CCIA Position Paper: The proposed EU Regulation to prevent and combat child sexual abuse

Introduction

The Computer & Communications Industry Association (CCIA Europe) welcomes the overarching goals of the European Commission's proposal for a Regulation that seeks to prevent and combat child sexual abuse (CSA Regulation).[1] We fully support the objective of fighting child sexual abuse material (CSAM) and exploitation, including the strenghtening of existing efforts and of cooperation between national authorities. Digital service providers, civil society and authorities each have their part to play in the global fight against online CSAM.

CCIA Europe Members are already actively addressing CSAM.[2] While online services offer wide-ranging economic and social benefits, these technologies can be misused by malicious actors. Digital service providers have responded to this problem with a range of initiatives tailored to their respective services. These include voluntary scanning for known CSAM, partnering with expert bodies, developing innovative new technologies to detect previously unknown CSAM, and performing research into the detection of behaviour indicative of child exploitation (such as grooming).[3] Likewise, service providers have developed tools allowing children to use technology, access content, and interact with others in a safe, secure and private manner. These actions already have delivered significant public benefit, resulting in the successful investigation and prosecution of child sex offenders around the world.[4]

CCIA Europe believes the proposed CSA Regulation is an opportunity to build on these efforts without creating new rules that would contradict the EU ban on general monitoring, violate people's privacy and other fundamental rights, or undermine encryption. As it stands, CCIA Europe is concerned that the proposal is failing on all three counts, and several important improvements are necessary to achieve an effective, but proportionate, framework to combat and prevent online sexual abuse of children. As the European Parliament and the Council are seeking to develop their own position in the coming months, CCIA offers the following recommendations.

---

[1] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse COM/2022/209 final, May 2011, accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472

[2] There are many coalitions to which our members contribute, such as the Technology Coalition, the ICT Coalition, the WeProtect Global Alliance, and INHOPE and the Fair Play Alliance, that bring companies and NGOs together to develop solutions that disrupt the exchange of CSAM online and prevent the sexual exploitation of children.

[3] To detect known CSAM, databases of high-quality hashes and detecting technology are used. This technology allows digital companies to detect previously identified CSAM images for which a digital fingerprint or hash has been created and stored.
To detect new CSAM, machine learning classifiers are used. Classifiers apply machine learning to help identify content that shares similar characteristics to other content known to contain child sexual abuse, which can then be prioritised for human review. The use of classifiers combined with human reviewers help digital service providers to identify previously unidentified CSAM, and, in this way, help us keep up with bad actors who are constantly evolving their tactics and can lead to the identification of new CSAM and possible child victims undergoing ongoing harm and in need of rescue.

[4] Technology Coalition, Annual Report, August 2022, available at: https://www.technologycoalition.org/annual-report

CCIA recommendations

1. Risk assessment and mitigation (Articles 3 to 6, Recitals 14 to 19)

1.1 Ensure consistency with other EU rules, especially the Digital Services Act, General Data Protection Regulation and e-Privacy Directive

The draft CSA Regulation acts as a *lex specialis* to prevent and combat child sexual abuse, on top of the horizontal rules set by the Digital Services Act (DSA).[5] The obligations set forth in both the recently-adopted DSA and the CSA proposal should be consistent and not overlap or conflict. This is particularly the case for the provisions on risk assessment and mitigation, and user notification and redress. For instance, very large online platforms should be able to comply with Articles 3 to 6 of the CSA Regulation using a similar approach to compliance with Articles 26 to 27 of the DSA. Different approaches might lead to legal uncertainty and lack of clarity for these companies.

