December 2022

DOT Europe position paper

Regulation laying down rules to prevent and combat child sexual abuse

EXECUTIVE SUMMARY

Risk assessment and mitigation
Detection orders
Technologies
Scope
EU Centre and global reporting framework

DOT Europe, the voice of leading Internet companies operating in Europe, and its members welcome the ambition of the Proposal for a Regulation laying down rules to prevent and combat Child Sexual Abuse, published by the European Commission in May 2022.

This compiled paper presents DOT Europe's in-depth views on the proposal, by addressing five issues we believe need to be further improved as part of the considerations by the co-legislators in order to achieve a strong framework enabling stakeholders to effectively prevent, detect and report CSA online.

This proposal should aim at striking a fair balance between the different fundamental rights which could be affected by the measures contained therein. To make sure this is the case, we highlight how prevention, in addition to detection, is also an important tool at the disposal of service providers to avoid the harm from happening in the first place. It is therefore important to maintain the flexibility already granted in the proposal with regards the choice given to providers when they mitigate risks on their services and ensure allowed practices today can continue to be used tomorrow by creating the necessary legal basis (Paper 1). DOT Europe urges that detection orders be limited to the appropriate parties whose position in the Internet stack allows direct contact with end-users. We also strongly encourage to consider ordering detection only if and when detection technology is fully developed, tested and can allow a fair and correct balancing of privacy and safety rights (Paper 2). Indeed, the technology put forward as a solution is still nascent (Paper 3). Furthermore, the types of content and the providers in scope of this proposal should be reviewed in order to bring more clarity and make the text implementable in practice (Paper 4). An important part of this proposal should be dedicated to acknowledging and guaranteeing the possibility of a multistakeholder dialogue, where it is relevant, bringing together stakeholders to collaboratively find solutions to this global problem (Paper 5).

Finally, DOT Europe would like to emphasize how important it is that the CSAM proposal complements existing instruments and legislation already in place to bolster efforts to tackle CSA. This should be done by taking into account global initiatives to address CSA but also consider how the proposal will coexist with EU legislation in place, such as ePrivacy Directive and Digital Services Act.

DOT Europe's key asks:

- Enable voluntary detection with a robust legal base to provide continuity and ease of transition to the new framework;
- Maintain flexibility for companies to assess and mitigate risks, and select solutions suitable for their services;
- Target requirements at the right points in the ecosystem, i.e. at entities with a direct relationship with the user as opposed to infrastructure providers;
- Use detection orders only as a last resort;
- Design EU framework to support established international reporting structures;
- Foster a multistakeholder dialogue on the relevant aspects of online CSA;
- Remove conflicts of law and address them bilaterally on a different track.

ISSUE PAPER 1

Risk assessment and mitigation

Risk assessment and mitigation
Detection orders
Technologies
Scope
EU Centre and global reporting framework

The proposal requires hosting service providers and interpersonal communication providers to conduct a risk assessment in order to evaluate the risk of their respective services being used for the purpose of Child Sexual Abuse (CSA). Once this assessment is completed, providers are required to adopt mitigation measures to tackle the risks identified in their assessment. We welcome this approach which provides an incentive for providers to identify the specific CSA risks associated with their services and address them effectively.

DOT Europe first notes that the DSA also requires very large online platforms (VLOPs) to identify, analyse, assess and mitigate systemic risks their services pose to the protection of children. Recital 8 of the draft Regulation considers this Regulation as *lex specialis* in relation to the generally applicable framework set out in the DSA. Nevertheless, VLOPs would need to consider how their approach to compliance can be aligned under these two instruments in order to avoid potential overlaps.

Furthermore, as highlighted by the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS)[1], the proposal as it currently stands does not provide a clear understanding of what constitutes "significant risk". This is however a fundamental element to underlying both risk assessment and risk mitigation. Additionally, the "effectiveness of mitigation measures" (Recital 18) and the criteria under which Coordinating Authorities will determine the “appreciable extent” to which a service is used for the dissemination of CSAM (Article 7) needs clarification. The proposal lacks precision on how Coordinating Authorities will move to a detection order; it remains unclear whether services having successfully passed the risk assessment and mitigation phase can avoid detection orders or not.

