Internet Impact Brief

European Commission Proposal to Prevent and Combat Child Sexual Abuse

Callum Vogue, Internet Society
August 2022

Abstract

On 11 May 2022, the European Commission published a proposal for a regulation laying down rules to prevent and combat child sexual abuse (CSA Proposal). This proposal seeks to increase child safety online by imposing new obligations on online communication services providers, including an obligation to screen private communications to detect instances of child sexual abuse.

The draft CSA Proposal states that it is compatible with end-to-end encryption. However, no technical solutions currently exist that would allow providers to offer their users end-to-end encrypted services while still complying with their detection obligations under the proposal. As a result, the CSA Proposal pressures providers into either removing encryption entirely or offering a weakened version of encryption.

While the law enforcement goals that drive the CSA Proposal are legitimate and welcomed, the loss or weakening of secure communication technologies like end-to-end encryption creates new vulnerabilities that put European Internet users, including children, at risk. These risks not only include harm to individuals but also the erosion of trust in the Internet, threatening to derail Europe's ambitions for a Digital Decade.

This Internet Impact Brief illustrates how limitations on encryption arising from the CSA Proposal would move the Internet further from its potential as an *open, globally connected, secure,* and *trustworthy* resource for all.

Methodology

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

In order to assess whether the proposed actions have an impact on the Internet, this report will examine their impact on the IWN foundation the Internet needs to thrive as an open, globally connected, secure and trustworthy resource.

Context

The European Commission's CSA Proposal was published on 11 May 2022. This proposal seeks to create a legal framework to better prevent and combat child sexual abuse both offline and online. It builds upon and operationalizes the 2021 EU Strategy on the Rights of the Child, which introduced a high-level set of measures to promote and protect children's rights.

The CSA Proposal seeks to tackle child sexual abuse online by, among other things, setting new obligations for the "providers of hosting or interpersonal communication services". These include an obligation for providers to evaluate the risk of their service being used for child sexual abuse. Based on the outcome of a risk assessment, they will face additional detection obligations to identify child sexual abuse material (CSAM) on their platforms.

Providers are encouraged to detect CSAM on their platforms voluntarily but can be legally obliged to, through a detection order. Once an order is issued, providers are obligated to use "reliable detection technologies" to identify CSAM on their service. If CSAM is detected, they face further obligations to report, remove, and block the content. Providers that proactively discover CSAM on their services, before receiving a detection order, are also legally obligated to report their findings.[1] Companies that fail to follow these obligations would face penalties of up to 6% of their annual income or global turnover of the preceding business year.

The CSA Proposal additionally establishes a "European Centre to prevent and counter child sexual abuse" (the EU Centre) to create, maintain, and operate databases of indicators of CSAM that providers will need to use to comply with their detection obligations. The center is also encouraged to make detection technologies available to providers free of charge so that they have the option of using them when they receive a detection order. At the same time, the CSA Proposal emphasizes its technology-neutral approach and states that the endorsement of certain detection technologies by the EU Centre should not be seen as "incentivizing or disincentivizing the use of any given technology [including] the use of end-to-end encryption".[2]

The CSA Proposal states that it is technology-neutral and that it is compatible with end-to-end encryption. However, no technical solutions currently exist that would allow providers to offer their users end-to-end encrypted services while still complying with their detection obligations under the

[1] Article 12: Reporting Obligations. Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

[2] Recital 26. Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

CC BY-NC-SA 4.0

proposal.[3] In this sense, **the CSA Proposal pushes providers to either remove end-to-end encryption entirely or to offer a weakened version of encryption.**

Some European policymakers have pointed to encryption backdoors[4] and client-side scanning as possible detection technologies in the fight against CSAM.[5] End-to-end encryption means that decrypted data can only be seen and read by the two endpoints in a conversation: the sender and the intended recipient. Encryption backdoors that grant law enforcement or the provider exceptional access to decrypted messages therefore break end-to-end encryption's most basic principle. While the creation of backdoors do grant law enforcement access, it also creates an engineered vulnerability that can be exploited by criminals and hostile state actors, putting Internet users at risk.

