Joint industry statement on the proposal for a Regulation laying down rules to prevent and combat child sexual abuse

April 4th, 2023

The undersigned industry associations (ACT, CCIA Europe, CISPE Cloud, Dot Europe, eco, EuroISPA, FiCom, ISPA Austria and ITI) and their Members are deeply committed to making the digital space safe for everyone and, in particular, to protecting children online. We firmly support the Commission's objective to prevent and combat any type of child sexual abuse. However, we believe certain obligations and measures included in the proposal for a Regulation laying down rules to prevent and combat child sexual abuse need further reflection and amendment in order to achieve the Regulation's goals. We have listed below our main recommendations on key aspects of the proposed Regulation and remain open to discussing them further with the EU Institutions and parties involved.

1. Scope and definitions:

- The scope of the proposed legislation should be narrowed to focus on service providers that are best placed to take effective mitigation and enforcement measures. Therefore, the proposed legislation should focus on capturing services that present a high risk of abuse, taking into account the technical and contractual limitations of different services.
- As such, number-based interpersonal communication services (NB-ICS) and cloud infrastructure services should be excluded from the detection obligations of the scope, as they play little to no role in the proliferation of child sexual abuse material (CSAM) and grooming.
- Additionally, the proposed obligations on app stores to take 'reasonable efforts' to assess whether each app presents a risk for solicitation of children and to take 'reasonable measures' to prevent children from accessing such apps by means of age verification and age assessment measures might not lead to the desired outcome. App stores are not best placed to assess this risk as they are not privy to the inner workings of each app and, even with access to the developer's risk assessment, it will not be possible for the app store provider to conclude whether the app's mitigation measures are effective at managing the risk of solicitation of minors.

2. Risk assessments, mitigation and reporting:

- We appreciate how the risk assessment of this Regulation takes into account differentiated services and their contrasting realities. This is outlined in Recital 5 of the Commission proposal. We urge the introduction of delineated measures in the risk assessment framework depending on the nature of services and their features.
- The risk mitigation efforts recognised by the proposed CSAM Regulation should be broader and include voluntary efforts carried out proactively by the industry, including prevention work.

  Such efforts should also be allowed for number-independent interpersonal communication services (NI-ICS), through the adoption of a robust legal basis to process communications data for the purpose of detection and prevention of child sexual abuse, with all the appropriate safeguards.

- More clarity is needed as to the interplay between the risk assessment and mitigation requirements of the Regulation and the related obligations under the Digital Services Act (DSA). To avoid duplication, the European Commission should provide specific guidance on their interrelation. Safeguards with regards to the issuance of detection orders need to be further strengthened by adding clear substantive norms, such as the notions of 'significant risk' and 'appreciable extent'.
- The proposed CSAM Regulation should clarify how risk assessment and mitigation measures can be carried out consistently within the limits of the General Data Protection Regulation (GDPR), including the ‘data minimisation' and 'purpose limitation' principles.

3. Voluntary measures:

- The tech industry has long been active in the defence of child safety online. Under the current voluntary system, providers have invested heavily in developing state-of-the-art technology that has helped to prevent, detect, report and remove an increasing amount of child sexual abuse online worldwide. This progress has been made thanks to the strength of the current system which supports the voluntary detection of content by providers.
- Providers of ICSs are concerned that there is no operational plan to transition from the current ePrivacy Interim Derogation, which allows voluntary scanning, to the proposed CSAM Regulation, which would allow scanning on ICSs only with a detection order. This can create a gap in the safety of children online, due to the lack of an explicit legal basis in the Regulation. The issuing of detection orders would follow a lengthy procedure of checks and balances, which would likely lead to a lengthy period of inaction and thus a lack of children’s protection in ICSs during that time.
- Allowing voluntary detection and prevention efforts as a mitigation measure would provide vital continuity in the protection of children and the detection of crime by avoiding uncertainty around what measures, if any, could be undertaken during the waiting period spanning between the risk assessment and the issuing of a detection order.
- The Regulation should also clarify the status of other existing structures, including the hotlines, which through their work have proven that notice and take-down measures are effective, low-threshold and quick.

4. Orders (detection, removal and blocking):

- Detection orders, due to their severe consequences and the necessary procedural steps, should be a measure of last resort.
- Besides, the proposal should clarify that detection orders must be consistent with the recently reconfirmed principle in the DSA that prohibits general monitoring obligations by hosting providers.
- A ‘cascade approach’ to removal orders would be preferable, in line with the e-Evidence agreement. This defaults to issuing removal orders to ‘data controllers’ before ‘data processors’. Such an approach is crucial, as infrastructure providers lack granularity over the content and must often remove an entire resource as opposed to one ‘piece of content’.
- Blocking orders cannot be considered the most suitable measure to fight CSAM. Instead of targeting the content at source, they merely move it out of sight for parts of the general public. On the hosting side, domain names and host servers can easily be changed. On the user side,

technologies such as virtual private network services and alternative resolvers are easy to use and well-known tools to circumvent blocking measures.

5. Encryption:

- Encryption is fundamental to providing safe and secure private communications to Internet users and ensuring strong cybersecurity and data protection.
- Breaking encryption would have a serious impact on the technical Internet infrastructure and impede efforts to create an Internet which enhances trust, user privacy, and freedom of expression.
- Given the protection conferred to encryption in the ePrivacy Derogation, the strong incentives for encryption provided by the NIS2 Directive, and the recognition of its role in guaranteeing the security and confidentiality of the communications of children, it shall also be explicitly protected in the proposed CSAM Regulation.
- By requiring service providers that employ end-to-end encryption (E2EE) to filter and scan for CSAM and grooming, the proposed legislation risks weakening or breaking E2EE. Client-side scanning of communications is not a solution as it is not an E2EE-resilient technology.

6. EU Centre:

- More clarity would be welcomed when it comes to the EU Centre and its role within the global reporting environment. A framework for the industry on reporting of CSAM is already in place and in many cases coordinated via the National Centre for Missing and Exploited Children (NCMEC). Given that child sexual abuse is a problem that exceeds the borders of the European Union, it needs to be tackled comprehensively at the global level, encouraging cooperation with existing entities and streamlining processes. The role of the EU Centre in this process needs to be clarified, as well as its future interactions with existing bodies such as NCMEC, INHOPE and its hotlines, as well as Europol.
- It is necessary for the text to provide sufficient flexibility for the industry to either report to the EU Centre, the assigned local authorities, INHOPE hotlines or NCMEC. This would address the conflict of laws for certain companies headquartered overseas, while supporting existing international reporting mechanisms and avoiding the unnecessary duplication of reporting and costs. It is also important to ensure that providers are still able to use the technologies they have collectively been developing, testing and applying to prevent and address child sexual abuse online.

ACT | The App Association

ccia Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

CISPE.cloud

DOT. europe
Digital • Online • Tech

eco
ASSOCIATION OF THE INTERNET INDUSTRY

EuroISPA

FiCom
FINNISH FEDERATION FOR COMMUNICATIONS AND TELEINFORMATICS FiCom ry

ispa
Internet Service Providers Austria

ITI