The CSA Regulation should provide a clear legal basis for voluntary scanning - whether this takes place to detect known CSAM, unknown CSAM or grooming - and confirm that it can be used as a mitigation measure. The new rules should first align with Article 6 of the DSA - which allows intermediaries (including hosting service providers) to detect, identify and remove, or disable access to, illegal content such as CSAM - and explicitly allow data controllers to use Article 6.1.(d) of the General Data Protection Regulation (GDPR) as a lawful ground to process personal data "to protect the vital interests of the data subject or of another natural person".[6] The CSA Regulation should avoid repealing the Interim e-Privacy Regulation (2021/1232/EU) and make clear that voluntary detection, reporting, and removal of CSAM in the context of interpersonal communication services remains permitted under the conditions set out in the latter regulation.[7]

1.2. Fight child sexual abuse and exploitation while respecting fundamental rights and privacy

The CSA Regulation should clarify how risk assessment and mitigation measures can be carried out consistent with the GDPR, including the "data minimisation and purpose limitation" principles which limit the collection of personal data to what is directly relevant and necessary to accomplish a specific and explicit purpose.

[5] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] Regulation 2021/1232/EU on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32021R1232

In other words, processing should only take place if it is not possible to achieve the purpose by way of less intrusive means. For example, the CSA Regulation requires age verification and assessment by providers of hosting services (Article 3.2.(b)), interpersonal communications services (Article 4.3) and software application stores (Article 6.1.(c)). Tools to establish the age of users require digital service providers to collect a substantial amount of personal information about all users. Such tools should be used in a proportionate manner and must be balanced in relation to the associated risks to people's rights, including their privacy and the protection of their personal data.

In the context of the CSA regulation, this type of data collection should only occur if it is directly relevant and necessary to help prevent the online sexual abuse of children or to address CSAM. It is unclear how requiring hosting providers to collect and verify age information would further this goal. Even in those circumstances where assessment of age serves the goal, age assurance is a more proportionate way to achieve the policy goals while respecting users' privacy.[8]

1.3. Support prevention

CCIA Europe Members have built a comprehensive suite of tools to combat CSAM, including in the area of prevention. For instance, the detection of spam and scams helps to identify suspicious behaviour. These tools can be used to restrict account features and make it harder for malicious users to find and contact people they do not know, including children, thereby disrupting potential harm before it can happen. Machine learning tools are other instruments used to detect behavioural patterns that could lead to abuse.

The CSA Regulation should be consistent with a variety of measures that can help to prevent the dissemination of CSAM. There is not one technology that can single-handedly solve the spread of CSAM. That is why the Regulation should support a wide range of tools and processes, as these complement each other and prevent gaps in the detection and removal of CSAM.

2. Detection orders (Articles 7 to 11, Recitals 20 to 28)

2.1. Aim for EU rules that strengthen each other

(a) Respect and uphold the principle of no general monitoring obligation

CCIA's Members are committed to help prevent and combat the dissemination of child sexual abuse material and its exploitation. The CSA Regulation needs to be clear on how detection

[8] Age verification refers to the legal verification of a person's age using legal documents (e.g. passport, electoral registration). This usually refers to the verification of the age of adults and not children. On the other hand, age assurance refers to the process by which a company can infer a person's age using a range of insights including their behaviour, the language they use, what content they browse and the profile of their "friends". It might not be as robust as age verification, but it does not require the collection of sensitive personally-identifiable information and is more consistent with the data minimisation principle in the GDPR. It is also becoming the preferred way for assessing a child's age given the very strict GDPR requirements around the processing of children's data.

orders should be implemented in practice in light of the EU-wide ban on general monitoring required by the DSA. CCIA Europe is concerned that detection orders could breach this key principle by imposing a *de-facto* monitoring obligation. Indeed, the Regulation should make clear that regulators cannot challenge the ban on general monitoring. Additional clarifications and safeguards are thus required for Article 7 on the issuance of detection orders (especially Articles 7.4. to 7.7.).

