DIGITALEUROPE

04 March 2021

Position paper on the EU strategy for combating child sexual abuse and exploitation

Executive Summary

DIGITALEUROPE's membership fully supports the European Commission's efforts to strengthen the fight against child sexual abuse and exploitation in Europe.

Our members have undertaken extensive work to fight child sexual abuse online, including developing specific technology that plays a key part in the detection, removal and reporting of this vile material. Our members support law enforcement and civil society organisations and have forged important industry partnerships, such as the Technology Coalition, to facilitate the collective response against this crime.

In developing a long term framework in the fight against child sexual abuse, it is important that European policymakers carefully consider how the strategy fits with the wider legislative framework and in particular the Digital Services Act proposal. Policymakers should also use this as an opportunity to clarify how to effectively support both the need to keep children safe and the preservation of fundamental rights, like the right to privacy, and develop a framework that is able both to protect users (including children) and acknowledge individual rights to privacy.

The fight against child sexual abuse and exploitation is a global fight that involves governments, law enforcement agencies, civil society, communities and, of course, companies. DIGITALEUROPE's members acknowledge their important role in this fight and take this responsibility seriously. A well-rounded strategy needs to consider the role that everybody has to play in the fight against this crime and focus on how we can all better work together. For example, the system should effectively support the focus on detection with an equal attention to the importance of prevention and be complemented with more investment and support to law enforcement and a strong package of support for victims.

DIGITALEUROPE is committed to the fight against child sexual abuse and exploitation and is looking forward to working with the EU Institutions to help design a framework in Europe that contributes to eradicating this egregious content from our services.

To this end, we would like to outline - for your consideration - a few elements we believe are important in future legislation.

Table of Contents

Consistent application of existing rules

DIGITALEUROPE agrees with the Commission that there is lack of consistency and coordination in the fight against child sexual abuse across Europe. Efforts are fragmented, duplicated, and/or insufficient in some areas, as shown in particular by the monitoring of the implementation of the Child Sexual Abuse Directive (Directive 2011/93). In particular, the Commission highlights that "*the efficiency and effectiveness of Member States' efforts to assist victims of child sexual abuse is limited as they do not systematically make use of existing best practices and lessons learned in other Member States or globally*".

It is important to understand the lack of success in implementing the existing rules and, in particular, the barriers for Member States to transpose and implement the existing Directive. We need to avoid the risk of developing an additional framework that fails to address the underlying barriers to implementation that, in an attempt to solve this important issue, creates another layer of legislation that fails to dent the problem, and, worse, makes the problem even more difficult to solve.

Consistent and up to date definition of online child sexual exploitation and abuse

The strategy offers a good opportunity for the European Commission to develop a consistent and up to date set of definitions of child sexual abuse that reflects the reality of the crimes we are trying to tackle.

The Child Sexual Abuse Directive continues to talk about "child pornography", pornographic performance or child prostitution. Organisations working with victims of child abuse have long advocated for that terminology to be abandoned as it equates what is effectively the sexual abuse of children with a legal voluntary practice, failing to recognise that children cannot consent to these activities. Referring to child sexual abuse and exploitation or to child sexual abuse material is currently the preferred terminology as it reflects both the sexual and abusive nature of the crime.

Further, there is growing recognition that in order to stop these crimes, we need to ensure that children are not groomed by adults for sexual purposes. The definition in the Directive of solicitation of children for sexual purposes (Article 6) needs to be updated to reflect the current understanding of the process that may lead children to produce and share sexual material with abusive adults, plus recognition that the devastating effects of grooming can occur without an actual meeting.

Consistent definitions that reflect the current understanding of the nature of the crime will facilitate greater protection of children.

Proportionate regulation that encourages innovation

Regulation should reduce barriers to innovation, improve existing detection technologies, and adoption of these technologies, particularly by smaller online platforms and services. Providing supportive mechanisms for companies to share best practices will also encourage engagement across a wider spectrum of services.

Any framework should not proscribe which technology can be used and should account for both existing and emerging techniques to tackle abuse, such as using behavioural signals and traffic data in line with the evolving nature of the threat.

The framework should also reflect the varied and dynamic nature of online communications so we would advise against a one-size-fits-all solution. Policymakers should consider the nature of the underlying service, users' expectations in using the service, especially around privacy, and the various features or facets of the service in any definition, carefully limiting and tailoring in ways that recognise relevant differences between services.

