are sent or received to check against a repository of illegal content.[33] The application responsible for the client-side scanning then reports to a third party whether the scanned content matched anything in the repository.[34] The risk of client-side scanning is that it could be used without authorization, such as to search devices in scenarios that would normally require a warrant, or that it could be used to search devices for material that is legal by manipulating content in the repository.[35]

SUMMARY OF THE BILLS' PROVISIONS

The following aggregates findings from the EARN IT Act, Online Safety Bill, and the EU Scanning Regulation to illustrate what their monitoring obligations are and how these obligations impede E2EE. The provisions affecting E2EE can be found in Appendix A.

Table 1: Bill provisions that affect end-to-end encryption

Bill	Type of monitoring obligation	Provisions affecting E2EE	What the provision does	Effect on encryption
EARN IT Act[36]	Monitor for and remove CSAM	Section 5	Federal civil and state civil and criminal prosecutors can use the existence of encryption technologies as contributory evidence to hold platforms responsible or complicit in the distribution of CSAM.	While the bill does not outright ban E2EE, it places liability pressures on online services that use E2EE if they are found to be negligent in preventing CSAM on their services, pushing these companies to eliminate E2EE to avoid legal battles, fines, and state civil and criminal liability.
Online Safety Bill[37]	Monitor for and remove illegal content and monitor for and moderate legal but harmful content	Section 93 Section 104	The Online Safety Bill requires online services to prevent priority illegal content such as terrorist content and CSAM on their platforms and allows the enforcing regulatory agency to compel the prevention of this content using accredited technology if it considers there to be material risk of illegal content on the platform.	By including private communications in the scope of the legislation and failing to exempt these communications like other modes of messaging, the bill de facto compels services to scan all content to prevent priority illegal content, which goes against the principles of encryption and undermines E2EE.
EU Scanning Regulation[38]	Monitor for and remove CSAM and grooming or comply with the strict technical requirements of detection orders	Article 7 Article 10	Coordinating authorities have the ability to create detection orders for E2EE services, treat encryption as willful blindness by online services, and leave method of compliance up to the online services themselves.	Compelling services using E2EE to comply with any detection orders from the EU Centre that require the ability to scan and access the contents of messages will incentivize them to stop using E2EE, create a backdoor, or begin client-side scanning.

While the text differs, each bill focuses on encryption either explicitly or implicitly to strip it of the protection E2EE needs to survive.

THE EARN IT ACT

In January 2022, Senators Lindsey Graham (R-SC) and Richard Blumenthal (D-CT) along with 18 co-sponsors introduced the EARN IT Act of 2022, a bill that targets child predation and criminal activity related to CSAM online.[39] This bill had a predecessor, the EARN IT Act of 2020, from which it derived much of its text.[40]

Background on the EARN IT Act

The EARN IT Act targets what its sponsors call the "abusive and rampant neglect" of online services to protect children by amending Section 230—the U.S. intermediary liability framework for the Internet—to make online services liable for users conducting presumed child predation online.[41]

Section 230 affirms that users, not services, are liable for what they post online and shield services from liability over their content moderation decisions.[42] Section 230 does not apply to content that violates federal criminal and intellectual property law, and Congress amended it in 2018 to not apply to content that violates federal and state sex-trafficking law—an amendment that has proven neither effective nor helpful in fighting sex trafficking.[43] Section 230 places the burden of liability on the creators of content, encourages the content moderation practices of online services, and does not impede federal enforcement of criminal, intellectual property, or sex trafficking laws.

Section 230 does not require platforms to police content on their sites, remove any content, or engage in content moderation of any kind.[44] However, Section 230 does not protect online services if they "refuse to report or remove" CSAM because creating, possessing, and distributing CSAM is illegal under federal criminal law.[45]

The EARN IT Act's Monitoring Obligation

The EARN IT Act's defining feature is a monitoring obligation that amends Section 230 to open online services to civil and state liability charges if their services are found to have CSAM.[46] Section 5 of the EARN IT Act would expose online services to federal civil action, state criminal prosecution, and state civil prosecution if they fail to prevent the advertisement, promotion, presentation, distribution, or solicitation of CSAM on their website.[47] If a state finds that a platform should have known there was CSAM on its platform and failed to remove and report it, the online service could be held liable for possessing and sharing that content.[48] Section 5 of the text effectively creates a monitoring obligation by removing intermediary liability protections for civil action against the presentation or distribution of CSAM on online services.[49]

Under EARN IT, online services face an impossible task of being damned if they do, damned if they don't.[50] Online services can't continue to host and moderate content and report and remove CSAM when reported or found; instead, online services must prevent criminals from ever posting CSAM by monitoring private communications or prescreening before evidence exists, or potentially face state civil and criminal and federal civil action. If online services fail to predict when CSAM could occur, they could be subject to endless litigation under over 50 different legal regimes for CSAM when it is already a federal criminal offence to produce or distribute CSAM—something that will push online services to remove large swaths of potentially legal speech from survivors and of-age individuals that could potentially be deemed as fodder for litigation.[51]

EARN IT Act's Effect on End-to-End Encryption

With regard to encrypted communications or services that use E2EE, the use of E2EE could be seen as knowing recklessness or the failure to prevent the presentation and distribution of CSAM on their services. Section 5(7) allows federal and state prosecutors to use the implementation of E2EE on services, the inability to decrypt, or the lack of removing E2EE as potential evidence in court if and only if used in conjunction with another reason for liability.[52] In cases where prosecutors cite public issues with the services that benefited predators, implementation of E2EE on an online service can be used to corroborate the claims.

Other reasons for liability would be dependent on more than 50 different standards of civil and criminal recklessness. States could choose the lowest threshold for prosecution and make online services liable for CSAM they did not even know existed or was present.[53] Litigation under these circumstances would be highly subjective and could compel providers to weaken encryption protections to ensure that they do not become liable under obligations presented in EARN IT.