Similarly, client-side scanning technologies have the effect of breaking end-to-end encryption by scanning messages on users' end devices before they are encrypted and sent.[6] Like with backdoors, client-side scanning also creates new vulnerabilities for criminals and hostile state actors to take advantage of. This can be done by manipulating the database of indicators to enable social engineering attacks, extortion, or blackmail.[7] Together, the weaknesses that arise from encryption backdoors and client-side scanning reduce encryption's value as a tool to guarantee security and confidentiality for Internet users, including children.

The European Data Protection Supervisor (EDPS) has recognized encryption as a main tool to guarantee the security of our information and as a necessary enabler of the digital economy and the protection of fundamental rights, including privacy and free speech. Importantly, the EDPS states that:

> "While law enforcement requires the means to fight crime on the internet, any new measure would have to first pass the test for necessity and proportionality, based on substantiated evidence. While encryption makes bulk data collection and mass surveillance difficult, it is not a limiting factor in more targeted and specific

[3] https://www.globalencryption.org/2020/11/breaking-encryption-myths/

[4] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption

[5] https://xnet-x.net/img/20201020-EDRi-Open-letter-CSAM-and-encryption-FINAL.pdf

[6] https://www.patrick-breyer.de/en/posts/messaging-and-chat-control/

[7] https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/

CC BY-NC-SA 4.0

measures. Restrictions on encryption pose significant risks to the economy and society in general."[8]

This Internet Impact Brief, based on IWN model methodology, examines how the CSA Proposal, and particularly the limitations it would place on the use of end-to-end encryption, would impact the open, globally connected, secure and trustworthy Internet.

How Does CSA Proposal Affect the Realization of the Full Potential of the Internet?

Goal	Enabler	Impact
Open Internet	Easy and unrestricted access	Providers will face the impossible task of creating safe and secure encryption backdoors. The development of backdoors in otherwise secure systems will be expensive and technically challenging, raising the costs of the resulting products and services. The safe operation of these compromised systems will also introduce new costs and procedural difficulties, which are likely beyond the capability of all but the largest providers. This creates a barrier for new providers hoping to enter the market and cements the dominance of existing large providers.
	Unrestricted use and deployment of Internet technologies	Innovators will be limited in how they can use end-to-end encryption in new technologies to create new products, hurting European innovation. Although not the intention, providers may also feel pressured to use detection technologies provided by the EU Centre, even if more efficient and secure

[8] https://edps.europa.eu/data-protection/our-work/subjects/encryption_en

CC BY-NC-SA 4.0

		alternatives for addressing the provider's specific goals exist.
	Collaborative development, management, and governance	Detection technologies provided by the EU Centre may unintentionally put pressures on providers to use technologies that have not necessarily gone through a collaborative process of development, management, and governance.
Globally Connected Internet	Unrestricted reachability	European Internet users may be excluded from global resources that are end-to-end encrypted, especially if global providers leave the European market to remain out of the scope of the CSA Proposal. Likewise, Internet users may decrease their activity online if the lack of strong encryption is seen as a threat to their privacy. These actions would reduce the flow of information and resulting opportunities for collaboration, innovation, and business.
	Available capacity	No significant impact identified.
Secure Internet	Data confidentiality of information, devices, and applications	Weakened encryption would put data confidentiality at risk as law enforcement backdoors create weaknesses that can also be exploited by criminals and hostile state actors. European Internet users have legitimate reasons for ensuring their privacy. This is especially true for certain professions such as journalists[9], civil servants, advocacy groups[10], and doctors. It is also the case for vulnerable communities including the LGBTQ+ community[11], abuse survivors, and minority groups. Research has also shown that laws that weaken

[9] https://www.internetsociety.org/resources/doc/2020/fact-sheet-how-encryption-can-protect-journalists-and-the-free-press/

[10] https://www.internetsociety.org/resources/doc/2021/factsheet-how-encryption-can-protect-advocacy-groups-and-social-changemovements/

[11] https://www.internetsociety.org/resources/doc/2019/encryption-factsheet-essential-for-lgbtq-community/