The voluntary use of technologies to prevent online CSA and to detect child sexual abuse material (CSAM) with appropriate safeguards is an important mitigation measure. While the text of the proposal indicates that hosting services may continue to voluntarily detect CSAM, providers of interpersonal communications services (ICSs) would only be allowed to use detection technology upon failing a risk assessment and receiving a detection order, which will constitute a legal basis to process communications data, traffic data or location data a limited time.

The fact that the proposed text does not recognise voluntary efforts, including prevention measures, as possible risk mitigation measures for ICSs is a **step backwards** compared to the current voluntary regime under the interim ePrivacy Directive derogation[2], which allows for the voluntary detection of

[1] EDPB-EDPS, Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, Adopted on 28 July 2022

[2] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of

CSAM subject to safeguards. The text also does not acknowledge the volume and quality of work already undertaken voluntarily, which has led to important innovation in the fight against CSA. This work involves significant historical and ongoing investment, to the benefit of consumers and law enforcement.

DOT Europe believes that the important voluntary work carried out by ICS providers should still be possible to carry out once the interim ePrivacy Directive Derogation[3] reaches its sunset clause. We therefore believe that **the Regulation should include an express legal basis** for ICS providers to use technology for the voluntary detection of CSAM and for the processing of communications metadata for the purposes of prevention and detection, all of this with appropriate safeguards.

Voluntary detection measures and other mitigations conducted by ICSs could be supervised by the relevant Coordinating Authority and Data Protection Authority. This would provide the appropriate safeguards and avoid creating a scenario where companies cannot effectively mitigate the risk in their services because they cannot implement voluntary measures which they then are asked to implement later by a detection order, creating a gap in companies' ability to detect and thereby give perpetrators room to continue to spread this heinous content online.

Last but definitely not least, the proposal introduces possible new obligations on age verification/assurance for ICS providers in need to mitigate solicitation risks on their service. This could de facto result in an obligation for many individual services to each develop their own age verification solutions, without being able to rely on a clearly agreed industry approach on this important issue. As this is an area where the Commission expects to make progress as part of the Better Internet for Kids (BIK+) strategy[4] and the code of conduct[5] that will emanate from it, the proposed legislation should avoid legislating on a contested and evolving matter and instead **defer to the BIK+ strategy for the development of appropriate age verification approach and mechanisms**. The proposal should encourage a multistakeholder discussion in the context of the upcoming code to develop effective solutions. Indeed, the proposal's provisions could de facto result in an obligation for many services to each develop their own age verification solutions, without being able to rely on a clearly agreed industry approach on this important issue. The debate surrounding age verification is technologically complex and will have broader consequences fundamental rights, data, security and privacy. In order to consider all possible outcomes, prior to introducing any new obligation entailing a specific group of digital service providers, DOT Europe sees the value in a **multistakeholder discussion** to develop sustainable technical and technological approaches.

number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1232&qid=1667993362830

[3] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse

[4] A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN

[5] "A comprehensive EU code of conduct on age-appropriate design", see point 5.1 of the BIK+ Strategy

Examples of current practices

Discord's proactive content moderation includes:

- Scanning images uploaded to the platform using industry-standard PhotoDNA to detect matches to known child sexual abuse material.
- In the course of Discord's proactive content moderation efforts, when Discord discovers data suggesting that a user is engaging in illegal activity or violating their policies, Discord investigates their networks, their activity on Discord, and their messages to proactively detect accomplices and determine whether violations have occurred.
- Discord also strives to inform its users about best practices to set up a safe server and a safe account through information disseminated in their Safety Center and Policy and Safety Blog.

Meta developed a multi-layered approach to safety on its private messaging services, which focuses on: working to prevent abuse from happening in the first place; giving people more controls to help them stay safe and; responding to reports on potential harm. This is bespoke and takes a slightly different, but complimentary, approach to how the company keeps people safe on its public services - like Facebook - using signals from those public spaces to help keep private messaging safe.