In simpler terms, this section would push online services into legal battles over whether continuing to use E2EE is knowingly reckless behavior and their failure to prevent child predation on their services. If a platform should have known there was illegal child predation, then the government could argue that its use of E2EE was reckless and contributed to its failure to prevent the presentation and distribution of CSAM on its service, and thus is punishable under the EARN IT Act. Because online services that use E2EE cannot scan encrypted content without undermining the confidentiality of users' data, the monitoring obligation within EARN IT could compel platforms to remove or weaken E2EE in their offerings for fear of endless litigation and other harsh legal risks.

Recommendations for the EARN IT Act

Instead of trying to fix the EARN IT Act, Congress should prioritize legislation that improves how online services report CSAM and maximizes federal efforts to investigate and prosecute these crimes. For example, Senator Ron Wyden (D-OR) and Rep. Anna Eshoo (D-CA) have sponsored the Invest in Child Safety Act to address CSAM by establishing a new office in the White House to coordinate federal efforts to prevent, investigate, prosecute, and treat victims of child exploitation, increasing funding for law enforcement activities to prevent child exploitation and creating standardized reporting requirements for online services to use when notifying authorities of potential crimes.[54] These steps would help law enforcement agencies and online services work together more efficiently to find perpetrators and shield children from harm.

Additionally, Congress should prevent the banning or de facto banning of encrypted services in future legislative proposals. This includes protecting private communications from the scope of future legislation and content moderation proposals.

THE ONLINE SAFETY BILL

In March 2022, the United Kingdom introduced the Online Safety Bill, which requires search engines, social media, and other services focused on user-created content to follow duties of care—binding legal obligations designed to prevent harm to others—to seek and remove a variety of online content.[55] The Online Safety Bill has put the U.K. government at the forefront of global efforts to address the spread of harmful content online.

Background on the Online Safety Bill

When the United Kingdom was part of the EU, online safety and content moderation was regulated under the EU's e-Commerce Directive—a negligence liability model for intermediary liability.[56] The e-Commerce Directive gives online services the broad immunity to choose to moderate and does not prescribe a general monitoring obligation of content on online service providers. But it does hold the liability protections provided contingent on removing and reporting all known illegal activity on the platforms once they become aware of it.[57]

In 2019, the Department of Digital, Culture, Media, and Sport pitched the Online Harms White Paper, a proposal that would eventually become the Online Safety Bill, to redesign its online safety regime post-Brexit.[58] The U.K. government proposed the bill in May of 2021 and officially introduced the Online Safety Bill in the House of Commons in March of 2022.[59] The bill was then amended in the Public Bill Committee in May and June of 2022 before it hit its report stage.[60] (As a matter of timing, it is important to

note that as of the first week of November of 2022, the Online Safety Bill did not have any amendments that fixed its issues facing E2EE.)

The Online Safety Bill's Monitoring Obligation

The Online Safety Bill imposes a general monitoring obligation for all user-to-user and search content providers to moderate illegal and certain types of legal but harmful content on their platforms. Depending on the size, risk, type, and other relevant indicators of an online service, the Online Safety Bill can compel services to monitor for more or less content, with all services required to moderate for illegal content and content that is legal but harmful to children. Services that are either exclusively a search service or contain a regulated search engine will face duties to prevent fraudulent advertising. And higher risk or Category 1 services—likely online services with the largest audiences and a range of high-risk features—will be required to additionally moderate for content harmful to adults, protect content of democratic importance or journalistic content, and prevent fraudulent advertising.[61]

User-to-user services are only exempt if their only user-created content is emails, SMS messages, MMS messages, aural communication, reviews, or some combination of these types—and if these services do not contain bill-regulated pornographic content, do not have a "significant number of United Kingdom users," and do not consider the United Kingdom a "target market."[62] All other user-to-user services are covered, including over-the-top messaging platforms such as Signal and WhatsApp that might associate an ID with a phone number but send images, text, and files through the Internet to users specifically instead of to their phone number.[63]

The duties of care within the bill focus on the removal, scanning, prevention, and risk assessment of these types of user-created content. Safety duties regarding illegal content require online services to prevent users from seeing the problematic content, minimize the time the content is on the service, and swiftly take down such offenses.[64] The Online Safety Bill also contains an accredited technology requirement, which creates an enforceable scanning requirement for services that Ofcom—the U.K.'s communication regulator—finds noncompliant with the duties of care surrounding illegal content.[65]

Online Safety Bill's Effect on End-to-End Encryption

The Online Safety Bill would potentially force messaging platforms and other online services covered by the legislation—even those that use E2EE—to scan all user content for terrorism content and CSAM, which is not possible if services use E2EE, unless they use client-side scanning.[66]

Section 104(2)(b) of the Online Safety Bill would require all providers to build the capabilities to scan content on their services in case these services face detection and accredited technology notices from Ofcom.[67] The Online Safety Bill also requires firms to produce risk assessments about how they moderate content regulated in the Online Safety Bill.[68] It would be impossible for online services that use E2EE to determine in their risk assessments whether users are sending illegal content through their services. Additionally, if Ofcom finds it to be a necessary and proportionate measure to deal with priority illegal content, then Ofcom can compel online services to "use accredited technology to identify … and swiftly take down" terrorism and CSAM content "whether communicated publicly or privately by means of the service."[69] Because this obligation would presume the scanning of all user-created content, online services would need to find a workaround that scans previously E2EE content for priority illegal content. The bill defines whether an accredited technology notice is necessary and proportionate based on if a platform has previously received a warning notice; whether the warning notice has expired; and Ofcom's consideration of a variety of factors including the potential prevalence, dissemination, and risk of relevant illegal content on the platform.[70]

The Online Safety Bill also criminalizes when skilled persons or senior managers provide encrypted information in response to an information notice from Ofcom with the intention of preventing Ofcom from understanding the information.[71] Section 93(4) essentially requires all encrypted information to be understandable (read unencrypted) for Ofcom to audit and judge whether a provider has complied with enforceable requirements or whether there are ways to mitigate the risks of noncompliance.[72] While Section 93(4) hinges on whether a person at the provider's "intention" were to prevent Ofcom from understanding the information, the Online Safety Bill fails to define or explain what would constitute "intention."[73] The penalty for noncompliance is £18 million, 10 percent of qualifying worldwide revenue, or even summary convictions for staff.[74]

