Joint submission from Global Encryption Coalition Members to the European Commission Public Consultation - Fighting child sexual abuse: detection, removal and reporting of illegal content online

The undersigned members of the Global Encryption Coalition,[1] and organisations and technical experts concerned with communications security, welcome the opportunity to submit this written response to the European Commission's Public Consultation on Fighting child sexual abuse: detection, removal and reporting of illegal content online.[2]

We fully support the Commission's goals of ensuring the safety of children and the importance of finding successful ways to fight child sexual abuse. As a society we must remain vigilant, and we must collaborate to strengthen existing approaches and to identify new and innovative ones to keep children safe from exploitation. Education regarding how to use and navigate the online world is paramount, especially for children. Education and skills development are areas we hope the Commission will emphasize in fighting the sexual exploitation and abuse of children both online and offline.

We are concerned that the monitoring requirements proposed in two of the policy options outlined in the related Inception Impact Assessment (Options 2 & 3) published in December 2020 would have unintended consequences for encryption, and therefore the security and privacy of all EU citizens, including the children that the policy intends to protect.

However, Policy Option 1, which appears to aim to establish a clear legal framework for the voluntary detection, reporting and removal of child sexual abuse could help encourage stakeholders to implement these voluntary measures where technically possible.

The European Union Relies on Encryption

Encryption is essential for securing the personal safety of the European Union's citizens and businesses as well as the national and regional security of its member states and institutions.

On a daily basis, and especially in this pandemic period, EU citizens rely on the Internet to telework, engage in online schooling, consult with health professionals, pay their bills, and communicate with friends and family. People living and working in Europe depend on encryption to keep these activities safe. In particular, end-to-end encryption, which is widely recognized as the gold-standard for securing digital communications, helps ensure that sensitive, confidential information remains confidential and out of the hands of criminals and other bad actors.

In addition to general security, end-to-end encryption is particularly vital for the personal security of members of at-risk groups, including children. Journalists rely on end-to-end encryption to protect the identities and safety of confidential sources.[3] Members of the LGBTQ+ community depend on end-to-

[1] The Global Encryption Coalition is a group of national coalitions, civil society groups, companies, academics, and technologists dedicated to promoting and defending the use of strong encryption around the world. Founded in 2020, the Coalition has grown to over 120 members and also supports efforts to implement encrypted services. https://www.globalencryption.org/

[2] 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/public-consultation

[3] https://cpj.org/2020/03/cpj-internet-society-journalist-encryption-fact/

end encryption to help ensure their privacy and safety as they navigate coming out.[4] Domestic violence survivors rely on end-to-end communication tools to provide a secure channel for a survivor to make plans and communicate with trusted individuals.[5]

Businesses rely on encryption to securely deliver services, accept payments, protect their customers' data, commercial assets, and internal communications. European businesses depend on strong encryption to manage the data of EU citizens in a compliant and safe manner, and end-to-end encryption is crucial to "a growing European technology sector."[6]

Encryption helps prevent spies, criminals, and hostile governments from accessing and exploiting confidential communications of government officials, and from penetrating computer systems and databases and causing wide-scale, systemic disruptions to economies, infrastructure, and security.

Parents rely on end-to-end encryption to protect themselves and their families. Adults make decisions about how to help their children stay safe online by choosing methods of communication that keep their child's personal information most protected. In end-to-end encrypted messaging apps, closed group membership keeps strangers out and encrypted group chats keep strangers from snooping on children's conversations. End-to-end encrypted conversations keep personal information away from criminals seeking to use social engineering techniques to interact with potential victims. Hidden profiles keep strangers from locating potential targets who are children. Strong passwords and two-factor authentication help keep strangers from breaking in.

End-to-end encryption protects children; weakening encryption threatens them.

Mandatory Content Monitoring and Unintended Consequences for Encryption

The related Inception Impact Assessment offers three legislative options to address child sexual abuse and improve identification and protection of victims of child sexual abuse. All three legislative options reference "measures for the detection, reporting and removal of child sexual abuse on their services." However, only policy options 2 and 3 take the dangerous step of requiring the use of these measures. Policy Option 2 requires the detection, reporting and removal of known child sexual abuse material, while Policy Option 3 requires the detection, reporting and removal of *both known and unknown* child sexual abuse material, including grooming.