Prevention is at the core of the work Meta does to protect safety, with its main objectives being:

- Preventing people from being exposed to harmful contact or harmful content;
- Preventing potential offenders from contacting potential victims;
- Preventing offenders from contacting each other;
- Contribute to the broader public safety effort, including by continuing to respond to law enforcement requests and providing reports to NCMEC.

TikTok works with families and youth safety advocates on a holistic approach to keeping children safe. TikTok works to educate families on the safeguards available to help them manage their TikTok experience at the Youth Portal, Safety Centre, and in-app videos. In addition to detection and the use of PhotoDNA, TikTok has taken an upstream, safety by design approach to prevention: it does not permit off-platform images or videos to be sent via direct messages. TikTok also disabled direct messaging for registered accounts under 16.

Google and **Youtube** have invested heavily in fighting child sexual abuse and exploitation online and developed cutting edge technology to deter, detect, remove and report offences on their platforms.

- They use hashing technology to identify, remove, and report copies of known images. This technology allows them to automatically detect illegal content that matches the content that has previously been identified as CSAM.
- In 2015, YouTube engineers created CSAI Match, world-leading technology that can be used to scan and identify uploaded videos that contain known CSAM. YouTube makes this technology available to other platforms and NGOs free-of-charge.
- In 2018, Google engineers created the Content Safety API which, based on machine learning technology, helps identify content that is likely to contain abuse, at scale, more quickly by helping reviewers to prioritise the most likely CSAM content for review.

Google and YouTube support others fulfilling their commitments in the fight against CSAM by offering our cutting-edge technology free-of-charge for qualifying organisations to make their operations better, faster and safer.

Microsoft takes a range of actions to protect children across its consumer hosted services, including the use of technology to detect online child sexual exploitation and abuse and the provision of family safety controls for Windows and its Xbox gaming services. Microsoft's Digital Safety Content Report covers actions that Microsoft has taken in relation to child sexual exploitation and abuse imagery.

Snap Inc has built extra protections for teenagers from the beginning. On Snapchat, teens have to be mutual friends before they can start communicating with each other, by default, friend lists are private and teens are not allowed to have public profiles. Snap recently introduced its Family Center, a tool designed to offer parents, caregivers and other trusted adults insight into who their teens are communicating with on the app, while at the same time protecting teens' privacy, autonomy and growing independence. Adults can view their teens' friends' lists, who they communicated with in the last 7 days and report to Snap accounts that may be of concern to them. Snap employs a multi-pronged strategy, which includes investing in and deploying the latest technologies, leading, collaborating and engaging with others in industry and across sectors and raising awareness among and educating its community about online risks.

Twitter has developed a #ThereIsHelp prompt for child sexual exploitation (CSE) which is designed to help users when looking up terms associated with various manifestations of CSE and to provide them with information about Twitter's zero tolerance policy encouraging users to report such content. The prompt is also intended to connect users to local partners that offer intervention and prevention programs in the national languages. This feature is currently available in 6 countries worldwide (Germany, India, Indonesia, Philippines, Taiwan and Thailand) and in 7 languages.

