DIGITALEUROPE

31st AUGUST 2022

Creating an effective framework for combating child sexual abuse and exploitation online

Executive summary

DIGITALEUROPE fully supports the European Commission's goal to create a comprehensive legislative framework that involves the tech sector, government and civil society to ensure better protection of children against sexual abuse and exploitation.[1]

Our members play an important role in the battle against this horrible crime and take this responsibility seriously. They have carried out extensive work to fight child sexual abuse and exploitation online, including developing technology vital to the detection, removal, reporting and prevention of this material.

The detection and removal of illegal material online is only one element of this fight. The work to keep children safe online requires a holistic approach – with an equal focus on prevention, in addition to detection. This includes developing tools that help ensure that when children use technology, access content and interact with others, it is done in a safe, secure and private environment.

To this end, the final Regulation should:

- Provide appropriate derogations from the ePrivacy Directive that are not contingent on receiving detection orders.[2] This will allow providers to continue to expand on their voluntary efforts with sufficient legal certainty and without fear of liability;
- Focus its scope on capturing services that present a high risk of abuse, taking into account their technical and contractual capabilities, particularly in relation to business-to-business (B2B) and infrastructure services;

[1] COM/2022/209 final.

[2] Directive 2002/58/EC, as modified by Directives 2006/24/EC and 2009/136/EC.

- Enable detection of unknown material and grooming on a voluntary basis, with appropriate safeguards, given that existing technology remains insufficiently developed and inaccurate. This also applies to age verification;
- Avoid transparency requirements that could help bad actors avoid detection and result in key evidence being destroyed;
- Provide a clear stipulation that the requirements apply without prejudice to end-to-end encrypted communications; and
- Ensure that the EU Centre can act transparently and independently from law enforcement, and that the EU and US can promptly engage in a dialogue to ensure legal disclosure in both jurisdictions.

Table of contents

- Executive summary 1
- Table of contents 3
- Legal basis for voluntary detection 4
- Scope 4

B2B services 4

Infrastructure services 5

App stores 6

- Risk assessments 7
- Detection orders 7
- Grooming 8
- Encrypted communications 8
- Age verification 9
- Transparency requirements 9
- EU Centre 10

Independence 10

Hash databases 10

Interplay with the global framework 11

Legal basis for voluntary detection

The proposal allows hosting service providers to continue to carry out voluntary measures without a detection order. However, interpersonal communications services (ICS) would not be able to carry out voluntary measures without a detection order.

Under the current voluntary system, DIGITALEUROPE members have invested heavily in developing state-of-the-art technology that has helped detect and report an increasing amount of child sexual abuse material (CSAM) worldwide, resulting in tens of millions of reports to authorities worldwide last year alone.[3]

In addition to detection, our members have also developed a range of risk-mitigation and safety-by-design tools designed to help prevent child sexual abuse from happening in the first place. This progress has been made thanks to the strength of the current system of voluntary industry-led measures.

The final Regulation should provide appropriate derogations from the ePrivacy Directive that are not contingent on receiving detection orders. This will allow providers to continue to expand on their voluntary efforts with sufficient legal certainty and without fear of liability.

By contrast, the need to wait for the issuance of a detention order will discourage innovative, proactive efforts in ICS or on-device detection that may prove key in this nascent area.

Scope

In order to ensure proportionality, the final Regulation should capture services where there is a high risk of abuse, based on empirical evidence and taking into account a service's technical and contractual capabilities.

B2B services

The proposal appears to impose obligations equally on data controllers and data processors by extending detection and monitoring requirements to providers of all 'hosting services' and 'interpersonal communication services.'[4] This appears to require data processors to monitor accounts of their enterprise

[3] NCMEC, *CyberTipline 2021 Report,* available at https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.

[4] Defined, by reference to the Digital Services Act (DSA, COM/2020/825 final), as a 'service that consists of the storage of information provided by, and at the request of, a recipient of the service.' For 'data controller' and 'data processor,' we use the definitions contained in the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679).

customers, including commercial, business and public sector enterprises such as governments and academic institutions.