DIGITALEUROPE urges the Commission to ensure that the framework takes into account important differences between services. For example, cloud infrastructure service providers in particular act as an initial layer of foundational infrastructure and enable customers to build and run their own cloud-based IT systems which the latter then design, control and manage. The cloud infrastructure service providers cannot access or control specific pieces of content, only the customer has this technical ability. If a cloud infrastructure service provider were ordered to remove a specific piece of content, it would have to remove all the customer's data on that service, meaning that lawful content from other users would also be removed.

Focus on strengthening voluntary measures

We disagree with the Commission's starting point that "current absence of legal obligations to detect and report child sexual abuse online results in a lack of clarity and certainty for the work of both law enforcement and relevant actors in the private sector". Under the current voluntary system, DIGITALEUROPE members have invested heavily in developing state-of-the-art technology that has helped us detect and report an increasing amount of child sexual abuse images worldwide. This progress has been made thanks to the strength of the current system of voluntary measures which supports providers to detect content without fear of losing liability protections.

In 2020, the National Centre for Missing and Exploited Children (NCMEC) received 21.7 million reports, a 28% increase compared to 2019. Over 170 companies reported content to NCMEC over this period[1]. The volume and spread of reports has been made possible by the investment in technology and the commitment of our members to tackle child sexual abuse in their platforms.

We recommend that the Commission focus its efforts on strengthening a system that encourages and does not penalise providers' voluntary efforts, consistent with the eCommerce Directive and the upcoming Digital Service Act. It should also strengthen the provisions that protect online platforms from liability and incentivise them to undertake certain proactive measures to protect users against illegal content.

We understand that the Commission is considering a system for the mandatory detection of child sexual abuse material. While obligations to detect known and even unknown CSAM can be seen as the solution to address inaction by some providers, these measures need to be considered as part of the wider regulatory framework, as it is currently being developed as part of the Digital Services Act and taking account of obligations in the General Data Protection Regulation and the Charter of Fundamental Rights. A system that imposes the detection of CSAM on providers constitutes a radical departure from the principle of no mandatory general monitoring on providers.

Further, in considering mandatory detection requirements for known CSAM, the Commission needs to consider how the system would work in practice. For example, how known CSAM would be defined, how hash information would be collected and shared across industry and how the system would be maintained and monitored. While companies have developed robust technology to allow hash matching detection, the wider infrastructure to detect known CSAM is not well developed and would need to be in place before any requirement is considered.

There are questions of jurisdictional incompatibility and unintended consequences also to be assessed in relation to the introduction of mandatory requirements to detect known CSAM.

The requirement to extend the obligation also to unknown material suffers from additional problems. As it stands today, this requirement would be technically impossible for most companies. The detection of not previously known child sexual abuse material relies on classifiers to help detect content that is likely to

[1] NCMEC (2021) 2020 Exploitation Stats

contain child sexual abuse material that is then prioritised for human review. Even with the most sophisticated classifiers, large quantities of photos and videos would need to be checked by human reviewers to confirm that they contain child sexual abuse material. This is beyond the capability of most small and medium-sized companies.

The role of the European Centre in receiving reports of child sexual abuse

We support the Commission's proposal to strengthen the European infrastructure to fight against child sexual abuse and exploitation. The creation of a centre covering law enforcement, prevention and victim support at the EU level would be of high value in the fight against this crime. If sufficiently resourced, it could contribute to providing a coordinated response to what is by nature, a global crime.

The Commission specifically sees a role for the centre supporting the mandatory measures under consideration, with the centre potentially receiving reports of child sexual abuse material from providers.

In considering options for the centre and its role, the Commission needs to ensure that the proposed system does not undermine the existing processes for the reporting of CSAM currently in operation, with many companies globally reporting to the National Centre for Missing and Exploited Children (NCMEC). In a world of limited resources, the Commission also needs to consider the impact of the different options on providers and institutional resources and how they can be deployed to maximise the protection of children.

Over the years, NGOs, law enforcement, and providers worldwide have invested in making this system work in the fight against this global and borderless crime. It is often difficult for a provider to establish the geographic provenance of a particular CyberTip, for example where a victim or offender is located: the individuals sharing the content may be in different parts of the world, sharing collections involving children from all over the world.