DOT Europe's recommendations

- In order to have a workable and coherent text, the proposal should not duplicate risk assessments, where a provider is subject more than one regime. For example, the DSA also requires very large online platforms (VLOPs) to assess and mitigate systemic risks their services pose to the protection of children. To avoid any risk of duplication with the DSA requirement for VLOPs to assess and mitigate systemic risks their services pose to the protection of children, one risk assessment should satisfy both obligations, taking the DSA as a baseline.
- The proposal needs to provide a clear understanding of what constitutes "significant risk" and "the likelihood that the service is used to an appreciable extent" (Recital 21). Coherence of understanding on this concept among all Competent Authorities is essential.
- We suggest including a recommendation to clarify the language in the text around the "effectiveness of mitigation measures" and the criteria under which Coordinating Authorities will determine the “appreciable extent” to which a service is used for the dissemination of CSAM. Currently it remains unclear whether services having successfully passed the risk assessment and mitigation phase can avoid detection orders.
- Voluntary efforts to fight CSA should be expressly authorised for all providers in scope of the Regulation. The Regulation should explicitly recognise voluntary efforts as part of the package of risk mitigation strategies available to all service providers under Article 4.
- In addition, the Regulation should create an express legal basis for ICS providers to process communications metadata for the purposes of prevention and detection, with appropriate safeguards. This would ensure continuity with the principles of the interim ePrivacy Directive derogation rather than focusing solely on mandated detection as the basis for detection. The Regulation fails to recognize the importance of prevention, when relevant, and existing voluntary efforts. The proposal should also incentivise the development and use of new detection technologies by permitting them as a mitigation measure. Such technologies play a vital role in detecting new CSAM and expanding the volume of high quality hashes to the benefit of both industry and law enforcement.
- Regarding the risk mitigation measures, Recital 17 clarifies that service providers remain free to assess their respective CSA risks and select which technology and risk mitigations are appropriate for their services. Language of Recital 17 should be reflected in the actual text of the proposal, which should ensure the mitigation measures include prevention, detection and/or other measures that meet the requirements of Article 4.
- Similarly, Recital 18 and Article 4 provide some degree of flexibility when it comes to considering the mitigation measures suggested by the proposed text. DOT Europe underlines the need for the Regulation to maintain the possibility for providers to take into account relevant differences, including between content types and services, when selecting appropriate and proportionate mitigation measures. This will enable providers to ensure mitigation measures are carefully tailored, in line with the intent of Article 4(2). Additionally, the Regulation should require Coordinating Authorities to take these differences into account in evaluating the mitigation measures a provider has taken on its services.
- DOT Europe strongly encourages a multi-stakeholder coordinated discussion via the foreseen age-appropriate design code to first identify the best way forward and accordingly develop sustainable technical and technological approaches before any obligation is laid down in the Regulation.

ISSUE PAPER 2

Detection orders

Risk assessment and mitigation
Detection orders
Technologies
Scope
EU Centre and global reporting framework

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[6]. 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 **state of the technology** for the detection of this type of content and behaviours[7], 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

[6] Please refer to our first issue paper on Risk assessment and mitigation.
[7] Please refer to our third issue paper on Technologies.

expression and information, as noted by the European Commission[8]. 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[9].

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[10], 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.

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

[8] EC Impact Assessment Report, p. 94.

[9] 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

[10] Please refer to our fourth issue paper on Scope.

EDPB[11], 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[12], 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 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

[11] Op. cit.

[12] Please refer to our third issue paper on Technologies.

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.

ISSUE PAPER 3

Technologies

Risk assessment and mitigation
Detection orders
Technologies
Scope
EU Centre and global reporting framework

The proposed text adopts a tech-neutral approach when it comes to methods of detection and other mitigations. DOT Europe welcomes this. However, several areas of concern arise from the proposed provisions.

While the proposal does not specify particular technologies, scanning seems to be the favoured approach. **The Regulation should be open to a broader range of technological mitigations** under the Article 3 and 4 assessment and mitigation process, as long as they are effective, targeted and proportionate. This would allow providers to adopt detection measures which accommodate their respective service features, including E2EE, while also respecting user security and privacy. Indeed, no technology currently exists that allows for scanning in an E2EE environment without breaking encryption.

In addition, the proposal empowers the new EU Centre to develop or endorse particular technologies and mandate their use. This merits further reflection. It will take time for the EU Centre to build the necessary expertise to develop or assess technologies so the proposal must facilitate a more flexible and pragmatic approach to ensure continuity of detection and technological innovation. Mandating by the EU Centre should, like detection orders, be a last resort and defer to providers' risk assessments and choice of mitigation measures in the first instance.

Many smaller providers who do not have the resources to develop their own detection technology will come to depend on the technology vetted and recommended by the EU Centre. It would be therefore essential to give those interested players the opportunity to **participate in the process** lead by the Technology Committee to issue its recommendation to the EU Centre. Interested players should be afforded the opportunity to stress test the technology they might need to deploy going forward.

The proposal also empowers the EU Centre to develop and manage databases of indicators. There are robust processes and procedures in place to ensure that databases currently used by providers are of high quality. It is important that **any new databases developed by the EU Centre meet the same high standards** of classification as those currently in use.

