Position Paper on the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

Introduction

ISPA Belgium (Internet Service Providers Association) brings together the entirety of the Internet industry ecosystem in Belgium, representing the collective voice of the Internet community. ISPA members are committed to making the digital space a safe space for everyone and to protecting children online in particular, and support the EU strategy for a more effective fight against (online) child sexual abuse. ISPA therefore shares the objectives of the proposed Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (CSA). This legislation is timely given that the ePrivacy Directive Interim Derogation, that currently provides us with a legal basis to detect child sexual abuse material (CSAM) in private communications, will expire in August 2024.

Moreover, ISPA favors harmonization and an EU-led approach on the matter, rather than many national approaches, as fragmentation of rules only leads to more inefficiency.

However, ISPA members are concerned about the operability of the Regulation, as well as the possible legislative gaps it creates.

End-to-end encryption (E2EE)

As currently drafted, the Regulation's provisions around detection orders could amount to mandating providers to filter and scan for known and new CSAM and grooming in end-to-end encrypted spaces, for instance through the use of client-side scanning technologies. In this regard, the proposed Regulation holds a risk of degrading and discouraging the use of E2EE. E2EE ensures the protection of the data of online services' users and creates an Internet infrastructure which is safe, trustable and protective of users' private life. Weakening E2EE would create serious issues for the safety of the internet, undermining privacy requirements and representing a great risk to cybersecurity. While we are mindful of the risks that encrypted communications can hold, end-to-end encrypted spaces should be explicitly excluded from the detection orders and other specific mitigation measures.

Recital 26 of the CSAM Regulation proposal currently states that the providers are left with a choice of technologies to comply with detection orders and that the Regulation should not be understood as disincentivizing the use of any given technology, such as E2EE.[1]

However, ISPA believes that E2EE should be more explicitly protected in the Regulation, and advocates for the inclusion of language stating that nothing in the Regulation can be interpreted as weakening or prohibiting encryption, in line with the ePrivacy Directive Interim Derogation. E2EE services should be clearly excluded from scanning obligations and should be allowed to meet their obligations to mitigate the risk of child sexual abuse without being forced to access the content of private communications.

Prevention-led approach

The proposed Regulation heavily focuses on the detection of CSAM but fails to recognize the importance of prevention. ISPA believes a more prevention-led approach should be included in, and actually at the forefront of, the Regulation, based on the proportionality principle. Child sexual abuse must be prevented from happening in the first place, not just reported and detected once it has happened. Mandatory efforts should only follow when voluntary efforts are not enough to mitigate risks. Detection orders should be measures of last resort, as they hold a risk of contradicting the prohibition of general monitoring, a core tenet of European law recently reaffirmed in the Digital Services Act (DSA).[2]

ISPA advocates for voluntary measures to be recognized and accommodated in the text. Providers should be able to develop approaches to tackle CSA that are effective, proportionate and appropriate for their service, adapted to the technical realities and the business of the provider. This means that operators should be free to use the type of blocking technology that is best suited to the business. Several ISPA members have tools in place for voluntary detection of CSAM and prevention of CSA within their own systems. The current Regulation does not allow interpersonal communications services (ICS) to continue their important voluntary efforts, as it does not create an express legal basis for data processing for the purpose of prevention and detection of CSA. Indeed, the proposal outlines that only upon failing a risk assessment, a company would receive a detection order from a designated competent authority that could constitute a legal basis to process communications data. ISPA believes that providers should be enabled to (further) develop

[1] Recital 26 Regulation: *"The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the detection orders issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with detection orders and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. That includes the use* ***of end-to-end encryption technology****, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. When executing the detection order, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users."*

[2] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

preventive approaches and measures, and that should be done by creating an express legal basis to process communications metadata for the purposes of prevention and detection with appropriate safeguards in the text.

Internet Access Service (IAS) providers should be regarded as the location of last resort to disable access to CSAM, and play an important role in implementing accurate blocking lists

Building upon the previous point, the disabling of access should as a principle happen as close to the source as possible. Therefore, providers of internet access services (IAS) should be regarded as the location of last resort to disable access to CSAM.

While we advocate for the disabling of access to CSAM as close to the source as possible, we would like to bring to the attention that some IAS-providers already today block for CSAM content based on blocking lists managed either by national authorities or by NGOs having the public authorities' sanction to manage such blocking lists, such as the list provided by the IWF. This system ensures that no employee within the ISP's organisation needs to verify the content as this is already managed centrally by the entity distributing the blocking list.

We see an important role in the proposed EU Centre: there is a unique opportunity to let the EU Centre manage a state-of-art blocking list containing appropriate blocking information to allow providers of information society services to deploy blocking of known CSAM content. We believe that this should be the main purpose of the EU Centre. Providers directing their services towards end-users situated within the EU should be obliged to deploy such a blocking list to their services.

Nevertheless, in the understanding that CSAM content should be dealt with as close to the source as possible, in order to have the most effective and timely response, there are a number of issues with blocking lists, which should therefore only be considered as the last resort:

- These can be technically easy to bypass (e.g. use of VPN or other DNS-servers), including by using new technical developments such as browser-built DNS over HTTPS (DoH) or Apple Private Relay, which leave the ISP with no influence in the process
- Blocking lists can also be complex in practice: are proxies and mirrors also to be blocked?
- Blocking lists also risk falling in the space between inefficacy (does not solve the root problem) and over-blocking (risk of blocking legitimate content when using IP-addresses)

Number-based interpersonal communication services (NB-ICS) and Business to business (B2B) services

Including NB-ICS in the scope seems rather unfeasible. As pointed out by the EDPB/EDPS in their Joint Opinion 4/2022, the scanning of audio communications, like voice messages and live communications, is intrusive and should remain out of the scope of the detection obligations in the Regulation.[3] Traditional ICS such as phone calls and SMS technically do not allow for any risk mitigation measures and should therefore not fall under the scope of the Regulation.

[3] EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse : https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en.

Equally, as they do not hold a risk of transmitting CSAM, also B2B services should be exempted from the scope of the Regulation.

Conclusion

The European Parliament and the Council have laid down rules to prevent and combat child sexual abuse (CSA). ISPA members are committed to making the digital space a safe space for everyone, and thereby share the objectives of this proposed Regulation.

However, ISPA is concerned about the protection of E2EE, the absence of a prevention-led approach and the current role of IAS, NB-ICS and B2B services in the Regulation. Furthermore, once passed, this legislative proposal will be immediately applicable in Belgium and impact its active providers.

Given that the Minister of Justice is responsible for the CSAM file and in this framework participates in negotiations in the Council of the EU, ISPA hopes its position could be taken into account by the Minister in these negotiations.

Our sector association is happy to welcome the opportunity to further explain our views at a physical meeting.