DOT Europe questions document

on the Regulation laying down rules to prevent and combat child sexual abuse

On the scope of the proposal

- Does the Commission wish to reduce the total number of services that scan for/detect known CSAM via detection orders or can companies that currently scan expect to continue doing so under the Regulation?
- The scope of "interpersonal communication services" (ICS) in the proposal is ambiguous. Could we get more clarity as to which ICS are included?
- The inclusion of interpersonal communication services encrypted by default in the scope of the proposal would raise further privacy issues. Can we perhaps get some more insight into the reasoning behind the inclusion of these services? What measures do you consider the most appropriate to cater for this requirement? What type of privacy-protective measures could be put in place for interpersonal communication?
- Do the co-legislators intend to clarify that app stores are not expected to check the age of users on all services that include interpersonal communications?
- Could the legislator provide more clarity as to the services covered by the proposal? It will be crucial for all implicated services to ensure that they are prepared to comply with the Regulation instead of being caught off guard.
    - Regarding ancillary services, why does the CSAM Regulation treat these features differently compared to the European Electronic Communications Code and the Digital Services Act?
    - Regarding hosting services, the DSA in its recital 40a states 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. How can the Regulation appropriately reflect the technical and legal limitations that some services may face in this regard?
- We would welcome more clarity as to why no distinction between service providers was introduced. By imposing the same detection obligations on any 'hosting service', the Commission may fail to take into account important differences between services. For instance, to the extent cloud infrastructure may qualify as a hosting service, it is technically unable to comply with any type of detection order. This is due to the fact that the underlying IT infrastructure provider cannot control or access any of the data or content uploaded by the customer. Do co-legislators plan to identify, for example, a sub category of hosting provider to better target the Regulation?

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

- How could 'solicitation of children' be more accurately defined to make sure it is more precise and enforceable and to allow service providers' technology to be less invasive and controversial?
- How is it possible to reconcile the crucial role played by encryption with requirements to de facto break it as prescribed in the Regulation? Would any mitigation measure other than decryption be considered sufficient?
- How is it possible to reconcile the ban on a general monitoring as recently re-stated under the DSA with the requirements laid out in the Regulation? We have heard Commission officials claim that the provisions of the CSAM Regulation are compatible with the prohibition of general monitoring – but could we get some clarity on how scanning all content on the service on the basis of a detection order does not constitute general monitoring?
- Shouldn't the proposal focus more on prevention mechanisms and initiatives to address the problem in the first place; both offline and online rather than mainly dealing with the lack of prevention mechanisms? Did the European Commission foresee further initiatives to better address the issue of child sexual abuse in itself?
- How will the Regulation work with other pieces of legislation, such as the DSA, the GDPR and upcoming legislation and codes of conduct in the area of child safety?

On risk assessments and mitigation measures

- Is it envisaged that providers conduct risk assessments in closed services like private cloud, email, group messaging and private social media groups? How does the draft Regulation enable providers to conduct risk assessments in a way that is compatible with privacy and data protection law? This risk assessment appears to be a prerequisite to receive a detection order and, therefore, for scanning to continue on such services. While the European Commission seems to confirm that voluntary scanning can continue on hosting services while an order will be necessary for interpersonal communication services, more clarity in the text would be welcome.
- The risk assessment provisions feature a safeguard clarifying that companies which provide low risk services or have effective mitigation measures shall comply with obligations proportionate to the risks linked with their services. However, it remains unclear whether a service provider that has "passed" the risk-assessment can still be subject to detection orders. It would be helpful to clarify that mandatory detection orders cannot be imposed to services that don't represent any risk or that have proper risk mitigation measures in place.
- Does the obligation to carry out a risk assessment extend to domestic email services provided by retail telecoms providers, as well as web-based mail services (as described in Recital 5)?
- Will evidence from law enforcement agencies be used to inform a Coordinating Authority's consideration of a service provider's risk assessment?
- What are the parameters of the 'mitigation measures' envisaged in Article 4(2)? Could these measures include voluntary detection of known CSAM or could this only take place following a formal reception of a detection order?