When it comes to technology, huge investments have been made in the last 15+ years to advance hash-matching tools for the detection of known CSAM[13]. This is the only area where mature, robust and proven effective detection technology exists. Indeed, DOT Europe notes that, as it currently stands, technology to detect new CSAM based on machine learning classifiers requires heavy

[13] See for instance Lee, Hee-Eun; Ermakova, Tatiana; Ververis, Vasilis; Fabian, Benjamin (2020). Detecting child sexual abuse material: A comprehensive survey. Forensic Science International: Digital Investigation, Volume 34, 301022. doi:10.1016/j.fsidi.2020.301022

investment in human reviewers to verify the content. Indeed, these classifiers do not in themselves 'detect' CSAM. Instead, they are trained on the basis of certain classifiers, to flag suspicious content that is likely to contain abusive content, for review and confirmation by human reviewers. While classifiers exist that help companies prioritise content for review, this technology is different to hash matching technology for the detection of known CSAM in that the work of automated detection tools need to be systematically complemented through human review. The technology to detect solicitation remains nascent and particularly challenging as well. This is because no reliable solicitation detection technology exists that allows for an accurate and automated process, requiring limited human review (only for technical/operational purposes), and **it is unclear at this stage whether/when such technology will exist**. Indeed, solicitation is insidious, context-based and by nature difficult to detect. The Regulation expects these maturing technologies to have an unrealistically low false positive rate for the detection of solicitation, which could disincentivise investment and interrupt innovation by service providers. Also considering continuous developments of circumvention techniques, it is important that the Regulation does not inadvertently block the development of new types of detection. The risks arising from testing and refining such technologies can be addressed effectively within Article 4 and appropriate mitigations could be supervised by the relevant Coordinating Authority and Data Protection Authority.

Examples of current practices

Google develops and shares cutting-edge technology, Content Safety API and CSAI Match, free of charge for qualifying organisations to make their operations better, faster and safer, and encourages interested organizations to use these child safety tools to combat child sexual abuse. Content Safety API helps organisations classify and prioritise potential abuse content for review, so they can identify problematic content faster and with more precision so they can report it to authorities as applicable. CSAI Match is an API that helps organisations identify re-uploads of previously identified child sexual abuse material in videos so they can responsibly action it in accordance with local laws and regulations.

Meta developed and open-sourced its photo- and video-matching technologies (TMK and PDQ) so that industry partners, smaller developers and non-profits can use them to more easily identify abusive content and share hashes — or digital fingerprints — of different types of harmful content.

Microsoft's PhotoDNA tool has been in use since 2009 to identify and remove child sexual exploitation and abuse imagery from online platforms and services. PhotoDNA is used by many companies across the industry, including Discord, Google, Snap Inc, Twitter, TikTok and Meta.

As a part of the **Technology Coalition** , Amazon, Apple, Discord, Dropbox, Google, Meta, Microsoft, Snap Inc, TikTok, Twitter and Yahoo actively support an industry initiative launched in 2020 that includes a multi-million-dollar investment into research and innovation to prevent online child sexual exploitation and abuse.

DOT Europe's recommendations

- The Regulation should respect technology neutrality and enable providers to define effective, targeted and proportionate mitigation measures, including detection technologies, to address CSAM on their respective services. This is why DOT Europe welcomes Recital 26 and calls for preservation of language on technological neutrality and tailored solutions in the final text. This approach will allow the Regulation to adapt to new service types and features both now and in the future.
- The Regulation should clearly reflect the differences in maturity of technology to detect known CSAM, new CSAM and solicitation to ensure a proportionate approach that limits the risk of false positives and protects the privacy rights of users.
- Article 19 safeguards designated companies from any related legal challenge related to the use of the new EU Centre's technologies and this provision should be maintained in the final text. Moreover, companies' responsibility should be limited to ensuring deployed technology following a detection order works smoothly.
- More clarity is required when it comes to the timing foreseen to develop the databases managed by the EU Centre and the process for mandating their use and under what circumstances.
- Where the EU Centre develops new technologies, the process should be transparent and industry players should be involved in the stress-testing process, for example by industry experts joining the proposed Technology Committee. Moreover, we recommend continuing to engage with a range of experts to ensure the Regulation balances privacy, safety, and security in a way that can be implemented in practice.
- On the other hand, the Technology Committee should not replicate existing work being done elsewhere, and should take into consideration the great work done by existing groups.
- Novel technologies can initially be less accurate, so the Regulation must be flexible enough to allow such technology to be tested and developed under the Article 3 and 4 risk assessment and mitigation framework, with mitigations supervised by the relevant authorities. This approach recognises that companies are the main source of new technologies and innovation, especially with respect to solicitation and new CSAM, in this space and that the Regulation should not stifle but enable and incentivise beneficial cycles of industry investment and collaboration.
- The Regulation should avoid an overreliance on accuracy of online detection solutions as the metric of effectiveness since testing is often conducted in controlled environments, considering that technology solutions are not at a point where industry can remove the need for human intervention and review.

