DOT. europe
Digital • Online • Tech

December 2022

DOT Europe position paper on the Regulation laying down rules to prevent and combat child sexual abuse

ISSUE PAPER 2

Detection orders

Risk assessment and mitigation obligations will be 'complemented where necessary' by specific orders for detection and removal of CSA. We appreciate the efforts the European Commission has made to ensure that procedural safeguards are in place for detection orders, especially the involvement of the Data Protection Authorities and the need for a judicial order. The proposal aims at imposing targeted measures that are proportionate to the risk of misuse of a given service for online CSA but the provisions would benefit from further clarity, as we have explained previously[1]. While the detection orders enable a targeted approach, DOT Europe highlights that several safeguards must be implemented to ensure that orders do not impinge on users' fundamental rights.

The concerns with the proposal's Chapter X, include (1) its exclusive focus on detection, rather than wider measures that could help mitigate the risk; (2) concerns with regards to the scope of the detection orders, both in terms of content (a) and providers (b) covered; and (3) the impact on end-to-end encryption (E2EE).

Focus on detection, rather than wider prevention measures

The proposed Regulation has the *prevention* of CSA as its main stated aim – in fact, it is clearly stated in the title of the proposal. However, when it comes to orders issued for failure to effectively mitigate the risk, the focus is squarely on detection. The issuing of a detection order will force providers to use technology for the detection of known, new material and solicitation, without any wider regard to the additional solutions that may be available to prevent and mitigate this type of content and abuse in the first place. The detection orders should consider wider solutions rather than focusing exclusively on the detection of content and solicitation.

Scope of detection orders

a) Content covered by the detection orders

The scope of the new detection obligations is very broad as it could entail known *and* new or never-before-hashed CSA. These obligations will apply not only to public-facing services (i.e. hosting services) but also to 'private' services, including ICSs. In addition to posing specific challenges, considering the

[1] Please refer to our first issue paper on Risk assessment and mitigation.

Rue du Trône, 60, 1050
Brussels, Belgium
Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

state of the technology for the detection of this type of content and behaviours[2], these obligations will likely result in heavy levels of intrusiveness in respect of the fundamental rights of users, and in particular on their right to privacy (including confidentiality of communications, as part of the broader right to respect for private and family life), right to protection of personal data and their freedom of expression and information, as noted by the European Commission[3]. Even if the proposal includes checks and balances, detection orders still risk being in conflict with the long-standing prohibition of general monitoring obligation, one of the cornerstones of the DSA and previously of the eCommerce Directive. This is because a detection order implies an obligation to implement a technology that systematically analyses all content on a service. This is particularly the case when the detection orders concern new CSAM and solicitation of minors.

In addition, the new rules will require providers to explicitly ensure human intervention and supervision to minimise the error rate in executing detection orders for solicitation, which will attribute private companies a disproportionate role, incompatible with the legitimacy of the whole process besides having a great adverse effect on the privacy of online communications, as pointed out in the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) joint opinion[4].

To achieve the aim of the proposal to impose targeted measures proportionate to the risk of misuse of a service, detection orders must be issued as a measure of last resort. The risk and proportionality threshold to be met to trigger detection orders should be clearly defined in the legislation and high enough to strike a fair balance between the fundamental rights of all parties involved and to ensure proportionate obligations on providers.

b) Types of providers covered by the detection orders

In addition to the scope of detection orders including a broad range of CSA, the proposal does not differentiate between all the providers falling under the definition of "hosting services", and thus may apply detection orders to service providers that are ill-suited to apply such technology, namely cloud infrastructure providers. As mentioned further in our position paper[5], it would be inappropriate to apply a detection order to cloud infrastructure providers, which offer cloud-based services that their customers then use to build, design, control and manage their services. It is the latter that are closest to the content hosted on their platforms, and who have the complete control and responsibility over the relationship with the end-users that upload this content. Cloud infrastructure providers do not have sufficient control on the level at which detection is applied to implement a detection order, which should "not go beyond what is strictly necessary to effectively address the [CSA] risk" in order "to avoid undue interference with fundamental rights and ensure proportionality" (Recital 23). It would thus be disproportionate to include cloud infrastructure providers in the detection obligations of this Regulation.

---

[2] Please refer to our third issue paper on Technologies.
[3] EC Impact Assessment Report, p. 94.
[4] 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
[5] Please refer to our fourth issue paper on Scope.

Impact on E2EE services

DOT Europe underlines that E2EE is a very important tool used to protect users' privacy, security and safety online as well as their human rights. A range of security and privacy experts, including EDPS and EDPB[6], have explained why E2EE is so important and should not be weakened. The proposal does not adequately protect end-to-end encrypted messaging services in its provisions and could therefore stop providers from offering E2EE.Indeed, providers would be forced to break this encryption and to build backdoors to enable the circumvention of the technology requested by scanning orders. As flagged further in our position paper[7], no technology currently exists that allows for scanning in an E2EE environment without breaking encryption. Thus, incorporating intentional vulnerabilities in such environments will disincentivize the offering of such technology and could even be considered irresponsible.

Moreover, practical implementation of these detection orders will raise a number of questions regarding the privacy costs possibly imposed by the new system, as stressed also by the joint opinion of the EDPB and the EDPS.

Examples of current practices

- **Meta** considers that the values of safety, privacy, and security are mutually reinforcing. As they are progressively moving their products towards E2EE systems, they are committed to continued engagement with law enforcement and online safety, digital security, and human rights experts to keep people safe.
- **Google** has developed machine learning technology to detect, and support partners, with the detection of new CSAM. The confirmation of the nature of CSAM is always done by human reviewers.

DOT Europe's recommendations

Acknowledgement of wider prevention measures

- The proposal should explicitly recognise that detection orders are not the only way to fight against CSA online and that providers have initiatives in place already that help to avoid CSA to happen on their services in the first place. The mitigation measures could include prevention and/or other measures that meet the requirements of Article 4 and move past the sole focus on detection for risk mitigation.

Scope of detection orders

- The text should also explain in detail how Coordinating Authorities will arbitrate between fundamental rights and to what extent "reasons for issuing the detection order outweigh

[6] Op. cit.
[7] Please refer to our third issue paper on Technologies.

negative consequences for the rights and legitimate interests of all parties affected" (Art. 7(4(b))).

- DOT Europe would recommend very clearly defining the threshold that has to be met in order to trigger a detection order. This threshold should strike a fair balance between the fundamental rights of all parties involved and to ensure proportionate obligations on operators.
- Detection orders should be as precise as possible and communication thereabout as efficient as possible so as to allow service providers to act without undue delay to address the egregious content.
- Detection orders should be considered as a measure of last resort. We welcome some of the procedural safeguards already proposed, in particular the need for Data Protection Authorities to be consulted, the need for a balancing against negative consequences for the rights and legitimate interests of all parties as well as the fact that the detection order must be based on court order. These safeguards are fundamental. In case they are issued, orders should be targeted (both in terms of recipients, content and timeframe) and subject to appropriate and robust safeguards. DOT Europe would welcome more detail regarding the content of a detection order to ensure that they will provide a stable framework for service providers.
- Detection orders should only be issued if relevant technologies are available, are proportionate and do not lead to an excessive rate of false positives, which would have negative effects on fundamental rights of all parties involved.
- DOT Europe recommends a similar approach to the e-Evidence Regulation proposal where corporate users would be the first approached for data before the cloud infrastructure providers themselves. Additionally, DOT Europe would welcome a text which limits responsibility, for this kind of providers, to options such as removal and blocking orders, suspension of service to or reporting of infringing users. Consideration should be given to the Recital 27 DSA, which recognises that notices should first be issued to providers that posses the technical and operational ability to act against specific items of illegal content.
- Private companies should not be requested to ensure human intervention and supervision in executing detection orders for solicitation since it would have a great adverse effect on the privacy of online communications.

Protection of E2EE services

- The Regulation should protect encryption, especially E2EE, reflecting language included in the ePrivacy Directive Derogation and the Digital Markets Act, and enable encrypted services meet their obligations to tackle CSAM without accessing message contents; for example, through product design, user reporting and other techniques - and empowered by an express legal basis to process communications data for the purposes of preventing, detecting and reporting CSA.

Detection of new CSAM and solicitation

- DOT Europe strongly cautions against imposing detection orders for solicitation of minors and detection of new CSAM before detection technology is fully developed, tested and can allow a fair and correct balancing of privacy and safety rights. The additional risks can be adequately addressed under Article 4.