CC BY-NC-SA 4.0

		encryption fuel business uncertainty and can result in economic harm.[12] Even if exemptions for strong encryption are created for certain use cases, recent history shows examples of flawed implementation where weakened encryption protocols unintentionally found their way into vital national infrastructure and were exploited by foreign governments.[13]
	Integrity of information, applications, and services	Weakened encryption puts sensitive information at risk of malicious attack by criminals and hostile state actors. Machine-in-the-Middle (MiTM) attacks could see trade secrets and national security information manipulated. Attempts to make exemptions that allow certain industries to retain strong encryption may prove difficult as businesses may use weakened encryption protocols in their supply chain if these options are more readily available or affordable.
Trustworthy Internet	Reliability, resilience, and availability	Internet users that use end-to-end-encrypted services expect that their communications are private and anonymized. Internet users that use weakened encryption will experience a disconnect when their expectations are not met, resulting in reduced trust in the Internet.
	Accountability	The CSA Proposal explains the process for the issuance of a detection order but does provide sufficient detail to assess whether that process is proportionate or operationally practical. For example, it states that the EU Centre should "limit [personal data] storage to what is strictly necessary

[12] https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/

[13] https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/

CC BY-NC-SA 4.0

		for the performance of the relevant tasks" but does not provide criteria for the type or volume of data to be shared with law enforcement. Additionally, providers that have received detection orders will be required to scan all communications and, to avoid liability, would likely err on the side of caution by over-reporting people's communications.[14] Without proper accountability functions for data usage and over-reporting, the CSA Proposal may reduce accountability on the Internet, decreasing its trustworthiness. While the CSA Proposal does acknowledge these risks, successful implementation of and public awareness of accountability functions will be essential for retaining trust.
	Privacy	The CSA Proposal states that the "least privacy-intrusive" detection technologies should be used. Yet, weakened encryption harms privacy by reducing the ability of Internet users to control the movement of their data and creates doubts as to who can access, share, and store their data. Without strong encryption, even the most stringent data laws will be unable to protect private data from criminals and third parties who exploit weaknesses. Loss of privacy has real world ramifications, including for children. Loss of privacy can harm the safety of children as predators may more easily obtain sensitive information for grooming purposes.[15]

[14] https://www.politico.eu/article/europe-online-child-abuse-law-make-us-less-safe/

[15] https://www.theguardian.com/technology/2022/jan/21/end-to-end-encryption-protects-children-says-uk-information-watchdog

CC BY-NC-SA 4.0

Summary and Conclusions

Proposals that work to protect children from sexual abuse online are important and welcomed but should not resort to the removal or weakening of key security technologies to accomplish their goals. Doing so creates weaknesses that can be exploited by criminals and hostile state actors and creates new risks for all Internet users, including children.

This Internet Impact Brief has found that restrictions on end-to-end encryption brought about by detection orders under the CSA Proposal would negatively impact all four of the qualities that maximize the Internet's potential as a resource for good: *open, globally connected, secure,* and *trustworthy.*

This impact on the Internet will have negative consequences for European businesses, Internet users, vulnerable communities, and the reputation of the European Union as a protector of fundamental rights. While the CSA Proposal seeks to increase safety on the Internet, this report demonstrates how the dismantling of strong encryption will expose Internet users, including children, to new arrays of harm.

This Internet Impact brief offers three recommendations:

1. That the CSA Proposal is redrafted so that is **compatible with end-to-end encryption**, recognizing the value of **strong encryption** in moving the Internet closer to its full potential as an open, globally connected, secure, and trustworthy resource.
2. That the **EU Centre dismisses encryption backdoors and client-side scanning** as detection technologies due to the security risks and harm to the Internet associated with these approaches. This includes harm to easy and unrestricted access; data confidentiality of information, devices, and applications; integrity of information, applications, and services; reliability, resilience, and availability; and privacy.
3. That the **upcoming Impact Assessment includes Internet impact** in its analysis to sufficiently identify the potential positive and negative impacts of the CSA Proposal on the Internet. We welcome the use of the Internet Impact Brief provided here for this purpose.

CC BY-NC-SA 4.0