ISSUE PAPER 4

Scope

Risk assessment and mitigation
Detection orders
Technologies
Scope
EU Centre and global reporting framework

DOT Europe fully supports the objectives of the proposal and maintains that CSA has no place either offline or online. Online service providers have an important role to play to fight against this horrendous crime. That said, it is essential to clarify the scope of the proposal on all levels as the lack of clarity will set false expectations, lead to legal uncertainty and may render the Regulation impossible to implement. We have attempted to identify some of the areas that we believe need to be addressed in greater detail through the negotiations.

Providers in scope of the proposal

While every DOT Europe member is willing to comply with potential obligations of the proposal in an attempt to contribute to bettering the situation, the proposed Regulation needs to reflect the diversity of services and the level of control each has over pieces of content or data. As a result, **different services are not in the same position to undertake detection or act** on potentially infringing content. For example, cloud infrastructure services act as a foundational layer for other companies to run their businesses and often do not contractually have the right to access or control the content. Therefore, the cloud infrastructure service providers may not be in a position to monitor the content and meet the requirements of Article 4 that mitigation measures be proportionate, targeted and effective. Rather, action should be taken at the point closest to the end user i.e. the providers of the services operating on top of cloud infrastructure. The same can be observed when it comes to other types of service providers currently in scope of the Regulation, for example software- and platform-as-a-service providers.

Software application stores are also in scope of the proposal, via Article 6. The related provisions are particularly problematic for two reasons. First, app developers currently rely on consistent and predictable review processes coming from app store providers, which the proposed provisions could challenge given that the disclosure of information regarding impact assessments must be kept to a minimum, for perfectly legitimate reasons. Second, it fundamentally misunderstands the capabilities of app stores that process millions of apps, but do not have any control over content, features and user interactions within an app. The focus of the proposal on solicitation could possibly lead to a situation where an app store would need to prevent children from accessing any app that has functionality where users can communicate. This would have a significant impact on children’s access to digital tools and services and be detrimental to their digital self-determination.

Types of content and conduct in scope of the proposal

The proposed text aims to tackle two different types of malicious content as well as one form of malicious conduct: known CSAM, new CSAM and the online solicitation of minors. While DOT Europe welcomes this comprehensive approach, we also underline that different tools are effective to help prevent, detect and report each[14]. The proposal should reflect the fact that **available technologies are at different stages as to maturity and reliability**. In our paper on detections orders[15] we go into further detail on what this entails and therefore also what the Regulation should take into account.

DOT Europe's recommendations

- The Regulation should enshrine the approach that action should be taken at the point closest to the user i.e. service provider level, so that a provider can adopt a holistic approach to detection and prevention of CSA. Action should only be expected by upstream suppliers as a very last resort. Taking action at the point closest to the user also leads to the most effective enforcement on online CSA, because it is there that the providers have most information on the content and users associated with it.
- The Regulation should recognise that different detection and prevention approaches are effective against known CSAM, new CSAM and solicitation. Providers should be able to select the approach that works best for their respective service(s), with oversight from the relevant Coordinating Authority and DPA. There should be no one-size-fits-all approach.

[14] Please refer to our third issue paper on Technologies.

[15] Please refer to our second issue paper on Detection orders.