Rather than face the potential fines and noncompliance punishments of the Online Safety Bill, these private communications platforms that use E2EE are more likely to leave the United Kingdom altogether to avoid undermining their security and privacy standards or weaken their protections in advance of being compelled by the U.K. government to avoid the potential for noncompliance. Head of WhatsApp Will Cathcart, for example, has publicly refused to kowtow to the mandates within the Online Safety Bill and weaken the platform's security protections.[75]

Recommendations for the Online Safety Bill

U.K. policymakers should, at minimum, amend the Online Safety Bill to make it compatible with E2EE. First, they should remove Section 104(2)

entirely to ensure that covered services do not have to undermine E2EE and build the capabilities to scan content on their services in fear of being issued an accredited technology notice. The liability structure created by allowing Ofcom to issue accredited technology requirements to online services de facto compels online services to create access points and weaknesses in their E2EE. Second, U.K. policymakers should remove Section 93(4) because it makes it a fineable offense to intentionally provide Ofcom with encrypted communications. And finally, they should protect services that use E2EE and encrypted communications from the scope of the Online Safety Bill, allowing U.K. users to choose to use encrypted protections online. Doing so would ensure that online services aren't obligated to weaken encryption to conduct risk assessments as well as minimize the potential for discriminatory content moderation litigation against E2EE services based on the Online Safety Bill.

Unlike how the proposed Online Safety Bill focuses on policing platforms, the United Kingdom could instead pivot to solutions that incentivize voluntary reporting and public-private partnerships with online services to tackle the worst the Internet has to offer. A focus on child safety legislation and law enforcement legislation that provides more resources to the nation's police and law enforcement to tackle cybercrime would be a strong start in pivoting toward the improved prosecution of online criminals. Similarly, providing Ofcom with the resources to work with online services could improve how they report illegal activity, which would significantly quicken the ability of law enforcement to track, remove, and prosecute cybercrime.

THE EU SCANNING REGULATION TO COMBAT CSAM ONLINE

In May 2022, the European Union issued a legislative proposal focusing on protecting children from criminal activity and exploitation online.[76] The EU proposal requires websites to filter and scan for CSAM as well as potential grooming on websites and online services.

Background on the EU Scanning Regulation

The e-Commerce Directive is not the only regulation that dictates online safety policy in the EU. The EU recently adopted the Digital Service Act—a new legislation for online safety that updates the e-Commerce Directive's content moderation regulation within the Union.[77] The Digital Services Act aims to make that which is illegal offline also illegal online.[78] The Digital Services Act creates obligations to counter illegal content quickly, strengthens traceability to fight counterfeits and crime on online marketplaces, increases transparency surrounding content moderation algorithms, and bans so-called "dark patterns"—deceptive design practices implemented to get consumers to buy, click, or subscribe to something—in

online interfaces.[79] During conversations over the adoption of the Digital Services Act, the EU Parliament approved language to protect rights to secure E2EE and anonymity, but these provisions ultimately did not make it into the final text.[80]

The proposed scanning regulation takes into consideration the EU's "Strategy for A More Effective Fight Against Child Sexual Abuse" and builds on the regulations that delineate CSAM offenses (the Child Sexual Abuse Directive). The "Strategy for A More Effective Fight Against Child Sexual Abuse" was developed from Europol reporting increases in CSAM during COVID-19 and specifically targeted E2EE as a technology that proliferates CSAM.[81] The goal of the strategy was to implement and update current legislation, create new legislation to fill the gaps, and create an EU Centre to coordinate new member state efforts and strengthen prevention programs. The strategy acknowledged that E2EE has privacy benefits but stated that a solution was needed for "end-to-end encrypted electronic communications."[82] The Child Sexual Abuse Directive was the EU's first comprehensive legislation detailing criminal offenses for CSAM online and offline and was a key first step in the EU's new strategy.[83] This new scanning regulation is the next step.

Scanning content may not even be allowed according to the e-Privacy Directive—an EU legislation designed to protect Internet users from privacy violations by private companies or governments.[84] Due to this policy conflict, EU lawmakers have created both proposals to filter communications for CSAM and declarations to balance encryption and privacy protections with content moderation challenges.[85]

The EU Scanning Regulation's Monitoring Obligation

The proposal targets information society services, hosting services, interpersonal communications, software application stores, and Internet access services to compel them to prevent, scan, and disable access to CSAM—targeting a broad swath of, if not all, online services that touch, host, or otherwise affect user-created content.[86] The proposal also applies these rules to all providers of the aforementioned online services within the Union, including those that are based abroad.[87] For this reason, it is not hyperbolic to say that the proposed regulation could affect almost all electronic communication in the EU.[88]

The proposal's monitoring obligation hinges on risk assessment, risk mitigation, and detection orders. In the risk assessment phase, online services must consider the existence and implementation of functionalities used to mitigate CSAM.[89]

Online service risk assessments must take into account the risk of solicitation of children, where the service is used by children, the risk of

solicitation by age group, and an analysis of the functionalities that can be used to create or reinforce the risk of solicitation.[90] The functionalities that must be analyzed include user-to-user contact, "in particular through private communications."[91] Online services must then tailor new mitigating strategies to the risks identified in their risk assessments that are effective, targeted, proportionate, and nondiscriminatory, and can be reviewed or expanded upon.[92]

After reporting the risk assessments and mitigation measures to the Coordinating Authority at a service's place of residence, the Coordinating Authority can issue a detection order if it believes the online service did not adequately mitigate the risks at hand "to an appreciable extent for the dissemination of known child sexual abuse material."[93] Online services that receive these detection orders must install and operate technologies that are either made available by the newly created EU Centre or comply with the requirements indicated by the EU Centre.[94] These technologies must be effective, the least intrusive to the confidentiality of communications, and able to extract the information that is strictly necessary to detect CSAM.[95]

The new EU Centre for CSAM would also be able to search and scan online services with its own filtering technologies. The proposal provides the EU Centre with the ability to use filtering technologies to verify needs for detection orders and assess the potential of publicly available CSAM on platforms before notifying the service providers.[96] In practice, this establishes a two-part obligation for online services. Online services would have to analyze, scan for, and prevent content before reporting their information to coordinating authorities—something they currently do through voluntary reporting. And coordinating authorities would be able to compel further action by online services as prescribed by the EU Centre for CSAM. At the same time, the EU Centre for CSAM would be able to search and regulate based on its own filtering technology.

