17th November 2025 - Comments on the EU Presidency's new proposal for the Child Sexual Abuse Regulation

Dear Members of the Council of the European Union,
Dear Ambassadors,

We are writing in response to the new proposal by the Presidency dated 13 November 2025 (15318/25).

We welcome the new changes in the new proposal that eliminated the mandatory nature of on-device CSAM detection. We believe this significantly improves balancing the very necessary protections for children online, with the security and privacy risks that these protections bring for society as a whole.

Yet, we are worried that other aspects of the proposal still bring high risks to society without clear benefits for children.

Broadening the scope of detection

The first aspect concerns the widening of the detection scope. By referencing the voluntary activities under Regulation (EU) 2021/1232 (the temporary derogation to Articles 5(1) and 6(1) of the ePrivacy Directive), the proposal reinstates the option to analyze content beyond images and URLs – including text and video – and to detect newly generated CSAM. As worldwide security experts already warned in an open letter in July 2023, current AI technology is far from being precise enough to undertake these tasks with guarantees for the necessary level of accuracy. False positives seem inevitable, both because of the inherent limitations of AI technologies and because the behaviors the regulation targets are ambiguous and deeply context-dependent.

Extending the scope of targeted formats will further increase the very high number of false positives – incurring an unacceptable increase of the cost of human labor for additional verification and the corresponding privacy violations. We have given several examples before for images, e.g., naked images sent to a doctor, or teenagers exploring their sexuality. The same arguments are applicable to text messages that might correspond to grooming. For example, grooming behaviors can be very similar to interactions that are perfectly acceptable in a friendly context, such as conversations with relatives or close friends, or conversations between teenagers exploring new relationships. Thus, expanding the scope of detection only opens the door to surveil and examine a larger part of conversations, without any guarantee of better protection - and with a high risk of diminishing overall protection by flooding investigators with false accusations that prevent them from investigating the real cases.

Mandatory age verification and assessment

A further worrying aspect is the mandatory age verification and age assessment for software stores and end-to-end encrypted interpersonal communication services that are deemed at high risk of solicitations. First, we would like to reiterate what experts explained in a recent open letter: adding age verification is not necessarily a synonym for extra security. If CSAM detection is not effective, age verification brings less benefits, and if age verification is not effective, CSAM detection is not useful (e.g., for grooming). Next, we would like to caution about issues with age assessment and age verification technologies.

Age assessment, cannot be performed in a privacy-preserving way with current technology due to reliance on biometric, behavioural or contextual information (e.g., browsing history)--contradicting the aforementioned Recital and Article 4(3). In fact, it incentivizes (children's) data collection and exploitation. Age assessment is currently mostly reliant on AI-based inferences, which for the particular data types necessary (e.g., biometrics) are known to have high error rates and to be biased for certain minorities. We conclude that *age assessment presents an inherent disproportionate risk of serious privacy violation and discrimination*, without guarantees of effectiveness.

Age verification typically relies on users presenting a document stating their age from an authoritative source. Presenting full documents (e.g., a passport scan) obviously brings security and privacy risks and it is disproportionate as it reveals much more information than the age. Privacy-preserving presentation, in which cryptography is used to just prove that the age of the user is adequate for accessing the service, reduces privacy risks, but does not come without challenges. These technologies are likely to introduce dependencies on secure hardware, or on particular software providers and thus can result in discrimination of users who do not have devices that comply with the latest technology. Mandating technological requirements without a guarantee that they can be deployed without infringing users' rights is extremely risky for society -- and contrary to the mandate in Article 4(3).

Even without the issues above, the mere introduction of the technology can result in discrimination, as only those people who can present a proof of age by an authoritative entity can use the system. There is a substantial fraction of the population who might not have easy access to documents that afford such a proof. These users, despite being adults in their full right of using services, would be deprived of essential services (even some as important as talking to a doctor). This is not a technological problem, and therefore no technology can address it in a satisfactory manner.

Finally, all the risks above are unfortunately not countered by a guarantee of effectiveness. Age verification controls can be easily evaded, by using providers outside the EU or VPNs to avoid geolocation checks (both have been observed recently in the UK). Both cases can result in higher risks for children because these alternate services are likely to present security risks (weak or absent encryption) and extensive tracking practices, sometimes for malicious purposes. These shifts can only be prevented by inserting more surveillance and controls on the internet, criminalizing use of privacy technologies such as VPNs, and centralizing even more

power in mobile phone manufacturers and their markets by forbidding alternative devices and app stores. These limitations are inherent to our current infrastructures and cast doubt that age verification can be deployed at the scale and breadth envisioned in the regulation in a proportional manner where the benefits outweigh the risks.

Overall, these issues have significant impact on privacy, on discrimination, and on accessibility, and ultimately on effectiveness; making the deployment of age verification and assessment and the goals set in Recital (16a) incompatible.

Voluntary detection still harms security and privacy

Finally, we would like to reiterate that, even if deployed voluntarily, on-device detection technologies cannot be considered a reasonable tool to mitigate risks, as there is no proven benefit, while the potential for harm and abuse is enormous. The effectiveness of detection technology is currently insufficient and unlikely to improve substantially in the future due to the nature of the task and the limits of AI technology (see the letter of worldwide security experts from July 2023). Moreover, implementing detection that informs anyone else except the sender and intended recipient of message content (e.g., the provider or law enforcement) means that the provider can no longer claim to provide end-to-end encryption. Thus, any communication in which results of a scan are reported, even if the scan is voluntary, can no longer be considered secure or private, and cannot be the backbone of a healthy digital society.

Signatories

Prof. Diego F. Aranha, Aarhus University (Denmark)
Prof. Olivier Blazy, École Polytechnique (France)
Dr. Anne Canteaut, Inria (France)
Prof. Cas Cremers, CISPA Helmholtz Center for Information Security (Germany)
Dr. Stephen Farrell, Trinity College Dublin (Ireland)
Prof. Kimmo Halunen, University of Oulu (Finland)
Prof. Jaap-Henk Hoepman, Radboud University (Netherlands), Karlstad University (Sweden)
Prof. Anja Lehmann, University of Potsdam (Germany)
Prof. Vashek Matyas, Masaryk University (Czechia)
Prof. René Mayrhofer, JKU Linz (Austria)
Prof. Kenneth Paterson, ETH Zurich (Switzerland)
Prof. Bart Preneel, KU Leuven (Belgium)
Prof. Kai Rannenberg, Goethe University Frankfurt (Germany)
Prof Peter Y A Ryan, University of Luxembourg, (Luxembourg)
Prof. Tjerand Silde, NTNU (Norway)
Prof. Juan Tapiador, UC3M (Spain)
Prof. Carmela Troncoso, MPI-SP (Germany) and EPFL (Switzerland)
Prof. Stefano Zanero, Politecnico di Milano (Italy)