ISSUE PAPER 5

EU Centre and the global reporting framework

Risk assessment and mitigation
Detection orders
Technologies
Scope
EU Centre and global reporting framework

DOT Europe welcomes the European Commission's proposal to establish an EU Centre to prevent and counter on Child Sexual Abuse (EU Centre) aimed at fostering cooperation and coordination between companies, non-governmental organisations and national competent authorities and also at supporting of victims and survivors. Despite the many benefits the EU Centre can potentially bring to the fight against CSA, DOT Europe is concerned that several aspects in the proposed text on the EU Centre lack consideration.

First, it is important to mention that **a global framework for the reporting of CSAM is already in place** and works well for participating entities. This global framework is coordinated via the National Centre for Missing and Exploited Children (NCMEC)[16], which analyses and sorts reports and transmits them to the relevant law enforcement agencies, including EU27 countries, to facilitate investigations and prosecutions. Companies based in the United States are legally obliged under US law to report CSAM to NCMEC. This global approach to reporting is helpful for providers which can rely on a single process, allowing them to avoid fragmentation and diversion of costs related to the fight against CSA. CSA is not only a European problem, therefore it **needs to be tackled at the global level** in a comprehensive way, which encourages cooperation with existing entities and streamlines processes.

Secondly, the role of the EU Centre, including in this global reporting framework, is not clear in the proposal. The proposed provisions require companies to report to the EU Centre, even if they are already reporting to other bodies. This **duplication may lead to a fragmentation** both with regards to knowledge and database management, ultimately undermining the fight against CSA. DOT Europe also has some concerns regarding the tasks and powers foreseen for the EU Centre and whether they will lead to the most effective outcomes. For instance, replacing the hash lists developed over many years by companies, NGOs or other entities will be an arduous task for the new EU Centre. Finally, the impact of the duplicated reports should not be underestimated as it could disrupt investigations or lead to a duplication of efforts due to EU law enforcement agencies receiving reports for identical matters from multiple entities, e.g. NCMEC and the EU Centre.

Additionally, there are concerns regarding the **legality of reporting CSAM to the EU Centre under US law**. Since some of DOT Europe's members are American companies subject to US domestic federal law, this issue is of utmost importance and should be resolved before the new rules enter into force. While reporting CSAM to NCMEC under the US Code does not amount to illegal distribution of CSAM[17], reporting CSAM to a new EU Centre would be contrary to US data disclosure laws and could be considered as illegal distribution of CSAM under US federal law. There is no legal immunity from civil

[16] For more information: https://www.missingkids.org/HOME

[17] U.S. Code § 2258A - Reporting requirements of providers, available at https://www.law.cornell.edu/uscode/text/18/2258A

claim or criminal charge for distribution of CSAM to an EU Centre under US CSAM reporting laws. The issue of the conflict of law with the US and of the interplay between NCMEC and the EU Centre is not at all addressed in the proposal and could create problems if not addressed in the final text. Issues arising from conflict of law with the US and double reporting obligations would be particularly problematic in cases falling under multiple jurisdictions (i.e. with a victim in the US and abuser in the EU and vice versa).

Lastly, the **powers of the EU Centre lack clarity** in the proposal. Article 49 grants the EU Centre the power to conduct searches on hosting services for the dissemination of "publicly accessible CSAM". While we appreciate the role of the EU Centre to avoid revictimization and the absolute need to support victims, more detail would be welcome as regards the methods employed and the extent of these searches. It seems reasonable that a judicial order be obtained to conduct these searches and that providers be notified before the searches happen, and not after as is suggested in Art. 49(2), in order to maintain a collaborative relationship between the providers and the EU Centre.

Examples of current practices

Amazon, Apple, Discord, Dropbox, Google, Meta, Microsoft, Snap Inc, TikTok, Twitter and **Yahoo** are members of the Technology Coalition which is focused on expanding the number of firms doing voluntary efforts against CSA, informing development of new technology, maintaining law enforcement dialogue and championing industry transparency initiatives.

In 2020, members of the Tech Coalition came together to announce Project Protect: A plan to combat online child sexual abuse – a renewed commitment and investment expanding the Tech Coalition's scope and impact to protect children online and guide its work for the next 15 years.