(b) Ensure legal certainty and coherence with EU privacy legislation

In order to deliver the required legal certainty, the CSA Regulation needs to clarify how detection - mandatory and voluntary - will coexist with the GDPR and the ePrivacy Directive. For example, the proposal already provides important derogations to Article 5(1) and 5(3) of the ePrivacy Directive.[9] However, it should also clarify that a mandatory detection order is considered a "legal obligation" under Article 6 of the GDPR[10] and that related decisions - e.g. about the balancing of individual rights and the detection and investigation of crime - are the sole responsibility of the Coordinating Authority and the competent judicial authorities.[11] That is also why the CSA Regulation must provide additional safeguards for detection orders in order to ensure they remain proportionate and aligned with EU privacy rules.[12]

2.2. Safeguard encryption

The CSA Regulation should acknowledge and preserve the role that encryption (including end-to-end encryption) plays in providing the private and secure communication that today's users - including minors - demand and expect.

As pointed out by the European Data Protection Board and the European Data Protection Supervisor,[13] the wording of the proposal, specifically Recital 26, Article 8(3) and Article 10(2), could discourage providers from implementing or maintaining strong encryption technologies since it cannot refuse execution of a detection order based on technical impossibility.

Given that encryption plays a key role in safeguarding the safety of users, scanning obligations

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
[10] As acknowledged in the explanatory memorandum, but not the body of the proposal: "the proposal, in particular the detection orders issued on the basis thereof, thus establishes the ground for such processing referred to in Article 6(1)(c) GDPR, which provides for the processing of personal data that is necessary for compliance with a legal obligation under Union or Member State law to which the controller is subject".
[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[12] See EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse Adopted on 28 July 2022 available at https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf
[13] See to that effect section 4.10 of EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse Adopted on 28 July 2022 available at https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf

should be proportionate to the known risks,[14] and should not entail any form of *de jure* or *de facto* prohibition or weakening of encryption. The new rules should instead focus on building the right conditions for innovative and privacy-preserving detection technologies, which can be deployed to detect behaviour that may put children at risk.

2.3. Avoid overwhelming false positives

The CSA Regulation should adopt a holistic risk-based approach. The detection of unknown material and possible grooming of children should be left to voluntary measures, and not be subject to detection orders. The Commission proposal appears to rest on the assumption that technology is inevitably evolving to the point where the detection of new and unknown CSAM is possible and accurate. In practice, however, the detection of known CSAM requires scanning against existing hash databases, which only include images that have been established to qualify as CSAM. On the other hand, the detection of unknown CSAM and grooming relies on classifiers and artificial intelligence (AI) to detect unlawful CSAM. Whilst these classifiers are continuously improving, they unfortunately remain unreliable, leading to far higher false positive rates than for known imagery.

In its current shape, the Commission's proposal would likely result in very high numbers of non-CSAM images being incorrectly flagged. This has the potential to result in many false accusations against innocent users, with serious real-world consequences for these people and interference with their privacy and data protection rights.

2.4. Target detection orders to the right players

It is essential that the CSA Regulation acknowledges and differentiates between the various types of hosting service providers and their distinct technical capabilities to detect CSAM. For now, the proposal does not yet differentiate between hosting providers. Indeed, it seeks to introduce detection orders for any service performing the "storage of information at the request of a recipient of the service". IT infrastructure companies like cloud service providers, however, only offer computing resources that enable customers to build and run their own IT operations. As data processors, cloud vendors generally have no control, let alone knowledge, of the content and nature of the data they process on behalf of their customers. The control over the actual data stored on the IT infrastructure lies entirely with the customer.

Indeed, for the past two decades, cloud products have been specifically designed to leave cloud customers with sole control over their data in order to guarantee a level of confidentiality and integrity of European data and IT systems that is equivalent, if not higher, to processing performed on in-house IT infrastructure. To now require cloud vendors to scan, monitor and filter their customers' data would constitute a disproportionate interference into the confidentiality and integrity of cloud customers' data. It would also severely undermine European and global customers' trust in data processing services in Europe.

[14] Unicef, Encryption, Privacy and Children's Right to Protection from Harm, October 2020, available at: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf

With this in mind, CCIA Europe calls on lawmakers to ensure that detection orders under this Regulation should only be addressed to data controllers, and exempt providers that supply data processing or sub-processing services from complying with detection orders.