EU Scanning Regulation's Effect on End-to-End Encryption

The EU scanning regulation's use of detection orders and filtering technologies requires the ability to scan and access the content of messages—something that is not possible in transit due to E2EE and would only be possible at rest through technologies such as client-side scanning. Requiring online services to assess risk on E2EE platforms would be near impossible, which could lead coordinating authorities to issue a detection order due to the online service not adequately mitigating the risks for CSAM, as per Article 7.[97]

In fact, these detection orders could force previously end-to-end encrypted communications to scan for both identified CSAM as well as potential solicitation and risks of CSAM. To do so, platforms would need to

undermine their encryption, as E2EE cannot access such user-created content without removing the protections to push forth scanning technology of any kind. Online services that use encrypted communications will most likely be compelled to remove E2EE to best comply with any detection orders sent should they arise, create a backdoor that can be exploited by cyberattacks, or begin client-side scanning—a tool that is particularly ripe for abuse. Similarly, allowing coordinating authorities the opportunity to push forth detection orders and treat encryption as potentially willful blindness by online services can and will disincentivize the use of E2EE in the first place. The threat of a detection order is enough for many online services to weaken encrypted communications or remove E2EE on their services.[98]

Recommendations for the EU Scanning Regulation

The EU should redraft the proposal to protect E2EE from the potential detection technologies, including by amending the proposal to exempt E2EE services from either the detection orders or the legislative text altogether. Similarly, the EU should also prevent misuse of Article 7 of the legislative text by prohibiting coordinating authorities from issuing detection orders based on the use of E2EE.

Additionally, the EU should better coordinate with national law enforcement at the supranational level by both providing further investment and guidance in child protection and well-being services and cyber-forensics operations and dedicating more resources to pursue CSAM and child predation online. Focusing on prevention programs and law enforcement capacity could be a strong way for the EU to strengthen its current "Strategy for A More Effective Fight Against Child Sexual Abuse" that acknowledges the benefits of E2EE, further tackles child predation and CSAM online, fills legislative gaps, and better coordinates member state efforts.

CONCLUSION

In response to growing concerns about online safety, three international proposals have created a new foundation for online content regulation that tips intermediary liability on its head for the worse. The American EARN IT Act, the United Kingdom Online Safety Bill, and the recent EU proposal to prevent child abuse online all create monitoring obligations for online services that will incur a de facto prohibition of E2EE. Given the potential consequences—especially the privacy implications—there is a need for more viable solutions that will ensure that legislative solutions do not undermine encryption and encrypted communications.

APPENDIX A: PROVISIONS AFFECTING E2EE

EARN IT Act

Section 5 (6) of the EARN IT Act

Section 230(e) of the Communications Act of 1934 (47 U.S.C. 230 (e)) is amended by adding at the end the following:

> *"(6) NO EFFECT ON CHILD SEXUAL EXPLOITATION LAW. — Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit—*
>
> > *"(A) any claim in a civil action brought against a provider of an interactive computer service under section 2255 of title 18, United States Code, if the conduct underlying the claim constitutes a violation of section 2252 or section 2252A of that title;*
> >
> > *"(B) any charge in a criminal prosecution brought against a provider of an interactive computer service under State law regarding the advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material, as defined in section 2256(8) of title 18, United States Code; or*
> >
> > *"(C) any claim in a civil action brought against a provider of an interactive computer service under State law regarding the advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material as defined in section 2256(8) of title 18, United States Code.*

Section 5 (7) of the EARN IT Act

"(7) ENCRYPTION TECHNOLOGIES. —

> *"(A) IN GENERAL. — Notwithstanding paragraph (6), none of the following actions or circumstances shall serve as an independent basis for liability of a provider of an interactive computer service for a claim or charge described in that paragraph:*
>
> > *"(i) The provider utilizes full end-to-end encrypted messaging services, device encryption, or other encryption services.*
> >
> > *"(ii) The provider does not possess the information necessary to decrypt a communication.*
> >
> > *"(iii) 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."*
>
> *"(B) CONSIDERATION OF EVIDENCE. — Nothing in subparagraph (A) shall be construed to prohibit a court from considering evidence of actions or circumstances described in that subparagraph if the evidence is otherwise admissible."*

ONLINE SAFETY BILL

Section 9 (3) of the Online Safety Bill

A duty to operate a service using proportionate systems and processes designed to— (a) prevent individuals from encountering priority illegal content by means of the service; (b) minimise the length of time for which any priority illegal content is present; (c) where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, swiftly take down such content.

Section 104 of the Online Safety Bill

104 Notices to deal with terrorism content or CSEA content (or both)

(1) If OFCOM consider that it is necessary and proportionate to do so, they may give a notice described in subsection (2), (3) or (4) relating to a regulated user-to-user service or a regulated search service to the provider of the service.

(2) A notice under subsection (1) that relates to a regulated user-to-user service is a notice requiring the provider of the service to do either or both of the following—

(a) use accredited technology to identify terrorism content communicated publicly by means of the service and to swiftly take down that content;

(b) use accredited technology to identify CSEA content, whether communicated publicly or privately by means of the service, and to swiftly take down that content.