In August 2019, NCMEC launched an updated Case Management Tool, funded by Facebook (now **Meta**) and developed with guidance and direction of its engineers. The tool is now available to law enforcement around the world making it easier for law enforcement to access reports in order to prioritise and respond to reports of child sexual exploitation. In the same year, Meta launched Stop Sextortion, a dedicated hub in its Safety Center, developed by Thorn, a leading NGO in the fight against child sexual abuse, with resources for teens, caregivers and educators seeking support and information related to sextortion.

The **Tech Coalition** issued a report in January 2022 outlining how the reporting framework works for US companies.

Discord sponsors the Family Online Safety Institute Conference, Trustcon (the first global conference dedicated to trust and safety professionals) as well as the Digital Wellness Lab.

Google launched a dedicated transparency report on Google's efforts to combat online child sexual abuse material, detailing, among other things, how many reports it made to NCMEC, URLs de-indexed from Search, accounts disabled for CSAM violations, and CSAM hashes contributed to the NCMEC industry database. Google also conducts periodic training to law enforcement on its CyberTip reporting and data disclosure practices, which can assist law enforcement in their follow-on child safety investigations.

Snap Inc uses industry-leading tools to detect, report and remove both images and videos containing this type of content immediately to NCMEC. Snap Inc chairs WeProtect Global Alliance's Private Sector Reference Group and firmly believes that collective action is key to meaningful and measurable progress in the fight against child sexual exploitation and abuse online.

Twitter, TikTok, Spotify, Snap Inc., Microsoft, Google, Meta, Dropbox, Apple and **Amazon** are members of the WeProtect Global Alliance, created in 2020, which brings together governments, the private sector, civil society and international organisations to develop policies and solutions to protect children from sexual exploitation and abuse online.

Meta has a Safety Advisory Board of leading online safety non-profits, as well as over 400 safety experts and NGOs from around the world, who provide guidance and expertise on Meta's policies, products and tools. **TikTok**'s own European Safety Advisory Council includes leading external subject matter experts on technology-mediated crimes against children. Since 2018, **Snap Inc**'s Safety Advisory Board (SAB) - now a group of online safety-focused non-profits and related organizations, technologists, academics, researchers, and survivors of online harms - has been providing critical feedback on fostering the safety and well-being of the Snapchat community. Snap recently expanded its SAB to include a wider diversity of geographies, safety related disciplines and expertise.

DOT Europe's recommendations

- DOT Europe believes it is essential that policy-makers acknowledge the already well-established and well-functioning reporting processes in place today. We recommend to build on what is already in place and not to disrupt the mechanisms which are working very well to report CSAM and support law enforcement investigations.
- Policy-makers should clarify how the EU Centre will interact with the existing global cooperation network, establish consistency and avoid unnecessary overlap, notably in reporting requirements.
- The final text should also make clear that service providers are able to use other indicators developed by institutions, NGOs or industry for detection-purposes in Europe and not only be restricted to the use of the indicators provided by the EU Centre.
- The proposal should as a matter of priority address the potential conflict of law affecting US firms which are banned from transmitting CSAM to an EU Centre in the way proposed in the Regulation.
- Dual reporting to NCMEC and the future EU Centre should be avoided or mitigated to the maximum extent possible. A failure to do so would result in an inefficient duplication of efforts by NCMEC, the EU Centre as well as companies, which would ultimately slow down investigations, to the detriment of children.
- If a requirement to report to the EU Centre is maintained, a practical framework should provide clarity on how to distinguish between reports relating to EU offenders and/or victims that should be filed with the EU Centre and reports relating to, for example, U.S. offenders and/or victims that should be filed to NCMEC. A failure to address this issue would result in uncertainty for agencies such as NCMEC and the future EU Centre, law enforcement authorities, as well as companies.
- An effective framework should avoid duplication of efforts, by allowing the future EU Centre to exchange information with entities such as NCMEC to perform effective deconfliction, as well as by ensuring alignment between reporting flows.
- DOT Europe would also welcome more clarity on the powers granted to the EU Centre as regards search on hosting providers' services as well as more detail on what would constitute a search. DOT Europe also advocates for the EU Centre to obtain an order from a judicial authority before being able to conduct these searches.