If the mandatory detection, reporting, and removal requirements in policy options 2 and 3 are intended to apply to end-to-end encrypted communications, then regardless of whether the unlawful content is known, platforms would be forced to undermine end-to-end encryption. The consensus among cybersecurity experts is clear: **there is no way to enable a third party to monitor users' end-to-end encrypted communications without weakening the security and privacy for all of its users.**

In September 2020, a draft European Commission report called "Technical solutions to detect child sexual abuse in end-to-end encrypted communications" was leaked which highlighted different methods that were being considered to detect unlawful online content. An in-depth assessment by more than

---

[4] https://www.lgbttech.org/post/2019/11/22/lgbt-tech-release-encryption-one-sheet

[5] https://www.internetsociety.org/wp-content/uploads/2020/12/NNEDV_Survivor_FactSheet-EN.pdf

[6] https://techcrunch.com/2021/01/27/protonmail-threema-tresorit-and-tutanota-warn-eu-lawmakers-against-anti-encryption-push/

fifty global and European cybersecurity experts found that every detection method outlined in the leaked report would break end-to-end encryption and weaken the security and privacy of all users.[7] Whether a traditional encryption backdoor, like a key escrow system, or a newer concept like "client-side scanning," these methods create security risks and would present an attractive target for criminals. For instance, compromised key escrow systems can provide criminals with access to all user communications.[8] Criminals with access to a client-side scanning system could manipulate its database to track how specific content is being sent, when, where and to whom it is sent, undermining the confidentiality of the communication.[9]

While mandated encryption backdoors create vulnerabilities in users' end-to-end communications, their utility is unclear. Sophisticated criminals will switch away from services known or suspected to be complying with detection, reporting and removal requirements to end-to-end encrypted communications services existing outside the European Union's jurisdiction. Even if they continue to use services that comply with such requirements, criminals can implement their own encryption on top (or instead of) the services that would be impacted by the legislation. Thus, such requirements may have the unintended consequence of weakening the security and privacy of average users while failing in their original goal of improving identification and protection of victims of child sexual abuse.
The detection requirements proposed in policy options 2 and 3 would force companies to undermine the use of end-to-end encryption, putting all the service's users, including children, at greater risk of harm.

Conclusion
As the European Union explores policy options to address child sexual abuse and improve identification and protection of victims of child sexual abuse, it must not weaken the security and privacy of European citizens, businesses, member states and its institutions in the process. The European Commission must not hinder the implementation and use of end-to-end encryption, nor should it weaken it. Any measures to address child exploitation which are proposed must protect the security and integrity of networks and digital technologies and human rights. The technical measures currently proposed do not, and therefore risk doing more harm than good.

Signatories

Civil Society

Article 19

Association for Proper Internet Governance

Centre for Democracy & Technology

---

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

[8] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., ... & Weitzner, D. J. (2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, *1*(1), 69-79.

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

Derechos Digitales

Fundación Cibervoluntarios

Global Partners Digital

IBIDEM – Instituto Beta: Internet & Democracia

Internet Society

Internet Users Forever society iki.fi

IP.rec

ISOC Brazil - Brazil Chapter of the Internet Society

New America's Open Technology Institute

OpenMedia

Privacy International

Prostasia Foundation

The Tor Project

Companies

Nym Technologies SA

Ohmtel Ltda

ProtonMail & ProtonVPN

Surfshark

Tresorit

Tutanota

Trade Associations

eco - Association of the Internet Industry

Security Experts*

Claudia Diaz, Professor, KU Leuven

Sven Dietrich, Professor of Computer Science, City University of New York

Jens Finkhaeuser, Interpeer Project

Prof. Ian Goldberg, University of Waterloo

Dr. Sven Herpig, Director for Cybersecurity Policy, Stiftung Neue Verantwortung e. V.

Adam Shostack, Author: Threat Modeling: Designing for Security

*Affiliations listed for identification purposes only