(3) A notice under subsection (1) that relates to a regulated search service is a notice requiring the provider of the service to do either or both of the following—

(a) use accredited technology to identify search content of the service that is terrorism content and to swiftly take measures designed to secure, so far as possible, that search content of the service no longer includes terrorism content identified by the technology;

(b) use accredited technology to identify search content of the service that is CSEA content and to swiftly take measures designed to secure, so far as possible, that search content of the service no longer includes CSEA content identified by the technology.

(4) A notice under subsection (1) that relates to a combined service is a notice requiring the provider of the service to do any of the following—

(a) use accredited technology as described in subsection (2)(a) or (b), or both, in relation to the user-to-user part of the service;

(b) use accredited technology as described in subsection (3)(a) or (b), or both, in relation to the search engine of the service;

(c) use accredited technology as described in subsection (2)(a) or (b), or both, in relation to the user-to-user part of the service, and

use accredited technology as described in subsection (3)(a) or (b), or both, in relation to the search engine.

(5) For the purposes of subsections (2) and (3), a requirement to take down terrorism or CSEA content, or to take measures to secure that search content does not include terrorism or CSEA content, may be complied with by the use of accredited technology alone or by means of the technology together with the use of human moderators to review terrorism or CSEA content (as the case may be) identified by the technology.

(6) See section 105 for provision about matters which OFCOM must consider before giving a notice under subsection (1).

(7) OFCOM may give a notice under subsection (1) to a provider relating to a service, or (in the case of a notice described in subsection (4)(a) or (b)) part of a service, only after giving a warning notice to the provider that they intend to give such a notice relating to that service or that part of it.

(8) The warning notice under subsection (7) must—

(a) contain details of the technology that OFCOM are considering requiring the provider to use,

(b) specify whether the technology is to be required in relation to terrorism content or CSEA content (or both),

(c) specify any other requirements that OFCOM are considering imposing (see section 106(2) to (4)),

(d) specify the period for which OFCOM are considering imposing the requirements (see section 106(6)),

(e) state that the provider may make representations to OFCOM (with any supporting evidence), and

(f) specify the period within which representations may be made.

(9) A notice under subsection (1) that relates to both the user-to-user part of a combined service and the search engine of the service (as described in subsection (4)(c)) may be given to the provider of the service only if—

(a) two separate warning notices have been given to the provider (one relating to the user-to-user part of the service and the other relating to the search engine), or

(b) a single warning notice relating to both the user-to-user part of the service and the search engine has been given to the provider.

(10) A notice under subsection (1) may not be given to a provider until the period allowed by the warning notice for the provider to make representations has expired.

(11) A notice under subsection (1) relating to terrorism content present on a service must identify the content, or parts of the service that include content, that OFCOM consider is communicated publicly on that service (see section 188).

(12) For the meaning of "accredited" technology, see section 106(9) and (10).

Section 105 of the Online Safety Bill

105 Matters relevant to a decision to give a notice under section 104(1)

(1) This section specifies the matters which OFCOM must particularly consider in deciding whether it is necessary and proportionate to give a notice under section 104(1) relating to a Part 3 service to the provider of the service.

(2) The matters are as follows—

(a) the kind of service it is;

(b) the functionalities of the service;

(c) the user base of the service;

(d) in the case of a notice relating to a user-to-user service (or to the userto-user part of a combined service), the prevalence of relevant content on the service, and the extent of its dissemination by means of the service;

(e) in the case of a notice relating to a search service (or to the search engine of a combined service), the prevalence of search content of the service that is relevant content;

(f) the level of risk of harm to individuals in the United Kingdom presented by relevant content, and the severity of that harm;

(g) the systems and processes used by the service which are designed to identify and remove relevant content;

(h) the extent to which the use of the specified technology would or might result in interference with users' right to freedom of expression within the law;

(i) the level of risk of the use of the specified technology resulting in a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of the service (including, but not limited to, any such provision or rule concerning the processing of personal data);

(j) whether the use of any less intrusive measures than the specified technology would be likely to achieve a significant reduction in the amount of relevant content.

(3) The references to relevant content in subsection (2)(f), (g) and (j) are to—

(a) in the case of a user-to-user service (or the user-to-user part of a combined service), relevant content present on the service;

(b) in the case of a search service (or the search engine of a combined service), search content of the service that is relevant content.

(4) In this section— "relevant content" means terrorism content or CSEA content or both those kinds of content (depending on the kind, or kinds, of content in relation to which the specified technology is to operate);

"specified technology" means the technology to be specified in the notice under section 104(1).

Section 106 (9) and (10) of the Online Safety Bill

(9) For the purposes of section 10 4 and this section, technology is "accredited" if it is accredited (by OFCOM or another person appointed by OFCOM) as meeting minimum standards of accuracy in the detection of terrorism content or CSEA content (as the case may be).

(10) Those minimum standards of accuracy must be such standards as are for the time being approved and published by the Secretary of State, following advice from OFCOM.

Section 93 (4) of the Online Safety Bill

A person commits an offence if, in response to an information notice, the person—

> *(a) provides information which is encrypted such that it is not possible for OFCOM to understand it, or produces a document which is encrypted such that it is not possible for OFCOM to understand the information it contains, and*
>
> *(b) the person's intention was to prevent OFCOM from understanding such information.*

Section 8 (5) of the Online Safety Bill

An "illegal content risk assessment" of a service of a particular kind means an assessment of the following matters, taking into account the risk profile that relates to services of that kind—

> *(a) the user base;*
>
> *(b) the level of risk of individuals who are users of the service encountering the following by means of the service—*
>
> > *(i) each kind of priority illegal content (with each kind separately assessed), and*
> >
> > *(ii) other illegal content, taking into account (in particular) algorithms used by the service, and how easily, quickly and widely content may be disseminated by means of the service;*

EU Scanning Regulation

Article 7 (5) of the EU Scanning Regulation

(5) As regards detection orders concerning the dissemination of known child sexual abuse material, the significant risk referred to in paragraph 4, first subparagraph, point (a), shall be deemed to exist where the following conditions are met:

