Developers Alliance position on the European Commission's proposal for a regulation laying down rules to prevent and combat child sexual abuse

Developers Alliance welcomes the opportunity to provide feedback on the proposal for a regulation on preventing and combating child sexual abuse material (CSAM).

EU lawmakers need to wisely balance the tradeoffs before implementing a de facto online surveillance system in the EU. The chosen policy option ignored the following facts:

- *Companies will always err on the side of caution when faced with absolute obligations and strict sanctions.*
- *Technology, like human decision making, is imperfect; there will always be false positives which put at risk fundamental rights. Once broken, end-to-end encryption is compromised forever, with significant impact far beyond CSAM.*
- *Technology is not enough to protect children. Social problems are solved by tackling their roots.*

We are calling on EU lawmakers to reject such a disproportionate and radical proposal and focus instead on providing a solid legal basis for voluntary actions to counter CSAM online.

I. General remarks

CSAM represents some of the most abhorrent content on the internet and the developer community will always support efforts for preventing and combating the distribution of such material. But technology is a tool and no matter how advanced it could be, it will always have its limitations. While technology can help in addressing complex societal problems, it has to be complemented by other measures, especially in tackling the root causes of such disturbing social issues.

There is a delicate balance between the salutary objective of the regulation and the foreseeable effects of a disproportionate regulatory approach. We strongly recommend carefully assessing the cumulative impact of the proposed measures, taking into account the limits of technology and avoiding the over-reliance on future (and uncertain) technology. We also call on the co-legislators to re-consider the stringent legal obligations imposed on online service providers, basically an 'imposed private-public partnership' to set up an extensive government surveillance system in the EU while undermining the rights of law-abiding citizens in the digital world.

II. Technical and practical limitations on private surveillance of content and communications

The proposal is supposed to be technologically neutral, imposing obligations of result, not of means. However, service providers would be put in an impossible position and would have no choice but to rely heavily on automation and intrusive content and communication scanning solutions for detection, removal and reporting of CSAM, and for clearly identifying all "grooming" situations.

1. The impact on end-to-end encryption technology (E2EE)

Recital 26 provides an ambiguous perspective on the implementation of the obligations in the case of encrypted environments. E2EE is essential in ensuring thorough privacy, safety and security of online communications. Our community defines E2EE as our users would: the ability to share content and communication, confident that no one but those party to the exchange can ever access its content. As any other technological tool, E2EE can also be used by criminals as easily as law-abiding citizens. Indeed, E2EE allows secure and private communications, vital for the protection of fundamental rights, but at the same time it makes CSAM detection impossible. **It is impossible to apply 'exceptional access'/'selected backdoors' without compromising the underlying technology.** This is both a technical and philosophical tautology.

The US is preparing[1] measures mitigating the risk of quantum computers that can break public-key cryptography. This illustrates the importance of preserving strong encryption and the significant impact of any attempt to compromise it.

In order to ensure full compliance with the proposed obligations and trying, at the same time, to preserve users' privacy as much as possible, service providers would be forced to use techniques which ultimately provide backdoors. Solutions such as client-side scanning (CSS) and server-related methods (e.g. secure enclaves/trusted execution environment and homomorphic computation) are not foolproof. These will undermine the idea of private communications and secure content, thus eroding users' trust, as it would be impossible to ensure security against malicious actors inside or outside the government. Worse still, once implemented these capabilities would quickly be mandated by corrupt regimes whose national laws are equally binding on commercial actors.

There are various technical, legal and ethical issues which show that CSS is not a feasible 'privacy-preserving' and 'surveillance risk-free' option[2]. Research shows "that CSS neither guarantees efficacious crime prevention nor prevents surveillance. Indeed, the effect is the opposite. CSS by its nature creates serious security and privacy risks for all society while the assistance it can provide for law enforcement is at best problematic. There are multiple ways in which client-side scanning can fail, can be evaded, and can be abused."[3] There is the risk, for instance, of introduction of 'non-CSAM hashes' into the hash databases that the content is checked

[1] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[2] https://digitalcommons.wcl.american.edu/research/58/
[3] https://arxiv.org/abs/2110.07450

against. Beyond the technical limitations, one cannot exclude the re-purposing of CSS, once implemented, for other legitimate or illegitimate purposes other than combating CSAM. With regard to other alternatives, both trusted execution environments and homomorphic encryption are not foolproof against side-channel attacks[4].

In summary, the proposed legal requirements will have a disastrous impact on encryption technology and human rights, as there is no current or future viable solution to implement CSAM detection while preserving the integrity of E2EE.

