



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

ISSUE PAPER 5

EU Centre and the 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)¹, 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.

¹ For more information: <https://www.missingkids.org/HOME>





While reporting CSAM to NCMEC under the US Code does not amount to illegal distribution of CSAM², 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 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.

² U.S. Code § 2258A - Reporting requirements of providers, available at <https://www.law.cornell.edu/uscode/text/18/2258A>





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.