> *(a) it is likely, despite any mitigation measures that the provider may have taken or will take, that the service is used, to an appreciable extent for the dissemination of known child sexual abuse material;*
>
> *(b) there is evidence of the service, or of a comparable service if the service has not yet been offered in the Union at the date of the request for the issuance of the detection order, having been used in the past 12 months and to an appreciable extent for the dissemination of known child sexual abuse material.*

Article 10 (3) of the EU Scanning Regulation

(3) The technologies shall be:

> *(a) effective in detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;*
>
> *(b) not be able to extract any other information from the relevant communications than the information strictly necessary to detect, using the indicators referred to in paragraph 1, patterns pointing to the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;*
>
> *(c) in accordance with the state of the art in the industry and the least intrusive in terms of the impact on the users' rights to private and family life, including the confidentiality of communication, and to protection of personal data;*
>
> *(d) sufficiently reliable, in that they limit to the maximum extent possible the rate of errors regarding the detection.*

Article 49 (1) of the EU Scanning Regulation

(1) The EU Centre shall have the power to conduct searches on hosting services for the dissemination of publicly accessible child sexual abuse material, using the relevant indicators from the database of indicators referred to in Article 44(1), points (a) and (b), in the following situations:

(a) where so requested to support a victim by verifying whether the provider of hosting services removed or disabled access to one or more specific items of known child sexual abuse material depicting the victim, in accordance with Article 21(4), point (c);

(b) where so requested to assist a Coordinating Authority by verifying the possible need for the issuance of a detection order or a removal order in respect of a specific service or the effectiveness of a detection order or a removal order that the Coordinating Authority issued, in accordance with Article 25(7), points (c) and (d), respectively.

ENDNOTES

1. EARN IT Act of 2022, S.3538, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/senate-bill/3538.
2. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), https://publications.parliament.uk/pa/bills/cbill/58-03/0121/220121.pdf.
3. European Commission, "Laying down rules to prevent and combat child sexual abuse," May 11, 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en.
4. National Center for Missing and Exploited Children, "2021 CyberTipline Reports by Electronic Service Providers (ESP)," 2021, https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-esp.pdf.
5. Scott R. Ellis, "A Cryptography Primer," in *Computer and Information Security Handbook (Third Edition),* edited by John R. Vacca (Chicago: Morgan Kaufman Publishers), 35–58.
6. Dennis Luciano and Gordon Prichett, "Cryptology: From Caesar Ciphers to Public-key Cryptosystems," *The College Mathematics Journal,* Volume 18 (1987), https://www.tandfonline.com/doi/citedby/10.1080/07468342.1987.11973000?scroll=top&needAccess=true.
7. Joel Greenberg, "The Enigma machine," *The Turing Guide* (Oxford, 2017), https://doi.org/10.1093/oso/9780198747826.003.0018.
8. Seny Kamara et al., "Outside Looking In: Approaches to Content Moderation in End-to-End Encrypted Systems" (Center for Democracy and Technology, August 2021), https://arxiv.org/pdf/2202.04617.pdf.
9. "ITIF Technology Explainer: What Is Encryption?" (ITIF, March 2020), https://itif.org/publications/2020/03/06/itif-technology-explainer-what-encryption/.
10. Ibid.
11. Daniel Castro, "Why New Calls to Subvert Commercial Encryption Are Unjustified," (ITIF, July 13, 2020), https://itif.org/publications/2020/07/13/why-new-calls-subvert-commercial-encryption-are-unjustified/.
12. Proton Team, "What is end-to-end encryption and how does it work?" May 24, 2022, https://proton.me/blog/what-is-end-to-end-encryption.
13. "Why Wire?" Wire, accessed July 15, 2022, https://wire.com/en/; "Technical information: specifications and software libraries for developers," Signal, accessed July 15, 2022, https://signal.org/docs/; "About end-to-end encryption," WhatsApp Messenger, accessed July 15, 2022, https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=en.
14. "Password-protected Emails," Proton, accessed July 16, 2022, https://proton.me/support/password-protected-emails.
15. "End-to-end (E2EE) encryption for meetings," Zoom Support, July 20, 2022, https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings; Martin Hasal et al., "Chatbots: Security, privacy, data protection, and social aspects," *Concurrency*

Computation: Practice and Experience, May 10, 2021, https://onlinelibrary.wiley.com/doi/epdf/10.1002/cpe.6426.

16. Matthew Guariglia, Erica Portnoy, and Bill Budington, "Amazon Ring's End-to-End Encryption: What it Means," *EFF*, February 2, 2021, https://www.eff.org/deeplinks/2021/02/amazon-rings-end-end-encryption-what-it-means; "Ring: End-to-End Encryption," Ring LLC, July 13, 2021, https://assets.ctfassets.net/a3peezndovsu/5ihit68yvJLf0IJ2d0Hfu0/b9063f50382bbf3e143173bbf49e9781/Ring_Encryption_Whitepaper_2021-07-13.pdf.

17. Tom Warren, "Microsoft Teams is getting end-to-end encryption support," *The Verge,* March 2, 2021, https://www.theverge.com/2021/3/2/22308915/microsoft-teams-end-to-end-encryption-support-e2ee.

18. J.D. Tuccile, "Encryption Protects Ukrainians, Dissident Russians, and You," *Reason*, March 14, 2022, https://reason.com/2022/03/14/encryption-protects-ukrainians-dissident-russians-and-you/; Amelia Nierenberg, "Signal Downloads Are Way Up Since the Protests Began," *The New Your Times*, June 11, 2020, https://www.nytimes.com/2020/06/11/style/signal-messaging-app-encryption-protests.html; Michelle Siegel, "For LGBTQ Youth, Truly Equitable Internet Access Requires End-to-End Encryption," *New America*, January 28, 2022, https://www.newamerica.org/oti/blog/for-lgbtq-youth-truly-equitable-internet-access-requires-end-to-end-encryption/; Internet Society, "Fact Sheet: Understanding Encryption: The Connections to Survivor Safety," December 18, 2020, https://www.internetsociety.org/resources/doc/2020/understanding-encryption-the-connections-to-survivor-safety/.

