bitkom

Bitkom on the EU CSAM Proposal

23. Januar 2023

Content

1 Background and Initial Statement

The European Commission presented its proposal for the fight against child sexual abuse on May 11, 2022. This proposal aims to curb the widespread distribution of child sexual abuse material (CSAM) and online grooming, which has risen sharply during the pandemic. Bitkom strongly supports the objectives of the proposal guaranteeing the well-being and protection of children, both offline and online. However, the proposal excessively and disproportionately interferes with users' fundamental rights to privacy.[1] The objectives of the proposal should therefore be pursued by alternative means - the strengthening of law enforcement authorities and mechanisms in conformity with fundamental rights and in particular the equipment and development of know-how, as well as digital literacy programmes and education to raise awareness about online risks. A closer cooperation of authorities and institutions as well as the private sector for the protection of children and young people, online and offline, must have priority. With respect to legislative projects with partly similar regulatory objectives, it is also essential that no duplicate regulations or contradictions arise - this applies in particular to the Digital Services Act and the e-Evidence Package. 2

---

1   ↗ Statement on Chat Control and the Right to Encryption | Bitkom e.V.

2   Summary

Bitkom welcomes the aim of the proposed regulation to detect child sexual abuse material on the internet and to prevent its dissemination. It also welcomes the goal of protecting minors from grooming. However, the chosen instruments a) cannot be implemented adequately from a technical point of view as envisaged in the proposal and b) represent a disproportionate encroachment on fundamental rights in comparison to alternative mechanisms, such as the strengthening of law enforcement authorities and educational outreach to children and young people. Nevertheless, Bitkom fully supports the EUs aim to combat the dissemination of child sexual abuse material and grooming on the Internet.

3   General Requirements

Scope

Currently, the draft Regulation takes a broad approach to the services within its scope and does not fully take into account the technical and legal constraints that apply to different services in the value chain.

The legislative proposal imposes obligations on app store providers to take 'reasonable efforts' to assess whether each application presents a risk for solicitation of children and to take 'reasonable measures' to prevent children from accessing such applications by means of age verification and age assessment measures to identify child users. Application store providers are, however, often not best placed when it comes to assessing this risk posed by each application. We believe that the obligation should therefore be on the application developers themselves to properly assess the risk of grooming and solicitation of children on their services, and to then take the appropriate mitigation measures as needed. Requiring app store providers to assess in parallel and potentially prevent minors from accessing certain applications could result in not only duplicative efforts by all parties involved but could lead to different conclusions rendered by the app developer, the relevant authorities, and the app store provider, possibly resulting in legal action. The process should have streamlined age verification solutions and should remain with the party that is most familiar with their service and the vectors for abuse on that service.

In addition, the proposal would benefit from clarifying which role cloud infrastructure providers play in the fight against online child sexual abuse. Cloud infrastructure providers offer a collection of modular cloud services including computing, data storage, data analytics and machine learning that enable customers to build and run their own IT operations. Only the customers of cloud infrastructure have direct access and control over their data. They are best positioned to understand the forms of abuse that could take place on their platform. Detection of online child sexual abuse would be most robust and actionable with the customer who has control and knowledge about their end-user data. Placing Cloud infrastructure providers in scope of the detection orders in the same manner as downstream hosted products, would be unproportionate and fail to recognize technical challenges. Thus, we recommend cloud infrastructure providers be taken out of scope for the detection obligations.

Risk reporting and risk mitigation measures

Providers of hosting services and interpersonal communication services shall be required to prepare risk reports with regard to the risk of their service being used for the dissemination of child sexual abuse material and grooming activities. Based on these reports, providers are to assess risks and take risk mitigation measures and report them to the new EU centre. The basic idea of assessing one's own risk and designing and implementing measures to minimise the assessed risk is to be supported. The Digital Services Act will already impose an obligation for very large online platforms to assess and mitigate risks on their services. For those operators who will be subject to such broader risk assessment obligations under the DSA, there should be the possibility to build on that to comply with the obligation under the new proposal. Moreover, providers are currently already voluntarily implementing measures to make it more difficult to disseminate child sexual abuse material.

However, the draft regulation leaves several questions open: Among them are the criteria for classifying the risk. The assessment process, or rather the assessment criteria, must be designed in a transparent manner in order to also be able to assess the appropriateness of risk minimisation measures. Criteria must be developed that are known and common to all.