Enterprise customers consider secure communications to be vital to protect their assets from theft and cyberattacks. Any obligations for the service provider to scan their secure communications or services would be disproportionate given the lack of evidence that B2B services pose any significant risk for dissemination of CSAM, and would create security risks for European businesses and organisations.

To this end, the final Regulation should make it clear that obligations are limited to data controllers, and do not apply to data processors. This will ensure that such obligations can be met by the most appropriate actor.

Establishing a role for the data controller (e.g. enterprise customer) does not absolve the data processor (e.g. service provider) of its responsibilities. Under the final Regulation, the obligations for service providers acting as a data processor should be limited to proportionate and reasonable measures. This can include requests for engagement and coordination with non-compliant entities to facilitate the expedient removal of CSAM all the way up to discontinuing services or reporting customers when the data processor is notified or becomes aware of clear evidence that the data controlling customer is not complying with its own obligations.

The service provider should also provide appropriate tools and settings to support its enterprise customers to assess and mitigate risk, and detect and report abuse. However, responsibility to fulfil the provisions (age verification, detection, reporting, removal) is with the data controller (e.g. enterprise customer), not the service provider acting as a data processor.

The data controller has a trusted relationship with end-users and is better placed to understand risk according to the context. For example, if an ICS is used in an office environment, the IT administrator is aware of the identities of end-users. As such, with the support of appropriate tools, it will be able to detect and review potential abuses without general monitoring by the service provider. The IT administrator is better placed to determine context and improve accuracy by not reporting false positives. Additionally, it may be able to verify the age or age groups of users, without recourse to an age verification mechanism established by the provider. The service provider is unlikely to have this user information, in part for reasons of personal data minimisation in line with the GDPR.

Infrastructure services

This broad scope of ‘hosting service providers’ would also impose obligations on services deeper in the internet stack, such as cloud infrastructure service providers, failing to recognise that they are extremely limited in what they can (and should) do with the data controlled by their customers.

Infrastructures services like cloud infrastructure providers are the ‘building blocks for IT’ and offer services that include compute power, and database storage. As a technical and contractual matter, infrastructure service providers often do not have visibility into or control over the specific items of content that their customers store and share on their services. Data controllers, who are in closer proximity and control over data, are hence better suited to comply with detection orders. Therefore, in the final Regulation, detection obligations should be limited to data controllers and not apply to technology providers providing data processing services.

For removal orders, a ‘cascade approach’ should be introduced, where parties who are closest to the content, and whose services allow for the precise and limited removal of the content in question, are approached in the first instance. This will ensure that such obligations can be met by the most appropriate actor and as swiftly as possible without the need for redirections. Infrastructure providers are often unable to remove or block specific content, and having to do so may force them to remove lawful content from thousands of users or take down entire services.

The e-evidence proposal provides guidance on which service provider law enforcement authorities should contact first to issue removal orders.[5] It clarifies that when data is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, the order must be directly addressed to the company or entity (data controllers) unless there is risk of jeopardising the investigation or in case the data controller cannot be identified.

App stores

The proposal also introduces specific obligations for app store providers to assess, mitigate and report on risks posed by ‘each service offered through the apps’ they intermediate, and to take reasonable measures to prevent child users from accessing applications where there is a significant risk of use of the service for grooming of children.

These extensive obligations are unclear, possibly excessive and difficult to evaluate. They also do not recognise that most apps are created by third-party developers who retain control over the functioning of the application, not by the provider of the app store. The concept of ‘reasonable efforts’ and ‘reasonable measures’ is inherently vague. Moreover, these obligations would require app

[5] COM/2018/225 final.

stores to specifically collect personal data to certify that users meet the age threshold, and to monitor users’ activities to ensure their access to apps is age appropriate.