Nevertheless, when qualifying as hosting service providers, those providing IT infrastructure should carry out risk assessments for the relevant services they offer and outline their mitigation measures against CSAM (Article 3).

2.5. Inform users, but do not give malicious actors valuable information

Sexual predators constantly adapt their methods to approach children, looking for ways to bypass the protections put in place by information society services (ISSs). As it stands, certain transparency requirements in the CSA proposal could give perpetrators or other malicious actors a roadmap to circumvent detection (e.g. Articles 6.3., 10.5., 15.3.) and incentivise them to migrate between services. CCIA Europe is particularly concerned about the obligation for providers to inform users about the ways in which they operate detection technologies (Article 10.5.(a)). In addition, the obligation to inform users concerned when CSAM has been identified or potentially identified - Article 10.5.(b) and 10.5.(c) - actually provides malicious actors an opportunity to tamper with evidence, ultimately hindering law enforcement in the later stages of an investigation.

It is crucial to strike the right balance between informing users that their content might be removed or account suspended, without giving malicious actors valuable information that could help them game the system and circumvent processes that should protect children. Furthermore, informing users should be the sole responsibility of expert authorities in the EU member states, as they are best placed to decide how and when disclosure should occur.

3. Removal orders (Articles 14 to 15, Recitals 30 to 32)

As mentioned before, EU rules should be mutually supportive and contribute to creating a consistent legal framework. That is why the CSA Regulation, and Article 14 on the issuance of removal orders in particular, should be aligned with the politically approved e-Evidence Regulation.[15]

When an authority notifies the presence of known CSAM on their servers, infrastructure providers, due to their place in the internet technology stack, get much less precise orders when it comes to the removal of specific pieces of content.[16] Should such providers face removal orders for pieces of content flagged by a competent authority under Article 32 CSA, they may in

[15] European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

[16] It is not technically possible for an infrastructure provider to take down or disable access to one specific piece of content because the infrastructure provider does not have access to the customers' content.

effect be obligated to remove thousands of pieces of lawful content in the process, especially under tight deadlines.[17]

To avoid excessive removal of lawful content, the CSA Regulation ought to clarify that when data is stored on infrastructure like a cloud server, the customer of those services (i.e. the data controller) should first be issued removal orders for specific content. Only when all avenues have been exhausted should removal orders be addressed to providers lower down the internet stack (e.g. IT infrastructure providers that merely act as data processors). This would provide greater legal certainty to data controllers and processors alike. It is worth noting that such an approach has also been favoured in the e-Evidence Regulation (Articles 2.3 and 5.6). A similar approach for the CSA would ensure that removal orders, particularly those of an urgent nature, are received by the appropriate stakeholders - allowing them to react swiftly and remove CSAM content expeditiously.

4. Service providers' liability (Article 19 and Recital 34)

CCIA welcomes Article 19 and Recital 34 allowing ISSs to undertake voluntary investigations without being penalised for their good faith efforts. Measures of this nature will help to increase trust online at large, as ISSs will be empowered to more effectively tackle CSAM and its exploitation. However, the CSA Regulation proposed by the Commission is unclear as to whether digital service providers have a legal basis for voluntarily detecting child sexual abuse material as a mitigation measure following a risk assessment.

To further incentivise online trust and safety, the CSA Regulation should clearly state that it also covers voluntary investigations as well as the use of metadata covered by the ePrivacy Directive, or other actions aimed at enforcing the terms and conditions of ISSs.

5. Technological tools (Chapter II, Articles 3 to 24)

5.1. Provide incentives to innovate

Innovation is crucial in the fight against the dissemination and exploitation of child sexual abuse material as perpetrators and other malicious actors are always trying to find new ways to bypass protections and abuse the system.