2. Technical and practical limitations on age verification

There is currently no reliable technological solution for age verification, despite various methods implemented by service providers to detect a user's age. While there is significant exploration taking place in this area, many potential solutions weigh on opposing priorities such as data minimization, privacy, and general weakening of security online. Absolute obligations, disregarding this situation, would put the service providers in a difficult situation of legal responsibility with no appropriate mechanism for compliance.

Strict requirements on age verification will also create disincentives for service providers to maintain and offer online services to large audiences and instead restrain access only to verified adult users.

The distinction of different age categories is very important in content moderation in general, so many service providers are interested in applying age verification as precisely as possible. The main purpose is creating adequate user experience according to different age groups, but this is also important for preventing interactions between adults and underage users, as well as between different age groups amongst children. Restricted access or differentiated services based on age categories will not solve the problem of abuse between underage users. Moreover, it could expose children to offline abuse, as they are coerced to become online surrogate groomers for others.

Restricting access based on age verification doesn’t only represent a fragile solution in protecting children, it also raises other issues. Even without restricted access, law-abiding adults would avoid online interaction with children, or would select carefully their interactions with younger users, with obvious unintended consequences. The users would also be forced to self-limit the use of online and cloud services to avoid being victims of false positive detection (e.g. storage and sharing of family photos and videos or sharing of photos for online medical services[5]). This will only erode users’ confidence in using online services.

Stricter obligations for service providers and an extensive surveillance systems on legal online platforms will not affect the distribution of CSAM on the dark web, as well the child sexual abuse in

[4] https://arxiv.org/pdf/2006.13598.pdf; https://news.ncsu.edu/2022/03/stealing-homomorphic-encryption-data/; https://arxiv.org/abs/1906.07127

[5] https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html?smid=tw-nytimes&smtyp=cur

offline environments. As previously forementioned, preventing and combating child sexual abuse requires a range of measures, especially tackling the root causes of the problem offline.

There are also issues related to the compliance with existing data protection requirements[6]. The regulation needs to be correlated with the GDPR. The obligations that result should be proportionate, as service providers need to apply the principle of data minimization at the same time.

3. Technical and practical limitations on content blocking

Hashing is not a viable solution for detecting new CSAM and grooming, as even state-of-the-art machine learning systems - or human moderators - are not capable of clearly identifying such content. With respect to manual review, beyond the significant costs to deploy it widely, this requires direct third party access to the content and clear legal definitions of what constitutes a violation (the difficult situation of encrypted content is treated above).

Preventing access to content by network (URL) blocking is not an effective measure, as it can be easily circumvented. The use of virtual private networks (VPNs) can limit the measures applying blocking technology. However, VPN blocking is not a viable solution, as it would lead to broad internet censorship in the EU.

4. The impact of (legal) surveillance

The anonymous use of the internet, together with private and secure communication channels, are essential for certain categories of people to exercise their fundamental rights (journalists, human rights activists, victims of political violence, of domestic violence, of various discriminations, etc.).

The legality, risks and unintended consequences related to a comprehensive surveillance system need to be carefully taken into consideration. A recent case in the US[7] illustrates the risks of intrusive government access to the private information of online services' users, to the detriment of those citizens' rights (in that particular case, reproductive rights). We reiterate the disproportionate and unfair situation that the service providers face, between absolute obligations to respond to law enforcement and courts' requests, on one hand, and the respect for the private life and fundamental rights of their users and the contractual commitments towards their customers, on the other hand.

The privacy and security risks associated with an extensive centralized database of "suspects" could be significant and should be addressed accordingly. Furthermore, it should be assessed if this concentration of information is the optimal solution from a democratic perspective.

[6] https://iapp.org/news/a/age-verification-and-data-protection-far-more-difficult-than-it-looks/
[7] https://www.axios.com/2022/07/08/house-panel-probes-reproductive-health-data-collection

Other important legal issues that should be considered are the proportionality of the proposed system from the perspective of users' rights, specifically the discretionary approach of governments to monitoring EU and non-EU citizens.

III. Comments on specific provisions

Although the proposal is problematic and unworkable overall, the following comments focus on particular provisions.

1. On the scope and definitions

The regulation is proposed as *lex specialis* in relation to the e-Privacy Directive and the Digital Services Act (DSA). It is important to maintain legal clarity for the regulation's addressees. Also, the implementation needs to be in line with the principles and the related legal requirements of the GDPR (e.g. data minimisation, integrity and confidentiality).

Regarding definitions, we welcome the correlation with other relevant pieces of legislation, which already provide several legal definitions. There is an inconsistency claiming clarification, between the definitions of "child" and "child user", with respect to the age threshold (18, and respectively 17).

The scope of the legislation is quite broad. There is a risk that not all services that might fall under the scope are equally relevant to the pursued objective.

2. On the proposed obligations for providers

As mentioned in the General Remarks, the strict obligations listed in Chapter II denote a comprehensive content and communication monitoring, as well as comprehensive age verification for internet services, a de facto extended online surveillance system at the EU level.

The risk assessment and mitigation obligations are incumbent upon all providers, including small apps with minimal user interaction and those with a clear adult target audience. This will translate into additional costs for small businesses, regardless of the exemption from costs for the analysis performed by the EU Centre. Notwithstanding the costs and administrative burdens, the obvious outcome is a constant surveillance mechanism which every provider will have to put in place and maintain for their operations covering the EU. The mechanism to comply with these obligations includes constant supervision of both the Coordinating Authority of establishment and the EU Centre.

The mechanism also includes exhaustive age verification (art.3.2.e.ii - "where the service is used by children, the different age groups of the child users and the risk of solicitation of children in relation to those age groups" ; art. 4.3 - "(...) shall take the necessary age verification and age assessment measures to reliably identify child users on their services, enabling them to take the mitigation measures"). We reiterate that providers are put in an uncomfortable position, between two

categories of obligations, user authentication and respectively privacy and data protection. Weakening anonymity online (at least in the EU) is a foreseeable consequence of such obligations, as service providers will err on the side of caution and implement strict user authentication solutions.

With regard to the obligations for software application stores listed in art. 6, we note that the approach relies on their stewardship role for the digital ecosystems. However, it ignores the effects of other regulatory interventions, notably the Digital Markets Act (DMA), undermining the intermediation and curation role of app stores in important mobile ecosystems. It is essential that these obligations will be observed in the enforcement of the DMA, in applying safety and security safeguards.

Compliance with the detection orders is under a strict legal responsibility and creates strong incentives for providers to use the most intrusive technologies, including with an irreversible impact on encryption technology. There is a high risk of false positives and false negatives in ML detection, which the regulation seems to acknowledge, though it still imposes the expectation to ensure exhaustive detection of CSAM, including new CSAM and solicitation of children (grooming) to the extent that can be legally defined.

Concerning the detection of grooming, the current technology cannot provide a reliable solution, especially at scale. We strongly advise against imposing strict legal obligations for providers based on the expectation of yet-to-be-invented technological solutions. Service providers will not be able to comply with disproportionate/impossible requirements.

In the case of end-to-end encryption, compliance with the strict legal obligations related to the detection orders lead to a high risk of compromising encryption - both technically and practically. While recital 26 notes the important role of this technology “as an important tool to guarantee the security and confidentiality of the communications of users, including those of children”, it also provides an ambiguous interpretation on complying with detection orders from a technical perspective. Service providers should not face such a legal conundrum.

Article 10 lays down unreasonable conditions for technical compliance with detection orders, considering the current state of technology. Moreover, on one hand, the implementation is heavily reliant on the European Centre (including for providing technological solutions), but on the other hand, the providers are placed under strict responsibility to be fully compliant. This is a high legal standard. Worse still, necessary guidelines for detection obligations are the object of an optional obligation for the European Commission, Coordinating Authorities and the EU Centre (“may issue guidelines”).

The conditions for the issuing of detection orders, together with the transparency requirements, reporting, removing and blocking obligations, set up a system where service providers must, in practice, secretly monitor, intercept and block private content and communications of their customers on behalf of public authorities and under severe penalties.

Article 19 provides service providers a welcome but limited liability exemption. This should cover all activities, both voluntary and to comply with legal requirements, to prevent and combat online child sexual abuse on their services. Given that the regulation would repeal the Interim Regulation (EU) 2021/1232, it is important to maintain legal clarity for voluntary activities in relation with the obligations deriving from the e-Privacy Directive.

3. On enforcement

A new layer of national enforcement authorities is proposed, besides the EU Centre. It remains for each Member State to decide on the designation and additional tasks, as well as how to integrate this new authority in the current administrative structure and especially how it will interrelate with law enforcement authorities that are already competent in this area. Service providers, no matter their size, are interacting with a plethora of authorities for different aspects of their business. In the case of content moderation, they will need to adapt to interactions with multiple authorities, according to specific enforcement mechanisms, including the new one proposed for CSAM. It is to be noted that regulatory compliance for internet businesses in the EU is becoming more and more complex.