Risk assessments

We welcome the proposal’s risk-based approach, designed to allow providers to evaluate the specific risks of their services and to establish appropriate mitigation strategies tailored to their services.

However, more clarity is needed as to the interplay between the risk assessment and mitigation requirements and the related obligations under the DSA. The DSA also requires very large online platforms and very large online search engines to identify, analyse, assess and mitigate systemic risks their services pose to the protection of children. In order to avoid duplication, we recommend guidance on how the risk assessment conducted for one purpose would also suffice for the other.

Detection orders

While we welcome the safeguards attached to detection orders, including judicial review, they must be proportionate and effectively protect the privacy of all users. Detection orders must also be consistent with the recently reconfirmed principle in the DSA that prohibits general monitoring obligations.

We are concerned by the requirement to extend the detection obligations to unknown material and grooming. We believe this should be left to voluntary measures, with appropriate safeguards.

While the detection of known CSAM requires matching against established hash databases, detecting not previously known CSAM and grooming relies on classifiers and AI to detect content. Although these classifiers are continuously improving, they remain unreliable, leading to more challenging enforcement than for known imagery.

Reliance on such technology, in the absence of human eyes on each and every image, is likely to result in very high numbers of incorrectly identified materials being reported, and the potential for many false accusations against innocent users, with serious real-world consequences and interference with their privacy and data protection rights.

The high numbers of incorrectly identified materials would also have an adverse impact by creating a backlog of reports, therefore unnecessarily hindering the work of officials in combating child abuse.

Grooming

We recognise the increased targeting of children online for the purpose of sexually exploiting them and encouraging the production of self-generated CSAM.

The response to the risk that children are groomed for sexual purposes requires a comprehensive approach that focuses on developing safer and more age-appropriate experiences for children, educating users, and mitigating the risk factors that lead to an environment where grooming can occur. Focusing on identifying high-risk contacts once they have taken place is too late and is a strategy with significant privacy implications for all users.

Existing technology for detecting grooming conversations based on natural language processing is not sufficiently developed and accurate, and its deployment at scale could risk the privacy of all users who rely on the service – the vast majority without engaging in any unlawful practices.

The final Regulation should instead focus on enabling voluntary technological innovation in this space to take place, including by allowing for the use of metadata to help identify potentially problematic behaviours. Building on safety-by-design principles, this voluntary approach can help minimise children's exposure to online harms.

Encrypted communications

In developing a long-term framework to fight CSAM, policymakers should clarify how to effectively keep children safe while preserving other pressing fundamental rights. Essentially, the framework should both protect users and acknowledge the need to safeguard privacy and cybersecurity, including end-to-end encrypted communications.

Encryption plays a crucial role in providing private and secure communications that users, including children, demand and expect to keep them safe online. Even well-intentioned efforts to provide a lawful intercept solution in end-to-end encryption can undermine critical security benefits by making all users of such services more vulnerable to malicious attacks.[6]

[6] For more on the crucial role of encryption, see DIGITALEUROPE, *Encryption: finding the balance between privacy, security and lawful data access*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/03/DIGITALEUROPE-Position-on-Encryption-Policy-.pdf.

We are concerned that the current proposal constitutes a significant risk to encryption, and therefore urge a clear stipulation that the final Regulation applies without prejudice to end-to-end encryption technology.

The legislation should allow for the use of behavioural information and metadata signals, which can be deployed to detect behaviours that may be putting children at risk. Legislation should facilitate innovation and voluntary efforts to develop in this nascent space.

Age verification

The proposal effectively requires providers to verify the age of users in ICS and app stores where there is a risk of the service being used for the grooming of children. To establish the risk of grooming, the provider needs to know the extent to which its services are used by children and the provider must adopt age verification as a mitigating measure.

The technology for establishing the age of users with a high degree of confidence, especially at a granular level for users under the age of 18, remains imprecise.

This is an emerging area with no identified best practice as yet, with privacy-protective techniques still being established. Certainty, or a high degree of accuracy, about age would require providers to collect a substantial amount of private data from all users and track the activities of all children to ensure their access is age appropriate.