19. Cat Zakrzewksi with Tonya Riley, "The Technology 202: Here's what app downloads reveal about technology's role in the protests," The Washington Post, June 5, 2020, https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/06/05/the-technology-202-here-s-what-app-downloads-reveal-about-technology-s-role-in-the-protests/5ed9541488e0fa32f8232b5c/.

20. "Advanced Modules on Digital Rights and Freedom of Expression Online: Trends in Censorship by Private Actors," Media Legal Defence Initiative, accessed August 2, 2022, https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/06/Module-5-Trends-in-censorship-by-private-actors.pdf.

21. Folkert Wilman, "The EU's system of knowledge-based liability for hosting providers in respect of illegal user content - between the e-Commerce Directive and the Digital Services Act," *Journal of Intellectual Property, Information Technology, and E-Commerce Law,* December 3, 2021, https://www.jipitec.eu/issues/jipitec-12-3-2021/5343; Ashley Johnson and Daniel Castro, "Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved (ITIF, February 2021), https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved/.

22. David Banisar and Simon Davies, "Privacy and Human Rights: An International Survey of Privacy Laws and Practice," *Global Internet Liberty*

Campaign, accessed July 20, 2022, http://gilc.org/privacy/survey/intro.html.

23. Daniel Kardefelt-Winther et al., "Encryption, Privacy and Children's Right to Protection from Harm" (UNICEF Office of Research - Innocenti, October 2020), https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf.

24. Christopher Wray, "Statement Before the Senate Judiciary Committee: Oversight of the Federal Bureau of Investigation: The January 6 Insurrection, Domestic Terrorism, and Other Threats," *Federal Bureau of Investigation,* March 2, 2021, https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-the-january-6-insurrection-domestic-terrorism-and-other-threats; Courtney Linder, "The NSA Wants Big Tech to Build Software 'Back Doors.' Should We Be Worried?" *Popular Mechanics*, June 21, 2021, https://www.popularmechanics.com/technology/security/a34533340/nsa-tech-back-doors-software/; Russell Brandom, "US joins six countries in new call for backdoor encryption access," *The Verge*, October 12, 2020, https://www.theverge.com/2020/10/12/21513212/backdoor-encryption-access-us-canada-australia-new-zealand-uk-india-japan; Edward Snowden, "Without encryption, we will lose all privacy. This is our new battleground," *The Guardian*, October 15, 2019, https://www.theguardian.com/commentisfree/2019/oct/15/encryption-lose-privacy-us-uk-australia-facebook.

25. Tony Wu et al., "The ethics (or not) of massive government surveillance," Stanford University, accessed July 20, 2022, https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/tech_encryptionbackdoors.html.

26. Herb Lin, "'Back Doors for Good Guys Means Back Doors for Bad Guys—'--Unpacking Another Claim," *Lawfare,* December 22, 2015, https://www.lawfareblog.com/back-doors-good-guys-means-back-doors-bad-guys-unpacking-another-claim.

27. Robert Endeley, "Who Needs and Encryption Backdoor: Why Americans want Security over Privacy," *American Journal of Science and Engineering,* Volume 1, Issue 2 (2020), https://ajse.us/wp-content/uploads/2022/02/ajse_v1_is2-19-26.pdf.

28. Nick Sullivan, "How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer," The Cloudflare Blog, June 1, 2014, https://blog.cloudflare.com/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/.

29. Nicole Perloth, "Government Announces Steps to Restore Confidence on Encryption Standards," The New York Times, September 10, 2013, https://archive.nytimes.com/bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/.

30. National Institute of Standards and Technology, "Glossary: key escrow system," Computer Security Resource Center, accessed September 7, 2022, https://csrc.nist.gov/glossary/term/key_escrow_system.

31. Simson Garfinkel, "In praise of the Feistel network," *MIT Technology Review,* April 27, 2022, https://www.technologyreview.com/2022/04/27/1048456/in-praise-of-

the-feistel-network/; National Institute of Standards and Technology, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," *Federal Information Processing Standards Publication 197,* November 26, 2001, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

32. Dennis Fisher, "KEY ESCROW BY ANY OTHER NAME IS STILL KEY ESCROW," Decipher, April 27, 2018, https://duo.com/decipher/key-escrow-by-any-other-name-is-still-key-escrow.
33. Erica Portnoy, "Why Adding Client-Side Scanning Breaks End-To-End Encryption," Electronic Frontier Foundation, November 11, 2019, https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption.
34. "A Civil Society Glossary and Primer for End-to-End Encryption Policy in 2022," Alec Muffett, July 7, 2022, https://alecmuffett.com/alecm/e2e-primer/e2e-primer-web.html#e2e-and-intra-application-client-side-scanning.
35. "Fact Sheet: Client Side Scanning—What It Is and Why It Threatens Trustworthy, Private Communications," Internet Society, March 24, 2020, https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/.
36. EARN IT Act of 2022, S.3538, 117th Cong. (2022).
37. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023).
38. "Laying down rules to prevent and combat child sexual abuse," European Commission, May 11, 2022.
39. EARN IT Act of 2022, S.3538, 117th Cong. (2022).
40. EARN IT Act of 2020, S.3398, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3398/text.
41. EARN IT Act of 2022, S.3538, 117th Cong. (2022), Sections 1 and 5.
42. Ashley Johnson and Daniel Castro, "Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved (ITIF, February 2021), https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved/.
43. 47 U.S.C. § 230(e) (1996), https://www.law.cornell.edu/uscode/text/47/230.
44. 47 U.S.C. § 230(c)(2) (1996).
45. Riana Pfefferkorn, "The EARN IT Act Is Back, and It's More Dangerous Than Ever," The Center for Internet and Society at Stanford Law School, February 4, 2022.
46. EARN IT Act of 2022, S.3538, 117th Cong. (2022), Section 5(6).
47. EARN IT Act of 2022, S.3538, 117th Cong. (2022), Section 5.
48. Ibid.
49. Jeffrey Westling, "Unintended Consequences of the EARN IT Act," *American Action Forum*, February 23, 2022, https://www.americanactionforum.org/insight/unintended-consequences-of-the-earn-it-act/.
50. Kir Nuthi, "The EARN IT Act Would Give Criminal Defendants a Get-Out-of-Jail-Free Card," *Slate*, February 11, 2022,

https://slate.com/technology/2022/02/earn-it-act-fourth-amendment-violation.html.

