December 2022

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

ISSUE PAPER 4

Scope

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.

Rue du Trône, 60, 1050
Brussels, Belgium
Tel: +32 (0) 472 26 83 02

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

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[1]. The proposal should reflect the fact that available technologies are at different stages as to maturity and reliability. In our paper on detections orders[2] 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.

[1] Please refer to our third issue paper on Technologies.
[2] Please refer to our second issue paper on Detection orders.