ETNO POSITION PAPER

European Commission's proposal on preventing and combatting child sexual abuse

European Commission's proposal for a Regulation laying down rules to prevent and combat child sexual abuse

ETNO welcomes the initiative taken by the European Commission to prevent and combat child sexual abuse material online. ETNO members have been actively engaged in numerous initiatives to this end, including collaboration with law enforcement agencies, and the implementation of blocking lists.

The Commission's proposal is highly relevant and timely, given the prevalence of this serious issue, and telecommunications network operators have long been – and will continue to be – committed to playing our part in ensuring the safety of the digital ecosystem. Nevertheless, we believe there are some aspects of the proposed Regulation which require improvement, in order for the final rules to form part of a holistic and effective set of instruments to strengthen capacities and combat this type of crime.

Each player in the internet ecosystem, and indeed law enforcement agencies, government and society, has an important and distinct role. In order to develop a strong response to the prevalence of child sexual abuse online, the resources and capacities of appropriate national authorities must be reinforced. By way of example, when it comes to blocking known CSAM, it is important that law enforcement agencies be responsible for the identification of the URLs and guarantee their accuracy, and private operators carry out the implementation of blocking lists.

Above all, the guiding principle of this important piece of legislation must be that illegal content – in this case CSAM – should be removed as close to the source as possible. Not only does this protect the confidentiality of communications, ensuring a more targeted and proportionate legal framework, but it also improves the efficacy of the measures. In the case of solicitation, the place where the first contact is made (often social media / online platform) is the place where a timely and effective intervention should take place.

Number-based interpersonal communications services should be excluded from the scope of the Regulation, recognising the relevant locus of such criminal activity, and protecting privacy

The category of **interpersonal communications services** (ICS) does not distinguish sufficiently precisely between **number-based** and **number-independent** ICS (obligation to detect and report). Number-based ICS includes voice and text-based communications, which is now residual, and are typically not the services used to carry out the illegal activities.

Number-based ICS should be excluded from the scope, as detection and reporting obligations on such services would be particularly invasive. It is paramount that for NB-ICS public trust is maintained and that the **principle of confidentiality of communication is preserved**. Indeed, the proposed measures would contradict established law and the principle of confidentiality of communications, e.g. in the European Electronic Communications Code.[1] Furthermore, Article 6 of

[1] Directive (EU) 2018/1972

the ePrivacy Directive[2], limits the possibility of providers of publicly available electronic communications services to process personal, traffic and other data, with the explicit objective of setting a high standard of privacy and confidentiality in electronic communications.

For NB-ICS, **we recommend that the current system of interception remains in place for criminal investigations**, which is based on prior judicial orders to allow for interception. It must also be noted that the interim Regulation adopted between the entry into force of the ePrivacy Directive, and the forthcoming adoption of the CSAM Regulation, applies only to ***number-independent*** ICS, recognising that NB-ICS are not a relevant part of the ecosystem in this case.

A clear distinction between different types of hosting services to ensure only those services with the technical means to act are required to intervene

The category of **hosting services** does not distinguish between different types of hosting service, e.g. **Business-to-business cloud**. Hosting services would be required to detect and report, and to remove and disable CSAM content. The definition of hosting service providers should be aligned with jurisprudence of the Court of Justice of the European Union[3] to avoid the risk that passive hosting services are captured in the scope. Furthermore, for business-to-business cloud hosting services, **the provider has no technical ability to detect CSAM where such communication is encrypted**.

Consideration should be given to the Digital Services Act, in particular **recitals 27 and 51**, which recognises that notices should be directed to the providers of hosting services **that can reasonably be expected to have the technical and operational ability to act** against such specific items.

Encryption is an important feature in communications, and in the development of new networks, and should not be undermined

Encryption used for the purpose of **protecting network infrastructure** and **essential communication** services, such as NB-ICS, are key requirements in 4G and 5G networks. Any measures which require monitoring of such communications or content would undermine encryption, and could have the serious effect of **creating security risks in networks and communications**.

We note that in the joint position of the EDPB and the EDPS[4], it is recommended that the proposed Regulation do not undermine the security or confidentiality of electronic communications of European citizens, and that **the Regulation should clearly state that nothing in the proposed Regulation should be interpreted as prohibiting or weakening encryption**, in line with Recital 25 of the Interim Regulation: "End-to-end encryption is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. Any weakening of

[2] Directive 2002/58/EC
[3] Cf. L'Oréal v. eBay C-324/09, and Google France C-236/08 to C-238/08
[4] EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, July 2022

encryption could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be interpreted as prohibiting or weakening end-to-end encryption." [5]

In the case of the provision of cloud services, the information is often encrypted and, usually, the system/encryption keys are chosen by the (business) customers, and are not managed by the hosting provider. In that case, there are technical limitations that prevent the fulfillment of detection requirements on specific content.

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

Providers of internet access services (IAS) should be regarded as the location of last resort to disable access to child sexual abuse material. The disabling of access should as a principle happen **as close to the source as possible**.

While we advocate for the disabling of access to CSAM material 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**: with the establishment of the 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)

[5] Regulation (EU) 2021/1232

The proposed Regulation should be designed to be proportionate and effective to the aim of protecting children by dealing with CSAM in a targeted way, while protecting fundamental rights

While this proposed Regulation would appear to contravene the principles established in the EU acquis on the confidentiality of communications, such a derogation is foreseen in the ePrivacy Directive.[6] This possibility is defined in **Article 15 (1) of the ePrivacy Directive**: Member States have the possibility to adopt legislative measures restricting the scope of rights and obligations of ePrivacy Directive under certain conditions. Such a restriction must constitute a necessary, appropriate and **proportionate** measure within a democratic society for:

- Safeguarding national security
- Defence
- Public security
- Prevention, detection and prosecution of criminal offences

Furthermore, the same article mandates that such a restriction must be adopted in accordance with the **general principles of Community law**, including those referred to in Article 6(1) and (2) TEU (namely adherence to the **Charter of Fundamental Rights of the EU**, and the fundamental rights established and guaranteed by the **European Convention for the Protection of Human Rights**). The Charter of Fundamental Rights of the EU enshrines the protection of personal data, and freedom of expression and information.

Such freedoms are also guaranteed by the constitutional traditions of EU Member States, e.g. Article 10 of the German *Grundgesetz* [7]; and at the level of the United Nations, e.g. International Covenant on Civil and Political Rights.[8]

Furthermore, with respect to principle of **proportionality**, it must be considered if the measures proposed by the European Commission in the proposed Regulation are in keeping with this principle, as established in Article 5 TEU.

Since the interpretation of what constitutes an Information Society Service may need an interpretation of the European Court of Justice (CJEU), the CSAM proposal should align its scope with the findings of its own Impact Assessment by clearly including online platforms, social networks, browsers and search engines as examples of relevant information society services.

[6] Directive 2002/58/EC
[7] GG - Grundgesetz für die Bundesrepublik Deutschland (gesetze-im-internet.de)
[8] International Covenant on Civil and Political Rights | OHCHR

ETNO (European Telecommunications Network Operators' Association) represents Europe's telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For questions and clarifications regarding this position paper, please contact Ross Creelman (**creelman@etno.eu**).

ETNO (European Telecommunications Network Operators' Association) represents Europe's telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

European Telecommunications
Network Operators' Association

info@etno.eu
+32 (0)2 219 3242
WWW.ETNO.EU

@ETNOAssociation

#5GAndUs

Subscribe to our weekly digital newsletter