10 November 2023

EUROPEAN DATA PROTECTION SUPERVISOR

The EU’s independent data protection authority

EDPS Seminar on the CSAM proposal: “The Point of No Return?”

Summary Report

European Data Protection Supervisor

EDPS Seminar on the CSAM proposal: “The Point of No Return?”

Summary report

On 23 October 2023, the EDPS organised a seminar dedicated to the ongoing legislative works on the European Commission’s [Regulation Proposal on Child Sexual Abuse Material](#) (CSAM)[1]. The seminar gathered stakeholders who in the course of last years have been warning about risks associated with the proposal and misconceptions around its potential effectiveness[2].

1. Key takeaways

- Child sexual abuse is a terrible crime, and a complex societal problem. Different types of child sexual abuse and exploitation require different forms of prevention and investigation. The CSAM proposal does not address them.
- The proposed detection orders would interfere with the private communications of people without any connection to child sexual abuse. Children in particular are also likely to be adversely affected, as growing numbers of images flagged as CSAM involve self-produced content shared privately by young people exploring their sexuality.
- The proposed detection orders would critically undermine end-to-end encryption, which is crucial for countering cybersecurity threats.
- Existing detection technologies, in particular for unknown CSAM and grooming, are insufficiently reliable. Instead, the proposed detection orders for known CSAM would result in general and indiscriminate monitoring of private communications. Such generalised surveillance cannot be a remedy to the social problems of child abuse and exploitation.

2. Summary of interventions

Opening the seminar, Wojciech Wiewiórowski, the European Data Protection Supervisor, stressed the significance of the risks and threats that children are exposed to - both online and offline. He underlined the need to recognise the sensitivity of the topic, which requires caution in terms of the language used, and to show respect for different views. Complexity requires having due regard to evidence, data and expertise. He warned that the CSAM proposal questions the foundations of a democratic society, which, once undermined, might lead to radical shift from which there might be no return.

What is at stake?

During the first round of discussion, participants discussed the effectiveness, necessity and proportionality of the proposal and why the CSAM proposal has, in spite of its commendable objectives, received substantial criticism.

[1] COM(2022) 209 final.

[2] The event agenda, briefing note and video recording can be accessed here: https://edps.europa.eu/data-protection/our-work/publications/events/2023-10-23-edps-seminar-csam-point-no-return_en.

Several participants noted that the CSAM proposal focuses more on the dissemination of materials than on the prevention of child sexual abuse. In addition, it was submitted that:

- the proposal focuses too much on private communications, whereas actual child sex abuse material is often found on image hosting websites used to spread the material via the 'dark web'.
- the proposed detection orders risk being counterproductive as the sheer amount of images reported will further overflow the law enforcement systems in place, some of which are already overwhelmed with false positive images reported under current temporary legislation. Consequently, the proposed legislation would exponentially increase an existing problem instead of solving it.

Several participants underlined that a growing number of materials flagged as CSAM are not a result of child sexual abuse but rather self-produced and consensually exchanged images of sexual activity amongst young people. There is a risk of people being falsely accused or, similarly, wrongly identified as victims of child sexual abuse. Several participants called for bigger involvement of children in the debate, enhancing education and awareness raising, simplifying reporting and increased investment in the systems for investigation of child sexual abuse.

Several participants pointed out that privacy is an essential gateway to other rights and that privacy and safety are mutually reinforcing. In this regard, it was stressed that end-to-end encryption (E2EE) is crucial for countering cybersecurity threats; including in national security context. E2EE provides security and safety to children too, especially vulnerable ones (e.g. LGBTQ+ who use internet to explore their sexuality). There was also a warning that the proposal would undermine professional secrecy and legal professional privilege as well as eviscerate privacy and security protection for journalists, dissidents and human rights activists.

Another area of concern relates to the relationship between the proposed EU Centre and Europol. While Europol is a natural partner of the fight against CSAM, recent reporting has highlighted the risk of function creep. A related concern was that all detection reports that are not manifestly unfounded would also be forwarded to Europol.

During the discussion, several participants called for a multidisciplinary approach. Such an approach should restrain voluntary scanning, not legalise it, and ensure that the detection measures are sufficiently targeted. **The future regulation should enable providers to address CSAM with alternative techniques that do not involve scanning messages, such as product design to prevent harms, users' reporting, use of traffic data and others.**

Effectiveness, accuracy and legality: promises vs. reality

During the second round of discussion, participants were invited to consider the effectiveness, accuracy and legality of detection orders as envisaged by the CSAM proposal.

Several interventions made it clear that the proposed detection orders would critically undermine E2EE. Participants also stressed that **it is technically impossible to reliably detect new CSAM and grooming in encrypted content. Moreover, current AI-powered detection technologies for unknown CSAM have extremely poor statistics and would yield unreasonably high false positives and false negatives.** On the other hand, detection techniques for known CSAM are mainly proprietary, meaning the algorithms are not open for external review. As a result, much of the debate relies on assurances of the companies for the accuracy of the tools.

Tests by researchers have shown that it is very easy to evade detection of CSAM Moreover, the technologies for detection of grooming are insufficiently reliable. Existing age verification techniques trigger concerns in terms of reliability and/or intrusiveness.

The serious concerns about available detection technologies are supported by independent academic research. For instance, the UK National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) evaluated five proof of concept tools designed to detect or prevent CSAM on end-to-end encrypted platforms. None of the assessed tools satisfied the relevant criteria, leading to the conclusion that the tools are not ready to be deployed on a large scale on private messages within end-to-end encrypted environments.

Several participants focused on the **likely negative effects of the CSAM proposal on children**. They warned that technologies to detect CSAM would flag consensually produced and shared imagery, as these technologies cannot properly consider the context in which the exchange takes place. Neither platform moderators, nor the EU Centre would be able to filter consensual material because they too would not know the context of the exchange. There is a risk for criminal prosecutions but even if law enforcement authorities drop the charges, the investigation alone would be disturbing and constitute a violation of children's rights.

The legality of the CSAM proposal and the possible legal challenges were also discussed. It was noted that the Proposal could be found to violate the very essence of the fundamental rights to privacy and data protection and thus be invalid. The opinion of the Council Legal Service was also mentioned in this context.

Way forward

During the final round of discussion, participants explored alternative measures to tackle child abuse and its perpetuation on the internet, also looking at the approaches chosen in other countries, such as the recently adopted UK Online Safety Bill.

Experts also commented on the suggestion to use client-side scanning as an alternative to "breaking" encryption. It was noted that CSS was a very new technology with significant risks associated with its use, including possibilities to tamper with images either to avoid detection, or to generate collisions. Research is still nascent and results so far are inconclusive. More independent scientific research should be carried out before considering to legally require the use of such technologies.

The speakers underlined that **the detection orders should be targeted and limited only to persons suspected of committing CSAM-related crimes**. This would not be achieved through broad definition of "reasonable grounds for suspicion".

In conclusion, the participants stressed the need to preserve the integrity of Europe's rights-based system and called for due diligence and respect for the scientific consensus during the legislative process.

Wojciech Wiewiórowski closed the event by concluding that the discussion had showed how measures combatting child sexual abuse should in their design be complex, namely by addressing the problem on multiple levels and at different stages. Scanning of messages is not only a threat to the privacy, but also a means that produces extremely questionable results. In its current form, the CSAM proposal would fundamentally change the internet and digital communication as we know them.