If not designed carefully, requirements to verify users' age can risk the exclusion of certain groups, especially the most vulnerable, who may lack the required form of identification or may be unable or unwilling to share that information. The proposal also fails to address the shared responsibility of the app developers themselves in ensuring age-appropriate access to their services.

Transparency requirements

The fight against child abuse and exploitation is a fast-moving space, with perpetrators constantly updating their methods and looking for ways to bypass protections. While we recognise the importance of transparency, the proposal risks tipping the balance and rendering existing technology and protections ineffective.

For example, we are concerned that obligations to provide information to users outlining the detection technology and how it works within the transparency report could help bad actors avoid detection and result in key evidence being destroyed, jeopardising the ability to combat this crime.

The proposal requires providers to provide a detailed notice to the reported user if they don't hear back from the EU Centre within three months of making a report. Three months is insufficient time for law enforcement authorities to initiate, investigate or close a case. There remain tip-off concerns and potential impediment of an ongoing criminal investigation. Decisions about when and how to inform users about a CSAM report should therefore be a matter for law enforcement and social care authorities in Member States, and the final Regulation should relieve providers of this responsibility.

In addition, any obligation to report on the risk assessment and mitigation measures results should be limited to the Coordinating Authority of the Member State of establishment and the EU Centre. Making such information publicly available would enable bad actors (including perpetrators) to circumvent systems service providers have put in place to keep children safe and to migrate to other services. In this regard, Art. 5 of the final Regulation should make clear that the obligation under Art. 33 DSA, which requires reports on risk assessment, mitigation measures and related audits to be made publicly available, does not apply in the context of CSAM.

EU Centre

We support the Commission's proposal to strengthen the European infrastructure and capacity to fight against child sexual abuse and exploitation. The EU Centre on Child Sexual Abuse, if sufficiently resourced, can help strengthen the EU-level response against this crime, focus on prevention, support victims, ensure better coordination between Member State and international authorities, and help develop and share best practice across relevant service providers.

Independence

While we appreciate that the EU Centre is designed to be an independent entity, its proposed close ties to Europol, Coordinating Authorities and the Commission, and its plan to develop a hash database directly from Member State governments raises concerns about transparency and the independence of the system. The draft Regulation should therefore clarify how the EU Centre will operate at arm's length from law enforcement.

Hash databases

We would welcome language clarifying that industry will be able to continue using high-quality hash databases and AI classifiers for detecting CSAM – such as those provided by the National Center for Missing & Exploited Children (NCMEC) in the US, Thorn, the Internet Watch Foundation and developed by industry – and will not be obliged to utilise specific databases maintained by the EU Centre.

The final Regulation should also provide clarity as to liability where providers use databases and other technology developed by the EU Centre, particularly where technology is new and experimental. In this vein, the EU Centre should also regularly consult with industry to support its work on making technologies available.

Interplay with the global framework

The requirement to report detected CSAM content to the EU Centre creates a conflict of laws for US-established companies, who are currently legally required to report to the NCMEC when they become aware of CSAM on their platforms. Their ability to disclose the contents of a report elsewhere is proscribed by US statute.

Before the EU Centre establishes its reporting requirements, we encourage the EU and US to engage in a dialogue to ensure that any services would be allowed to disclose to the EU Centre without falling foul of US law. Additionally, the NCMEC and EU Centre reporting flows need to be streamlined to ensure effective follow-ups to combat child sexual abuse online. Under the proposal, there could be situations where the reports get sent to different places by NCMEC and the EU Centre, leading to dual and potentially uncoordinated investigations, as well as duplicative efforts by providers.

FOR MORE INFORMATION, PLEASE CONTACT:

Hugh Kirk
Senior Manager for Digital Commerce Policy

hugh.kirk@digitaleurope.org / +32 490 11 69 46

Alberto Di Felice
Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world’s largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world’s best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Banco Santander, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK