Internet Society submission to the European Commission Inception Impact Assessment - Regulation of the European Parliament and of the Council on the detection, removal and reporting of child sexual abuse online, and establishing the EU centre to prevent and counter child sexual abuse

The Internet Society as a stakeholder

The Internet Society is a global non-profit organization founded in 1992 by some of the Internet's early pioneers. Our global community is made up of thousands of energetic, enthusiastic, and committed individuals, organizations, and volunteers. We believe the Internet is a force for good and we are working towards an open, globally connected, secure and trustworthy Internet. We believe everyone should benefit from an open and trusted Internet. These beliefs form the pillars of our work.

The policy context

First and foremost, the Internet Society stresses the significance of child safety and strongly supports efforts to find successful ways to fight sexual abuse. As a society we must remain vigilant, and we must collaborate to strengthen existing approaches and identify new and innovative methods to deal with the abuse of children, both offline and online. Encryption is one such way and it is an indispensable tool in protecting children and ensuring their safety.

We welcome the work done to draft the Commission's July 2020 strategy about the state of play in addressing child sexual abuse online, and in particular its recognition that this is fundamentally a societal problem requiring multiple types of intervention, across multiple disciplines and reflecting the roles of multiple stakeholders[1]. We feel it important to note that industry quickly implements voluntary measures and collaborates with law enforcement to remove content swiftly.[2] We appreciate that the efforts made by industry may not be enough to address the issue, but they should not be underestimated for their contribution either.

Voluntary mechanisms, such as hotlines, as currently deployed by various technology companies, are more adaptable and responsive especially to emerging and new security and safety threats. Given how fast-paced technology is, any top-down prescriptive effort could prove to be counterproductive or be significantly detached from how technology evolves. In moving forward to find workable solutions, collaboration and knowledge exchange between interested actors will be key.

---

[1] "The fight against child sexual abuse needs to be fought on many fronts, including by society at large. Real progress can only be made when work is stepped up in relation to prevention, reporting, referral, investigation, protection and identification, treatment and follow-up of each and every case. Social services, health-care professionals, academics, researchers, educators, the judiciary, law enforcement, children, families, NGOs, media and broader society each have a role to play, in a true multi-stakeholder, multi-disciplinary approach." -- https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf

[2] Feedback from: .eco – Association of the Internet Industry on "Fighting child sexual abuse: detection, removal, and reporting of illegal content online", 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/F1385071

The (technical) context

In this submission, our focus is on encryption. Encryption is a critical component of our day-to-day security in the physical realm as well as the digital. It helps secure critical national infrastructure, such as electricity, transport and financial transactions. It keeps citizens' most vulnerable data, such as financial and health information, away from criminals and terrorists. It is also vital for ensuring the confidentiality of law enforcement communication, and civil authorities' ability to provide public services.

For the individual citizen, encryption is not just a matter of privacy or confidential messaging: increasingly, with connected vehicles, medical devices and home security systems, encryption protects the physical safety of individuals and their family.

In terms of online security and privacy, encryption is indispensable in protecting citizens against Internet-based crime such as identity theft. End-to-end encryption, which secures data all the way from its sender to its recipient, even if it must unavoidably be handled by third parties on the way, can ensure that sensitive information transmitted by billions of people online remains confidential and out of the hands of criminals, safeguarding day-to-day activities such as online banking and shopping, among others. It protects individuals' private and sensitive communications and offers a confidential helpline to those most at risk – helping vulnerable individuals get secure access to guidance, support and help.

Guiding principles

Effectiveness

Several approaches have been suggested to support law enforcement access in an environment where data may be encrypted - measures such as key escrow, adding ghost users, client-side scanning, traceability and other methods to weaken end-to-end encryption. The technical consensus is clear: "Strong cryptography, and in particular encryption, are key enablers of many services that are seen as essential in a modern, interconnected society. Strong encryption not only enables secure communication between individuals, public services, and companies, but also

- facilitates, e.g., investigative journalism,
- shelters whistleblowers,
- protects fundamental rights such as freedom of speech,
- safeguards critical infrastructures such as banks,
- supports military communication, and
- contributes to physical safety, e.g., in autonomous driving."[3]

Any measures that undermine encryption put us all at greater risk from those who would do us harm, including criminals and terrorists.

[3] https://sites.google.com/view/scientists4crypto/start

It is also questionable whether weakening security for the law-abiding majority prevents criminal behaviour. There is no evidence that establishing “exceptional access” to encrypted communications would stop criminals from finding ways to communicate secretly.

We believe that the Commission must be able to demonstrate that any proposal would not create vulnerabilities in the encrypted service or device which could be exploited by criminals. To this end, the Commission carries the burden of proving not only that appropriate checks and balances are in place, but also that they would actually preserve encryption's ability to protect law-abiding citizens.

This approach would also ensure that the rule of law and the right to privacy are not violated, which would minimize the risk of such measures subsequently being challenged before the courts.

Privacy

Weakening encryption through exceptional access would pose legal challenges with regard to the rule of law and the right to privacy.

In today’s Internet environment, privacy and encryption are inseparable[4]. Historically, Europe has been strong in setting and defending the rules for privacy and data protection. Two years ago, it took a huge leap when it established the General Data Protection Regulation (GDPR), a celebration of individuals' rights relating to data about them. Attempts to undermine encryption undermine privacy, and this strikes at the heart of Europe’s historical support for strong privacy protection, which have been also included in its digital agenda.