When NCMEC receives CyberTipline reports concerning child sexual exploitation incidents that originate from outside the United States, its primary goal is to make the report available to an appropriate law enforcement agency for further review and potential investigation so the child can be recovered and/or safeguarded. As stated in the NCMEC response to the Inception Impact Assessment, NCMEC has partnerships to provide CyberTipline reports via secure mechanisms to law enforcement agencies in more than 130 countries and territories worldwide. Every EU Member State receives CyberTipline reports either directly from NCMEC or through NCMEC's partnership with Europol. In addition, NCMEC has a partnership with Interpol that enables sharing elements of CyberTipline reports with National Crime Bureaus (NCBs) in any country not covered by a direct connection with NCMEC.

NCMEC has also invested in developing a robust infrastructure that enables companies worldwide to report child sexual exploitation incidents to the CyberTipline easily. Currently, several companies outside the US already utilise NCMEC's CyberTipline to report child sexual abuse content on their systems.

In designing the European centre and its potential role for the reporting of CSAM, we urge the Commission to consider how to build on the existing well functioning system and avoid a situation where providers must duplicate efforts, which reduces efficiency, wasting limited resources and undercuts providers' efforts to combat this crime. It should also have regard to NCMEC's deconfliction service to prevent law enforcement from disrupting existing investigations.

Further, the Commission needs to avoid creating a conflict of laws. For instance, US-established companies are legally required to report to NCMEC when they become aware of CSAM on their platforms. Their ability to disclose contents in a CyberTip report elsewhere is proscribed by US statute. The US and EU would need to engage in a dialogue to ensure that any services would be allowed to disclose to a European centre without running foul of US law. Any requirement to report to a European based centre needs to take this into account.

The role for the European Centre in supporting the wider infrastructure

The European Centre can play a key role in the fight against child sexual abuse and exploitation if designed to complement and build upon the existing infrastructure of NCMEC, the wider INHOPE network, related non-governmental organisations working on the prevention and support of child sexual abuse victims as well as Europol, national law enforcement and providers.

In particular, the centre can, among other things, play a role as a centralised hub for:

- sharing good practices to help the detection of child sexual abuse material;
- collecting and sharing information on the prevalence of child sexual abuse in Europe;
- coordinating victim identification efforts;
- leading the prevention and education efforts and increase public awareness in the fight against child sexual abuse; and

- coordinating victim support and providing training and funding for those working with child victims.

Legal certainty for the processing of personal data

According to NCMEC's figures, over the past two years, more than 5.3 million child sexual abuse images and videos reported to NCMEC originated from an offender in the EU, with over 95% of these images shared by EU offenders from an email, chat, or messaging service.

The debate surrounding the introduction of the European Electronic Communications Code (EECC), which brings number-independent interpersonal communication services (NIICS) under the scope of the ePrivacy Directive, has highlighted the importance of providing an explicit legal basis to enable private communications services to tackle child sexual abuse and exploitation, including through processing traffic data.

The proposed temporary derogation from certain provisions of the e-Privacy Directive for combatting child sexual abuse material online (the "interim derogation") is a good first step. Still, it needs to be designed in a way that provides legal certainty for providers to continue to voluntarily tackle child sexual abuse in the context of private communications.

The proposed temporary derogation is, by design, interim, and as such, limited in time. The sector would benefit from greater clarity to continue to tackle the problem of child sexual abuse and reduce its prevalence in private communications. This needs to be done in a way that respects the privacy of users and victims, does not create additional barriers for providers that can discourage them from addressing this problem in the first place, and fosters the necessary innovation that plays such an essential part in the fight against CSAM.

Additionally, legal clarity is needed for companies that are required to retain CSAM imagery for reporting to and preserving this content for law enforcement investigations.

Finally, we caution against promoting CSAM detection solutions that could undermine strong privacy and security protections, including end-to-end-encrypted (E2EE) communications. DIGITALEUROPE supports the importance of preserving E2EE to ensure private and secure communications that our users demand and expect, and that the UN has recognised as a fundamental component of free expression in the digital age[2]. At the same time, we are

[2] UN (2015) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

mindful of our responsibility to tackle child sexual abuse and exploitation on our platforms.

We want to engage with the EU institutions to develop a regulatory framework that effectively enables providers to protect children and uphold the privacy and security of all our users. End-to-end encryption is a vital tool to guarantee users' secure and confidential communications, including that of children, and its integrity should be safeguarded and not weakened.

FOR MORE INFORMATION, PLEASE CONTACT:

Hugh Kirk

Policy Manager

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

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, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20