- What is intended by 'functionalities enabling age verification'? What measures will be considered appropriate and proportionate in light of other EU laws? There are conflicting views on this at EU level and age verification can be very privacy intrusive and may involve a problematic lifting of pseudonymity online. Is article 4(3) limited to services where solicitation of children has been identified as a risk? Could age 'assurance' be a more appropriate approach?
- Can more guidance be provided as to what age verification or assessment measures would be considered necessary or reliable (in relation to Art. 4(3)? How are differences among different services taken into consideration?
- How will the effectiveness of mitigation measures be judged/measured? How can we make sure that Coordinating Authorities all share the same interpretation?
- Under what criteria will Coordinating Authorities determine the 'appreciable extent' to which the service is used for the dissemination of known child sexual abuse material? What if the service is used mainly for private storage and not dissemination of content?
- If 'online child sexual abuse' means the online dissemination of child sexual abuse material (and the solicitation of children), does the definition exclude private storage (i.e. content that is not shared or disseminated)?

On detection orders and detection technologies

- Can the text provide a legal framework for companies to keep on voluntarily detecting CSAM on their services when they are not subject to a detection order – especially in consideration of the fact that the e-Privacy Derogation, currently providing a legal basis for companies to detect, will expire in August 2024?
- What can the Regulation do to address the potential shift of offenders towards more secretive services once detection orders are in place on the mainstream ones? Could an organisation like the EU Centre be tasked to conduct research on current and new methods used by offenders?
- The Regulation seems to require services to 'fail' the risk assessment before a designation can be made and scanning/detection enabled. How will 'failure' be determined by the relevant Coordinating Authority?
- Will detection orders be specific as to what risks each service should address e.g.: could an order require scanning of known CSAM but not detection of grooming?
- What technologies will be made available by the EU Centre to facilitate smaller companies' compliance with detection orders? How can we make sure that these technologies are adapted to the very different services and business models of the companies subject to such orders?
- What will the 'databases of indicators' look like? What does the EC understand by 'indicators'? What does it mean in terms of compliance?
- What commitments can the Commission make to the quality of the EU Centre's database?

- Could the database of indicators possibly incorporate indicators from other databases, including non-EU databases? (cf. Article 54)
- Is the use of technologies (not indicators/hashes) made available by the EU Centre also limited to the timespan of a detection order, or can the provider continue using them once the detection order has expired?
- How long is the EU Centre expected to take to develop databases of "indicators" envisaged in Art 44? Who will assess and validate the quality and effectiveness of these databases?
- Will designated services be able to continue using high quality hash databases such as those provided currently by NCMEC, the Internet Watch Foundation and Thorn, or will they be required to only use the EU Centre's databases?
- Does the Regulation intend to hold the EU Centre liable for unintended legal consequences arising from any requirement on designated services to use its technology? Will the limitation to liability in Article 19 safeguard designated companies from any legal challenge arising from its use of technology developed by the EU Centre?
- Will the Regulation's focus on error rates in technologies developed stifle innovation in that field ? Any focus on error rates is likely to constrain industry activities, as well as the ability to innovate.
- What balance can be reached to allow companies to keep on innovating while still protecting their users' fundamental rights? In that regard, it will be important to clearly distinguish between the tools to detect known CSAM, unknown CSAM and solicitation of children. Accuracy will depend on a range of factors and "reliability" will look different across each of these three content types, given the unique challenges in detection and variances in the available data.
- Can providers mitigate the potential for higher error rates with human review of detected content before reporting it?
- Why does the Regulation fail to distinguish the technological tools to detect known CSAM and those to detect new CSAM and grooming? Differentiating between them would recognise the different privacy risks and could lead to a better outcome and a more targeted and proportionate proposal overall.

User information

- How is it possible to find the right balance between informing users that technologies are in place to execute a detection order and not reducing the effectiveness of the measures? Any information about the existence of such measures will certainly lead to a decrease in their effectiveness.
- Will a generalized statement around technologies used to detect CSAM be sufficient?
- Likewise, given the peculiar characteristics and gravity of CSAM, what purpose does requiring the provider to inform the user, provide information on the content of the report, on the manner in which the provider became aware of the potential CSAM, on the follow-up given to the report, etc. serve? How do the CSAM Regulation requirements in this regard interact with the DSA user notification and redress requirements?

- How pertinent is an IP address to determine the geographic location related to the potential online child sexual abuse?

Legal issues

- Does the Regulation intend to differentiate the privacy risks associated with (a) the use of high quality databases of hashes of known CSAM in combination with mature, industry-standard automated scanning technology like PhotoDNA vs. (b) more experimental and proprietary technologies to prospectively detect previously-unknown victims and material, as well as potentially criminal user behaviour like grooming?
- Does the Regulation intend to hold the EU Centre liable for unintended legal consequences arising from any requirement on designated services to use its technology? Will the limitation to liability in article 19 safeguard designated companies from any legal challenge arising from its use of technology developed by the EU Centre?
- Does the protection from liability under Article 19 and Recital 34 also safeguard designated companies from liability under GDPR? Would a detection order be considered a "legal obligation" legal base under article 6 of the GDPR?
- Bearing in mind that Coordinating authorities cannot overrule Data Protection Authorities under Regulation (EU) 2016/679, could co-legislators provide clarity on how the two authorities will coordinate their efforts to provide clear and enforceable orders?
- How will the Regulation reconcile competing legal obligations on services that are designated but whose services are encrypted?
- Will the mandatory publicly available reporting channels be different to the reporting route provided to Coordinating Authorities as per the Terrorist Content Online Regulation? It is important that the aliases that companies will create to reporting channels are differentiated depending on the audience. Should the Coordinating Authorities be deemed to use the same alias as the general public, such may get lost and make compliance more burdensome?

On the EU Centre and interplay of the proposal with other jurisdictions

- What does it mean for the EU Centre to have the power to conduct "searches" on hosting services for publicly available CSAM?
- The added value of the EU Centre is determined by its capacity to intermediate with national authorities for judicial oversight and determination of illegality of the content reported and maintaining a database of reports sent with indicators enabling detection and quality of data. However, the content definitions and detection requirements are tied to the database of indicators to be held by the EU Centre. What does that mean for content detected in other ways, whether through user reporting, NCMEC hashes, internal classifiers, etc?
- How will the Regulation interface with the existing global approach to the detection and reporting of CSAM, operated via the National Centre for Missing and Exploited Children (NCMEC) in partnership with national law enforcement authorities?

- How can the operation of the Regulation streamline the cooperation between the EU Centre and other bodies outside of the EU, such as NCMEC in order to build on and make more effective, rather than fragment the fight against CSAM?
- How can the operation of the Regulation avoid unnecessary duplication of providers' reporting obligations to the EU Centre and to bodies in other jurisdictions that would ultimately harm the fight against CSAM– for example could reporting to NCMEC (plus triage and onward reporting to national agencies) be considered a means to comply with the Regulation and avoid a breach of legal obligations in other geographies e.g. the US legal prohibition which prevents companies from sharing CSAM with third parties other than NCMEC?
- How will the EU Centre monitor the number of removal orders per provider and accurately measure the time needed to remove or disable access to the items concerned?

Operational transition

- What does the Commission expect service providers to do if the derogation to the ePrivacy Directive expires before the Regulation comes in to effect and services are designated?
- Would the EU Centre make the names of companies designated under the Regulation public? If so, how will it respond when offenders inevitably migrate to services which are not designated? Would more services be designated?
- Bearing in mind that automated CSAM scanning and detection are a crucial element of the proposal, do co-legislators foresee any possibilities in helping service providers build consumer trust in the benefits of these automated scanning processes?
- The obligation on service providers to notify users when their activity has been reported to the EU Centre creates safety of life risk to both the individual user and to any child victims of sexual abuse in their care. Will the Commission remove this obligation and defer to the judgement of local law enforcement to ensure the safeguarding of all parties?