It should be avoided that the CSA Regulation becomes overly prescriptive in specifying which methods should be used to mitigate CSAM risks. Otherwise, the new Regulation might have unintended consequences such as constraining innovation. If the new rules narrow down the possibilities for compliance to one, or just a few methods, companies will not be incentivised to be creative when developing new solutions. Indeed, the CSA Regulation should introduce a transparent framework that incentivises the development of innovative safety tools.

[17] IT infrastructure service providers that are ordered to remove specific content would have to disable access to all content stored on the platform for that same service or customer.

However, the Commission's current proposal lacks incentives to detect and remove CSAM, which will discourage digital service providers from innovating and developing new technology. That is why the new CSAM rules should encourage ISSs to keep developing more advanced and innovative tools, allowing for the effective identification and removal of CSAM.

5.2. Adopt future-proof and technology-neutral rules

The tools for detecting and reporting CSAM and related suspicious behaviour to authorities will continue to evolve over time. Therefore the CSA proposal should not favour one technical solution over another, nor should it mandate specific technologies, as this would harm both innovation and competition.

The CSA Regulation should thus be technology-neutral, with its scope limited to identifying outcomes and providing flexibility as to which solutions and processes to use to reach those objectives. CCIA Europe encourages policymakers to build smart policy frameworks that promote innovation and maximise the benefits of technology by encouraging principles that are attainable for all.

6. EU Centre

CCIA Europe supports the creation of an EU Centre to support and coordinate the build-up of Europe's capacity to fight child sexual abuse material and its exploitation. It is crucial that this new centre allows companies to operate in compliance with pre-existing legal obligations, and does not lead to conflicting law or duplication. The CSA Regulation must allow authorities at EU and member state-level to continue to benefit from global frameworks.

For example, US companies already have the existing legal requirement to report all instances of CSAM only to the US National Centre for Missing & Exploited Children (NCMEC) and benefit from a legal exemption to do so. This legal exemption does not cover EU agencies - including the future EU Centre - but NCMEC does routinely share reports relating to EU-based users with the relevant national law enforcement agencies concerned.

To avoid such a conflict of laws, EU policymakers should work with the US government to resolve the issue and ensure that the EU Centre can only act as a repository of CSAM as soon as it is recognized under US law as an organisation which can receive CSAM detected by US companies, in the same way as with NCMEC. The NCMEC and EU Centre reporting flows also need to be better thought through to avoid potential conflicting follow-up which could undermine the effectiveness of efforts to combat child sexual abuse.

Until such a solution is reached, CCIA Europe calls on European lawmakers to ensure that the CSA Regulation recognises the importance of avoiding duplicative reporting regimes.[18]

Conclusion

CCIA Europe believes that the proposed CSA Regulation holds great potential to complement existing frameworks to combat and prevent online child sexual abuse and to better protect children, while respecting the EU ban on general monitoring, providing incentives for innovation, and without undermining data encryption.

We look forward to working with policymakers to improve the CSA proposal and provide information on how to address child sexual abuse material, while safeguarding the fundamental rights of Europeans.

Our members are strongly committed to assisting in the investigation and prosecution of these serious crimes. Digital service providers stand ready to join forces with the EU institutions to tackle any remaining challenges that existing initiatives haven't solved yet.

About the Computer & Communication Industry Association (CCIA)

CCIA is an international, not-for-profit association representing a broad cross section of computer, communications and Internet industry firms. CCIA remains dedicated, as it has for 50 years, to promoting innovation and preserving full, fair and open competition throughout our industry. Our members employ more than 1.6 million workers. For more, please go to: www.ccianet.org

[18] Such as in other legislation e.g. section 9 of Canada's *Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service* (S.C. 2011, c. 4), which states: "A person who has reported information in compliance with an obligation to report child pornography under the laws of a province or a foreign jurisdiction is deemed to have complied with section 2 of this Act in relation to that information". Available on https://laws-lois.justice.gc.ca/eng/annualstatutes/2011_4/FullText.html