Proportionality and stakeholder interests

As a law enforcement measure, access to encrypted data or communications without consent must satisfy the criteria of necessity and proportionality, both of which constitute fundamental legal principles in Europe. However, any approach that would weaken the security and privacy of all users would fail to satisfy such criteria.

Weakening encryption by creating “backdoor access” to prevent crime, is like trying to solve one problem by creating 1,000 more —and it establishes a dangerous precedent that could weaken encryption globally and make it virtually impossible to ensure the personal security of billions of people and the national security of countries around the world.

From the outset (Question 1) the consultation is based on the presumption that there are gaps in the range of preventive measures, that something must be done, and that encryption is an obstacle to something being done (with the implication that encryption must therefore be counteracted). Without debating whether or not those starting assumptions are true, they nevertheless frame the problem a way that pre-judges the "correct" answer and will fail to capture the full range of legitimate stakeholder views.

---

[4] https://edri.org/our-work/why-weak-encryption-is-everybodys-problem/

A policy that is based, from the start, on an incomplete and pre-judged set of stakeholder views cannot be proportionate, since it will fail to account for the full range of stakeholder rights and interests. As a result, this consultation is unlikely to be based on a complete risk assessment of the measures it is designed to support – particularly with regard to the rights and interests of law-abiding citizens and businesses, who have a legitimate need to maintain their confidentiality and security in the digital domain.

Economic impact

Additionally, the economic impact of the proposal is also a significant consideration. Research from the OECD[5] and elsewhere, including the Commission's own strategic initiatives[6], highlights the economic importance of trust in the digital domain. Measures that undermine encryption technology undermine trust, and this is likely to have a negative economic impact.

For example, if digital security products developed or deployed in the EU are known to have law-enforcement access measures built in, they will not be trusted. If companies developing such products in the EU are obliged to collaborate with security and surveillance agencies, their products and services will not be trusted. This will have a negative economic impact on the internal market (for example, for hosted services) as well as on the EU's ability to export secure technology products. It is also likely to discourage non-EU companies from developing products and services under EU jurisdiction, because of the likely loss of trust and the associated reputational damage. As Europe prepares for the next decade and aims to become a leader in digital technologies, it should be wary that companies “are not comfortable storing customer data” in places where controversial encryption laws are in place.[7]

Risks of client-side scanning

Finally, we are concerned with some of the proposed technical solutions, such as pre-emptive scanning of users' communications before they are sent and/or encrypted. Three factors are of particular concern.

First, the accuracy and reliability of automated image analysis. The consequences of "false positives" in this context are extremely concerning: if an individual is wrongly thought to have had or distributed illegal material, they could suffer disproportionate harm as a result[8]. Where such decisions are automated, this could also violate the individual's rights under the ECHR and/or Convention 108[9].

Second, the effectiveness of automated image analysis as a preventive mechanism. While vendors apparently claim that their methods are accurate and robust, and compensate for slight changes to digital content such as images, we do not believe these methods will

---

[5] http://www.oecd.org/sti/ieconomy/data-driven-innovation.htm
[6] https://ec.europa.eu/growth/tools-databases/dem/monitor/content/welcome
[7] https://www.abc.net.au/news/2019-03-28/microsoft-says-companies-are-no-longer-comfortable-storing-data/10946494
[8] For example, an unfounded accusation could result in the individual being banned from a platform, suffering reputational damage and family/relationship break-ups, losing their job, or having to go through court proceedings.
[9] See the Council of Europe Opinion relating to automated decision-making, here: https://rm.coe.int/t-pd-2019-09-en-opinion-on-cdmsi-draft-recommendation-1-/168098f0f6

prevent a motivated adversary from communicating illegal content. For instance, they may use simple steganography to "mask" illegal content and make it look innocent[10]. We have not seen evidence that existing tools would be effective against such an approach, which raises the question of transparency: too many of these measures appear to be discussed only in closed fora, lacking the participation of some legitimate stakeholders and robust technical scrutiny of the mechanisms proposed.

Third, pre-emptive monitoring of users' communications is potentially a disturbing systemic vulnerability. Once technical protections are weakened or bypassed by measures such as client-side scanning, the safety of the user depends on appropriate and effective governance; the consultation questionnaire acknowledges the need for appropriate oversight, but leaves fundamental questions unanswered. For example:

- Once such a mechanism is built into the system, how are users to be protected against its abuse for other purposes, such as repressive censoring of user communications, and prevention of access to information?
- Does the presence of client-side scanning mean that users' data is stripped of the legal protections it would enjoy once it was in transmission? If not, at what point would a warrant/approval be needed in order to scan and act on the information on a user's device?

The consultation, as framed, is unlikely to gather the evidence necessary to formulate a safe or proportionate policy.

Conclusion

We hope the Commission pauses to reflect on the real and tangible tradeoffs that are in play with this legislation. Encryption is a complex issue but, ultimately, it is about security: in simple terms, you cannot talk about technical security without talking about encryption. Throughout its regulatory history, Europe has been leading with the principles of proportionality, effectiveness and transparency. We hope to see these principles reflected in this instance.

[10] For instance, the steganographic techniques described here: https://threatpost.com/researcher-hides-files-in-png-twitter/164881/