Furthermore, the regulation should allow for the inclusion of voluntary scanning as it is the case in the interim regulation. This would guarantee that services can continue the work they are already doing and would prevent a temporary halt of scanning during the transition period. Regarding scope and possible exceptions for e.g., classified materials additional discussions about safeguards are needed. Under the proposed risk mitigation framework, companies should be at least allowed to continue proactive voluntary detection of known CSA material (CSAM). Considering the verified nature of criminal material and the proven/robust/non-invasive nature of hash-matching technology, proactive detection of known CSAM would pose limited risks to fundamental rights, while having the potential to swiftly and effectively avoid revictimization.

According to the draft regulation, the risk measures to be taken should be in proportion to the financial and technological possibilities as well as in proportion to the number of users of the providers. This is in essence to be welcomed. However, it also means that large messenger services will have to take more rigid measures than small niche services. Making it a logical assumption that perpetrators will switch to smaller service providers, which have to introduce less rigid measures. Due to this a feasible minimum standard must be established enabling smaller providers to implement the minimum standard and larger providers with additional leeway to implement additional risk mitigation measures. The EU Centre has to be able to provide the necessary technology to SMEs.

Detection order

Under the proposal, detection orders will be issued if the EU Centre is of the opinion that the risk reduction measures taken are not sufficient. However, the draft regulation currently lacks information on how the EU Centre arrives at its assessment. Which indicators will be used as a basis to assess risk and necessity? The chosen indicators, or at least the underlying guiding principles, should be defined in the proposal to ensure transparency and consistency. In addition, the indicators should be regularly evaluated regarding their accuracy and adjusted according to current technological develop-ments. Overall, orders should be issued only as measures of last resort.

The order preparation process will be complex, resource-intensive and impose burden-some requirements on the public and private sector, particularly on smaller operators since detection orders – particularly for new CSAM and grooming – will likely result in heavy levels of intrusiveness on users' fundamental rights.

Removal order

Bitkom welcomes the introduction of removal orders, and we are aligned with the goal of removing CSAM expeditiously. However, we want to point out that not all hosting providers are technically able to access their customer's granular content. To mitigate negative effects of large take downs of resources, we recommend that a similar approach to Art. 5.6 of E-evidence Regulation (political agreement) be issued in which Production Orders are first addressed to service providers that act as data controllers.

Blocking order

The idea of the blocking obligation presented in the proposed regulation can be com-pared to the basic idea of the German Access Impediment Act from 2010. The criticism from back then remains: The blocking mechanisms can easily be circumvented, making the blocking invalid. In addition, according to the draft regulation, access blocks are limited in time and deletion of the material does not take place. Thus, the material remains on the net and can be further disseminated via other ways and channels. Only consistent deletion of detected material will prevent it from being further dissemina-ted in the same way.

Technology

If, based on the analysis of the risk report and the proposed risk mitigation measures, the EU centre concludes that there is a risk that the service is being used to share child sexual abuse material or solicitation, then a detection order may be issued. This will impose a duty to implement technology that detects material containing child sexual abuse and grooming content.

Depending on technology, compliance with detection orders could result in disproportionate obligations that could become incompatible with the EU ban on general monitoring obligations for intermediaries. To avoid that, detection orders should be issued only if and when technology allows a fair balance among the fundamental rights of all parties involved.

Such technology currently exists to detect known CSAM (i.e. hash-matching technology). However, at this stage, it is unclear whether equally robust, proven, and scalable detection technologies for new CSAM and grooming exist at all. Detection of new CSAM and grooming is done through AI classifiers. Even assuming accurate and reliable technologies are developed in the future, escalation and systematic human review in such instances cannot be avoided. This is particularly relevant with regard to the complex task of validating suspected instances of grooming, which are highly dependent on context and intent that can only be discerned from extensive human review, and this raises significant privacy concerns.

Detection technology, often referred to as »chat control« due to its broad nature, needs more in-depth discussion and a careful balancing of interests and fundamental rights. Experts from this field are not aware of any technology that meets the required state of the art, has the lowest possible error rate and least invasion of privacy.[2] It is not very likely that such a technology will exist in the near future, especially during the implementation period of the Regulation. Additionally, there is too little information on the criteria of the implemented technology. However, a high error rate, such as ranging close to 10 %, would lead to the material having to be checked manually. This ties up resources that are lacking in the prosecution of the alleged perpetrators to prevent further child sexual abuse. The general use of scanning technology, regardless of suspicion, is an enormous intrusion into the privacy of millions of EU citizens several times a day. Bitkom firmly rejects this approach and recalls that the fundamental right to privacy also applies in the digital space and especially also regarding communication data, as recently shown in the CJEUs considerations of the former German Data retention Law and its approach to cover data independent of a concrete suspicion and without enough balance to the rights of the users.