51. Ibid.

52. EARN IT Act of 2022, S.3538, 117th Cong. (2022), Section 5(7).

53. Virginia Bruner and V. Kathleen Dougherty, "EARN IT Act Opens Online Service Providers to Liability for Online Child Sexual Abuse Hosted on Their Platforms," JD Supra, February 17, 2022, https://www.jdsupra.com/legalnews/earn-it-act-opens-online-service-3498087/

54. Invest in Child Safety Act, S.223, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/223/text.

55. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023).

56. European Parliament and European Council, "Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')," June 8, 2000, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031.

57. European Parliament and European Council, Directive on electronic commerce, Article 14.

58. "Online Harms White Paper," Department for Digital, Culture, Media & Sport and Home Office, April 8, 2019, https://www.gov.uk/government/consultations/online-harms-white-paper.

59. Online Safety Bill Draft, Bill CP 405, House of Commons (Session 2021–2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.

60. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), https://publications.parliament.uk/pa/bills/cbill/58-03/0121/220121.pdf.

61. Ibid., Section 3. Online Safety Bill, Bill 121, House of Commons (Sessions 2021-22, 2022-23), Section 34.

62. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Section 67(4).

63. Nicolas Wellmann, "OTT-Messaging and Mobile Telecommunication: A Joint Market? – An Empirical Approach" (Düsseldorf Institute for Competition Economics, July 2017), https://www.econstor.eu/bitstream/10419/162779/1/893137103.pdf.

64. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Section 9.

65. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Section 117.

66. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Sections 9 and 104.

67. "45 organizations and cyber security experts sign open letter expressing concerns with UK's Online Safety Bill," Global Encryption Coalition, April

14, 2022, https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill/.

68. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Section 8.

69. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Section 104(2).

70. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Section 105.

71. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Section 93; Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Schedules 12 and 13.

72. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Section 93(4).

73. Ibid.

74. Online Safety Bill, Bill 121, House of Commons (Sessions 2021–2022, 2022–2023), Schedule 13.

75. Shiona McCallum, "WhatsApp: We won't lower security for any government," *BBC*, July 30, 2022, https://www.bbc.co.uk/news/technology-62291328.

76. "Fighting child sexual abuse: Commission proposes new rules to protect children," European Commission, May 11, 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2976.

77. "REGULATION (EU) 2022/OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC," European Parliament and Council of the European Union, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

78. "Digital Services: landmark rules adopted for a safer, open online environment," European Parliament, July 5, 2022, https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment.

79. Ibid.

80. "Digital Services Act: Decision In Part Strengthens, In Part Threatens Privacy Safety, and Free Speech Online," European Pirate Party, January 20, 2022, https://european-pirateparty.eu/eu-parliament-adopts-dsa-position/; "EU's political deal on the Digital Services Act step in the right direction, but some questions remain," Access Now, April 26, 2022, https://www.accessnow.org/political-deal-digital-services-act/.

81. "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: EU strategy for a more effective fight against child sexual abuse," European Commission, July 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0607&from=EN.

82. "EU strategy for a more effective fight against child sexual abuse," European Commission, July 24, 2020.

83. "Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA," European Parliament and the Council of the European Union, December 13, 2011, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093.

84. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," European Parliament and the Council of the European Union, July 12, 2022, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

85. Maria Koomen, "The Encryption Debate in the European Union: 2021 Update," *Carnegie Endowment for International Peace,* March 31, 2021, https://carnegieendowment.org/2021/03/31/encryption-debate-in-european-union-2021-update-pub-84217.

86. "Laying down rules to prevent and combat child sexual abuse," European Commission, Article 1.

87. Ibid.

88. "EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse," European Data Protection Board and European Data Protection Supervisor, adopted July 28, 2022, https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf.

89. European Commission, "Laying down rules to prevent and combat child sexual abuse," Article 3.

90. Ibid.

91. European Commission, "Laying down rules to prevent and combat child sexual abuse," Article 3.

92. European Commission, "Laying down rules to prevent and combat child sexual abuse," Article 4.

93. European Commission, "Laying down rules to prevent and combat child sexual abuse," Article 7.

94. European Commission, "Laying down rules to prevent and combat child sexual abuse," Article 10.

95. European Commission, "Laying down rules to prevent and combat child sexual abuse," Article 10.

96. European Commission, "Laying down rules to prevent and combat child sexual abuse," Article 49.

97. "Briefing on Key Concerns Relating to a Proposal for Regulation laying down the Rules to Prevent and Combat Child Sexual Abuse (CSAM)" (Center for Democracy and Technology, June 2020), https://cdt.org/wp-content/uploads/2022/06/CDT-Europe-Briefing-on-Key-Issues-in-CSAM-Proposal.pdf.

98. “EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse,” European Data Protection Board and European Data Protection Supervisor, adopted July 28, 2022.

ABOUT THE AUTHOR

Kir Nuthi is a senior policy analyst at the Center for Data Innovation focusing on European digital policy. Previously, she worked as a public affairs manager at NetChoice, where she focused on emerging technology issues surrounding content moderation, competition policy, and the sharing economy. Kir holds an MSc in International Public Policy from University College London and a BA with dual focuses in Economics and Political Science from the University of California San Diego.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation is the leading global think tank studying the intersection of data, technology, and public policy. With staff in Washington, London, and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the nonprofit, nonpartisan Information Technology and Innovation Foundation (ITIF).

contact: info@datainnovation.org

datainnovation.org