When using AI, there are further questions about technology that need to be answered before its implementation. For instance, how are AI systems supposed to adequately and reliably recognise whether the material in question is footage of a 17- or

2   ↗ FraunhoferSIT-StudieJugendschutz.pdf

18-year-old person? In the context of detection of new CSA material, technology is unlikely to be able to correctly identify problematic material without human intervention. In addition, there are different age limits for sexual consent in the EU. Even young-looking but adult people can take intimate pictures of themselves and share them with mutual consent. There is a high probability that the AI will recognise this as a depiction of child sexual abuse, the file will be identified as false-positive and will have to be checked manually. The same applies, for example, to shots of toddlers at the beach or in the garden in summer, which are shared in the family group without ulterior motives. If such a depiction is filtered out and handed over to the authorities, firstly, additional work is again incurred, and time cannot be invested in the prosecution of criminal content but also the sender of the depiction turns up in the course of the investigation and their privacy is invaded.

Even if reliable and accurate detection technology is developed in the future, escalation and human review cannot be avoided. This rings particularly true for grooming.

Grooming indicia are embedded in language, which in turn continuously evolves, are very context-based and thus require interpretation given the context/intent specificity. Even assuming a 100% accurate detection technology, by nature a grooming detection obligation would still de facto require that every private text message scanned and identified by automated technology as potential indicia of a grooming conversation would have to be read and verified by a human reviewer. As a result, regardless of the quality of the available detection technology, scanning for grooming remains an extremely privacy-intrusive practice which would jeopardize the users' privacy.

The draft regulation requires providers of interpersonal communication services to include information on the technology used in their general terms and conditions. In general, transparency is to be welcomed, but there is a risk here that the alleged perpetrators will thus obtain information that makes it possible for them to circumvent the technology in order to continue sharing criminal content.

EU Centre for Preventing and Combating Child Sexual Abuse

In order to combat child sexual abuse and to coordinate law enforcement in this field, an appropriate EU centre should be established. To ensure communication between the EU centre and the providers, simple but secure communication channels and interfaces are needed to transfer data as sensitive as child sexual abuse material.

The communication should be based on already existing frameworks, such as the one proposed for the implementation in the e-Evidence regulation.

In order to be effective, the EU centre must be sufficiently well equipped from a financial and personnel point of view. It must be ensured that responsibilities and powers are defined from the outset to save duplication and uncoordinated action and thus valuable time to solve and prevent child sexual abuse crimes.

The EU centre shall create and maintain a database of hash values of known depictions of child sexual abuse. This hash database will work for the detection of known material but not for unknown or slightly altered material. The EU Centre should also work in close cooperation with NCMEC in order to ensure that the database is exhaustive.

The new rules will require companies to report to the EU Centre regardless of whether they are already reporting in other jurisdictions (i.e. NCMEC). This will not only create double reporting obligations with the obvious negative red-tape and administrative costs for companies. This will also create risks of fragmentation in terms of knowledge management and database maintenance by the various regional authorities. Reporting requirements should be harmonized as much as possible to existing reporting systems and mechanisms to ensure consistent knowledge management in this area should be put in place.

Alternatives

One of the justifications for the draft regulation, according to the Commission, is that the so-called transitional regulation expires in 2024 and there should be a legal successor. The measures made possible by the transitional regulation to limit the spread of child sexual abuse are having an effect. Many companies have voluntarily implemented measures. Therefore, an alternative, which would allow for the time to draft a regulation in conformity with technological possibilities and fundamental rights, would be that the transitional regulation is extended for a longer period.

In addition to the possibility of extending the transitional regulation, another measure could be that known material is filtered first and that this and known accesses to it are consistently deleted after discovery. In addition, users who send known content of child sexual abuse could receive an automatic warning that they are sending criminally relevant material. The idea here is that they feel caught and do not send the material.

The strengthening of law enforcement authorities and mechanisms in conformity with fundamental rights and in particular the equipment and development of know-how, as well digital literacy programmes and education to raise awareness about online risks must take priority. Furthermore, the close cooperation between the public and the private sector for the protection of children and young people, online and offline, has to be encouraged and developed further.

Conclusion

We support the aim to develop tools and improve the means of identification of child abuse material for companies and law enforcement agencies. Priority should also be given to the deletion of known material that can only be done by increasing the resources of law enforcement agencies to prosecute and investigate child sexual abuse. However, we do not consider the proposed approach to be suitable, necessary, or appropriate due to the reasons mentioned in this position paper. We are determined to proactively improve and develop technical solutions to stop the distribution of CSAM and eager to further discuss our abovementioned concerns to find solutions.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom