Microsoft

September 2022

Microsoft Position Paper on the

Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

Introduction

Microsoft welcomes the European Commission's **Proposal for a Regulation laying down rules to prevent and combat online child sexual abuse** (hereinafter the Regulation, the Proposal, or the proposed Regulation). The Proposal reflects the urgent need to address the challenge of online child sexual exploitation and abuse (**OCSEA**). It acknowledges the complexity of these crimes and the need for holistic solutions, including ensuring that any regulation is accompanied by work on prevention. As such, the European Strategy for a Better Internet for Kids (**BIK+**) will be key in complementing the proposed Regulation.

Microsoft has a deep and long-standing commitment to digital safety, as well as a long history of working closely with governments, industry, civil society organizations and academics to reduce the presence of illegal and harmful online content. For example, Microsoft's **PhotoDNA** tool has been in use since 2009 by many companies and law enforcement to identify and remove child sexual exploitation and abuse imagery from online platforms and services. Microsoft also supports the Voluntary Principles to Combat Online Child Sexual Exploitation and Abuse and is a member of both the **Tech Coalition** and the **WeProtect Global Alliance**. As a part of the Tech Coalition, we actively support an industry initiative launched in 2020 that includes a multi-million-dollar investment into research and innovation to prevent online child sexual exploitation and abuse. We also take a range of actions to protect children across our consumer hosted services, including the use of technology to detect OCSEA and the provision of family safety controls for Windows and our Xbox gaming services.

Based on these experiences and our multistakeholder engagement, Microsoft understands the critical importance of combatting OCSEA, including to protect the safety, privacy, and other fundamental rights of victims. We also understand that measures to tackle this crime must be carefully calibrated so that they do not disproportionately impact the rights to privacy, data protection, or freedom of expression and association of all users of online services. The proposed Regulation includes several measures designed to achieve this important balance. For example, we welcome the rules requiring providers to undertake risk assessments and to take reasonable mitigation measures that are tailored to the risks identified (Arts. 3 and 4). Similarly, we welcome

the involvement of judicial and independent administrative authorities in the issuance of detection orders (Art. 7).

That said, we believe that changes are required to make the proposed Regulation practical, effective, and proportionate. We are concerned that certain elements of the Regulation may raise significant practical challenges for in-scope services and may limit services' ability to take effective safety actions.

1. Permit voluntary use of technologies, subject to appropriate safeguards

Microsoft welcomes the technology-neutral approach in the proposed Regulation, which will enable providers to determine the technologies most appropriate for their services. Microsoft also agrees with the Proposal's focus on ensuring providers are using high-quality data in the training and implementation of those tools. However, we recommend considering how the proposed Regulation can empower providers to take effective, proportionate, and tailored safety measures across their different services.

We understand that the Regulation has been carefully developed to appropriately balance European users' rights, including the rights to communications confidentiality, privacy and safety online. However, we are concerned that the current proposal may inadvertently result in a reduction in the amount of OCSEA detected in Member States across the European Union, given the proposal appears to prohibit in-scope providers from conducting their current, voluntary scanning activities or using current hash-lists, classifiers, and other relevant indicators of OCSEA. The Regulation will reduce the amount of OCSEA that is currently legally detected under the interim Regulation 2021/1232 setting out temporary derogation from certain provisions of Directive 2002/58/EC (hereinafter **ePrivacy Directive**). Regulation 2021/1232 provides for strict safeguards and conditions, including prior consultation with the competent supervisory authority.

We therefore recommend the Regulation to be amended to allow practices that are currently in scope of the interim Regulation 2021/1232 and expressly allow providers to voluntarily use existing detection technologies, subject to the same robust safeguards. The proposal establishes a responsibility for providers to assess the risk of OCSEA on their services and to take proportionate measures in response. Voluntarily deploying such technologies should be recognized as an important mitigation measure in addressing any risk of OCSEA. This is essential to enable providers to prevent their services from becoming vectors for OCSEA and to help create the greatest level of protection for children. More broadly, the Regulation should allow providers to consider relevant differences in content, services, and crimes when selecting appropriate mitigation measures, and should require Coordinating Authorities to likewise take these differences into account in evaluating such measures and/or imposing new measures.

Therefore, the Regulation should specify in Article 4 that providers can use detection technologies as a reasonable risk mitigation measure, tailored to any risks identified through the risk assessment

required by Article 3 and not contingent on receiving detection orders, as long as they deploy robust safeguards similar to those in the existing interim Regulation 2021/1232. Detection orders should be a measure only of the last resort.

More broadly, the Regulation should also allow providers to take into account relevant differences, including between content types and services, when selecting appropriate and proportionate mitigation measures. This will enable providers to ensure mitigation measures are carefully tailored, in line with the intent of Article 4(2). The Regulation should likewise require Coordinating Authorities to take these differences into account when evaluating the mitigation measures a provider has taken on its services.

Alternatively, the Regulation could establish a framework for certifying particular detection technologies and/or indicators, which could then be used for voluntary detection of OCSEA within certain parameters. Such a certification mechanism should require Coordinating Authorities under the Regulation, in consultation with EU supervisory authorities (**SAs**), to assess whether technologies submitted for review provide sufficient safeguards (based on those set out in existing interim Regulation 2021/1232), and either approve or deny certification. Where the authorities deny such a certification, they should provide detailed reasons for denial and suggestions on how to change the technology and/or its deployment to obtain approval.

2. Clarify obligations for enterprise service providers

The Regulation appears to impose obligations equally on enterprise service providers and their customers by extending application to providers of all "**hosting services**" (defined, by reference to the DSA, as a "service that consists of the storage of information provided by, and at the request of, a recipient of the service") and "interpersonal communications services" (**IPCS**) (Art. 1(2)). For enterprise service providers to comply with the Proposal's requirements, however, they would need to surveil and access the data of their commercial and public sector enterprise customers, including European governments, academic institutions, and businesses. Microsoft does not believe the Regulation is intended to impose monitoring obligations on technology providers providing enterprise services, as such obligations would require them to monitor the communications or other content of their commercial entity or public sector agency customers and their employees or other end-users. This point should be clarified in the Regulation.

Enterprise service providers who provide Software as a Service, Infrastructure as a Service, and Platform as a Service technologies (collectively, **cloud services**) to enterprise customers are extremely limited in what they can (or should) do with the data controlled by their enterprise customers. As a contractual matter, cloud service providers often do not have visibility into or control over the specific items of content that their enterprise customers, and those customers' end users, store and share on their services, meaning they cannot scan, modify, remove, or otherwise interact with individual pieces of content. An enterprise cloud service provider typically

does not have the ability or right to scan and assess customer data in a way that would allow for targeted content moderation. To implement the detection and removal measures envisaged in the Regulation on enterprise cloud services would require a fundamental shift in the technical architecture, functionality, and business model for such services in the European Union, with far-reaching legal consequences for current and future enterprise customers, including government agencies.

Enterprise cloud service providers also typically do not have direct relationships with individual end users of those services (e.g., the enterprise customer's employees or customers), and don't have a contextual understanding of how end users interact with those services. Therefore, enterprise cloud service providers are not well positioned to actively monitor and enforce content moderation decisions regarding end user content.

The proposal for the E-Evidence Regulation, for example, requires law enforcement agencies to issue demands for data to corporate users of certain infrastructure services used to store or process data, not to the providers of those services, unless doing so would not be appropriate (e.g., where it might jeopardize investigation). The Regulation should take a similar approach in the context of detection and other orders.

We recommend that the Proposal be amended to (i) advise that, where feasible, removal and detection orders be sent to enterprise customers in the first instance and (ii) clarify that enterprise service provider's responsibility under the Regulation is limited to options such as (a)discontinuing services or (b)reporting a customer to the relevant regulator in cases where it is notified that its customer has failed to comply with its obligations under the Regulation. The unique situation of enterprise services could be explicitly acknowledged in Article (4)(2)(b). Noting that mitigation measures will necessarily differ for enterprise services could appropriately recognize the limitations for enterprise cloud providers (as outlined above) and ensure any order to detect or remove content is proportionate (with detection orders remaining a measure of the last resort for all services).

3. Ensure measures to detect and prevent OCSEA are practical and implementable

As outlined earlier, there is a need to ensure that the Proposal's approach to the detection and prevention of OCSEA also considers individual rights to privacy and data protection. We are concerned that the current Proposal may require further work to ensure that it balances considerations of privacy, safety, and security in a way that can be implemented in practice. Below are some instances in which the proposed measures may raise practical challenges for providers:

The accuracy of online detection solutions. The Regulation places significant weight on the need for "sufficiently reliable detection technologies . . . that . . . limit to the maximum extent possible the rate of errors regarding the detection" of OCSEA (Art. 7(8)). Technology has not yet

achieved this standard in relation to the types of detection activities that the Proposal envisages, however — in particular in relation to detection of child solicitation and unknown child sexual abuse material. Article 10(3)(d) similarly points to the importance of the reliability of technologies where providers are determining which technologies to use in response to a detection order. While the accuracy of detection technologies is an important factor in determining which solutions providers should deploy, the Regulation should expressly acknowledge that in some scenarios, it will be necessary to balance the need for effective technologies against the need to limit the rate of errors. While providers work to detect and prevent OCSEA, those that create and disseminate OCSEA work to circumvent our technology. Therefore, the Regulation should also acknowledge the need to maintain the space for innovation and technological development (especially with respect to child solicitation and unknown child sexual abuse material). Unfortunately, technology solutions are not at a point where industry can remove the need for human intervention and review.

In this regard, we also note that the Commission's Impact Assessment of the Regulation refers to a Microsoft technology that can detect child solicitation with 88% accuracy. (This figure also has been referred to on various occasions in the debate around this file.) We recommend against reliance on this figure when discussing EU policy. This figure relates to a single English-language technique trained on a small data set of known instances of solicitation within historic text-based communications, and in all cases merely serves to flag potential solicitation for human review and decision as part of a wider moderation process.

Encrypted data. As identified by the EDPB and EDPS in their joint opinion on the Regulation, detection technologies such as PhotoDNA cannot be used on end-to-end encrypted data. As such, implementing detection orders on encrypted services will pose very practical technical challenges.

Equally, end-to-end encryption is both widely available and viewed by many users—including many governments—as essential to protecting the privacy and security of their information. It is therefore vital that the Regulation does not constrain covered providers from offering such encryption, particularly if enterprise services remain in scope of the proposal.

Recital 26 could be read to suggest that detection orders may lead providers to cease offering end-to-end encryption, to break encryption they apply, or to build "backdoors" into any encryption they do offer. This would be problematic in many respects:

- Such a requirement would make currently secure services vulnerable to hackers and other bad actors, thereby undermining EU users' trust in online services and potentially degrading the integrity, confidentiality and availability of those services.
- Bad actors will also continue to use end-to-end encryption (e.g., by migrating their communications and content to services that continue to offer it, for example because they operate outside the scope of EU jurisdiction). Thus, any obligation that risks weakening end-to-end encryption could reduce security protections for EU enterprises and consumers while at the same time having little or no impact on fighting OCSEA.

Before adopting any Regulation that could be read to hinder the ability of providers to offer robust encryption, the EU institutions should engage in a meaningful debate with all stakeholders to determine whether the benefits of such an obligation outweigh the significant risks it would entail. This should include consideration of alternative methods to detect safety risks and on creating the conditions for continuing technological innovation.

4. Criteria to assess risk

The lack of objective, measurable criteria for all providers, and particularly app stores, to assess and mitigate risk will pose significant challenges and may have unforeseen consequences. As identified by the EDPB and EDPS in their joint opinion on the proposed Regulation, the criteria for assessing the risk that OCSEA will take place on a covered service are broadly and generically framed (e.g., references to "the manner in which users use the service and the impact thereof on risk" as a criterion for assessing risk). As a result, many providers may not be clear what is required to comply. Similarly, it is not clear when a service will be used "to an appreciable extent" for the purposes of OCSEA—meaning that providers will not have certainty about when they might be subject to a detection order. To address this lack of foreseeability, and to avoid the risk of inconsistent application between Member States, the Regulation should be more concrete about the criteria for assessing and mitigating risk, and the circumstances in which authorities may issue orders.

This is particularly relevant to app stores, which must assess whether "each service offered through the software applications that they intermediate presents a risk of being used for the purpose of the solicitation of children," and take specific measures in relation to such apps (Art. 6). Numerous apps could be seen as "presenting a risk of being used for the solicitation of children." Indeed, many apps, such as social media, messaging/communication services, and online games, are widely used by children today and for that reason alone arguably "present a risk of being used for the purpose of solicitation of children". Further, Article 6 does not specify the criteria app stores should use to assess risk, instead stating only that "the provider shall take into account all the available information". The discretion provided to app stores in proposed Article 6(3) to hide processes and criteria for determining the potential risk of child solicitation (in cases where exposing them may reduce their effectiveness) may further obscure unfair or ineffective processes from the public and developers.

Ultimately, the proposed Article 6 would place app stores in a position where they can (and in fact must) pick apps that children are allowed to download and apps that are deemed "adults only" due to risk of child solicitation based on vague criteria that they choose, interpret, and administer in their own discretion. This may lead to popular, well-known apps (as well as apps published by platform owners themselves) being widely available to all users, while new or unpopular apps from

third-party developers are deemed "risky" and only made available to a subset of users. There is also no requirement for any appeal/redress process for affected developers.

Further, as a practical matter, app stores are not well equipped to make this kind of risk assessment on many kinds of third-party apps, let alone hundreds of thousands or millions. App review and certification is already a time-consuming and costly process for those app stores that attempt to apply rigorous quality and safety criteria before distributing apps. App stores do not have expertise in assessing risk of child solicitation in the broad variety of types and genres of apps that they may distribute. App stores would be left to develop and apply their own subjective criteria to assess this risk—which would be unlikely to meet the goals of Article 6, as such criteria potentially could be ineffective or misapplied. This would also be problematic for developers, who rely on app stores having consistent and predictable app review/certification criteria, as well as for app stores themselves, who need consistency to make their services attractive to developers.

5. Align the Regulation with other EU laws to minimize potential conflicts

Microsoft welcomes the Commission's efforts to harmonise the rules on preventing OCSEA, reducing the possibility for variation between Member States and driving a comprehensive EU response to this harm. However, the EU institutions should carefully assess how the Regulation would interact with other EU and Member State laws, and should adopt provisions that mitigate the risk of conflicts, including with respect to:

- *The ePrivacy Directive and the draft e-Privacy Regulation (hereinafter ePR)*. The Regulation should ensure that providers of IPCS in scope of the ePD, or respectively the ePR (incl. IPCS that are ancillary to other services), are permitted to process communications content and metadata for the purposes of detecting and preventing OCSEA, when accompanied by appropriate safeguards.

- *The GDPR*. The proposed Regulation should ensure that a provider's good-faith efforts to comply with a detection order do not give rise to liability under the GDPR; a provider should not be forced to choose between compliance with the Proposal or the GDPR. In addition, where a detection order would require a provider to take steps that the provider believes are inconsistent or in conflict with an SA's recommendations, the Regulation should require judicial authorities to specify the precise measures that the provider must undertake. Likewise, Coordinating Authorities (under Article 5(4)) should have no power to require a provider to "introduce, review, discontinue, or expand" a mitigation measure where the provider has a reasonable belief that doing so would be inconsistent with its obligations under the GDPR or other data protection or privacy laws. At present, however, the proposed Regulation does none of these things. Further, the proposal does not provide sufficient guidance to providers attempting to develop an implementation plan for a

detection order where the provider's competent SA and a Coordinating Authority have conflicting expectations, nor any clear process for how any disagreement between regulatory authorities might be resolved.

- *The Digital Services Act (DSA)*. The proposed Regulation (recital 8) helpfully clarifies that it will be *lex specialis* to the DSA, and that specific obligations are complementary to, and can draw on, measures taken to comply with the DSA (e.g., conducting risk assessments and taking risk mitigation measures (*see* Recitals 15-16)). The Regulation should also make clear that the mechanisms available to users under the DSA do not apply to a provider's actions under the Regulation, including removing content. In addition, more clarity is needed as to the interplay between the risk assessment and mitigation requirements and the related obligations under the DSA. The DSA also requires very large online platforms to identify, analyse, assess and mitigate systemic risks their services pose to the protection of children, which creates a potential overlap between the two legal instruments. To avoid any risk of duplication, we recommend clarifying that a risk assessment conducted for one purpose would also suffice for the other.

The Regulation should also include a mechanism to resolve conflicts where compliance with obligations under the Regulation would require a provider to violate a third country law applicable to it. Indeed, some jurisdictions — including the United States — strictly limit the dissemination of OSCEA content to authorities other than to domestic law enforcement (or, in the United States specifically, the National Center for Missing and Exploited Children (**NCMEC**). Providers should not be required to violate one country's law to comply with their obligations under the Regulation. The Commission's proposal for the E-Evidence Regulation contains a mechanism designed to address conflicts between EU obligations and third country laws, which this proposed Regulation could draw on, with some potential refinements.

6. Provide limitations on civil and criminal liability for good faith efforts to comply

Article 19 of the Regulation exempts providers from liability for "child sexual abuse offences" where they carry out, in good faith, activities necessary to comply with the Regulation's rules.

Although we welcome this provision, providers may face other types of civil and criminal liability because of their good-faith efforts to comply with the Regulation. For instance, they may face claims for interception of communications, or civil claims for infringements of data protection laws, defamation, or breach of contract. Even where these claims are without merit, providers may face significant administrative burdens and costs in defending against them, which may act as a deterrent to robust compliance.

Article 19 should be expanded accordingly, and providers acting in good faith to comply with the Regulation should be exempt from all types of criminal and civil liability under both EU and Member State law.

7. Impose appropriate safeguards on powers of Coordinating Authorities

We welcome the fact that the Regulation imposes safeguards on the issuance of detection and removal orders by judicial and independent administrative authorities. These should help ensure that such orders are necessary and proportionate and take adequate account of the fundamental rights and legitimate interests of victims, all users and service providers.

We note with concern, however, that Article 5(4) appears to grant Coordinating Authorities the power to require providers to "introduce, review, discontinue or expand" mitigation measures, but without any of the procedural safeguards associated with detection and removal orders. While we appreciate that the Regulation requires Coordinating Authorities to be independent, this alone is not an adequate safeguard.

We urge policymakers to add such safeguards. For example, the Regulation could require Coordinating Authorities to obtain an order from a judicial or independent administrative authority before requiring providers to take any action that goes beyond the provider's chosen mitigation measures and that could adversely impact the fundamental rights or legitimate interests of any user.

8. Clarify the role and powers of the EU Centre

Microsoft welcomes the establishment of the EU Centre, in particular its role in maintaining a database of indicators of OCSEA (which, consistent with the definitions in Articles 2(l), (o) and (q) of the proposed Regulation, will be indicators of criminal conduct), providing training data for detection technologies, and coordinating with national Coordinating Authorities. We also welcome the acknowledgment that providers should not be expected to assess the legality of content but that the Centre can receive reports of suspected OCSEA based on a terms of service violation.

We note, however, that the EU Centre's role would overlap somewhat with that of NCMEC in the United States, meaning that many international providers will have multiple, possibly different, reporting duties to these authorities. To avoid conflicting obligations or overlapping requirements, the EU institutions should consider authorizing the EU Centre to share information with NCMEC and other, similar institutions in third countries. Such coordination could help ensure that

providers are not subject to conflicting legal obligations and could make reporting and acting on OCSEA more effective and efficient.

Although Microsoft also welcomes the fact that the EU Centre will maintain a central list of indicators of OCSEA (Art. 44), the Regulation should clarify that providers can lawfully detect OCSEA in ways other than scanning based on these indicators—for example, using indicators endorsed by other institutions (e.g., NCMEC), NGOs such as the Internet Watch Foundation, or maintained by a service provider itself. Replacing these hash lists (some of which have been developed over many years), will be a challenging task for the EU Centre. Maintaining access to an individual company's own indicators is particularly critical with respect to developing and training technologies to flag suspected child solicitation behaviors, given the language and other indicators of risk may vary significantly from service to service, based on the different ways users communicate and act on different services.

Moreover, a single conversation may signal that risky behavior is taking place on a service but may be unlikely to rise to a threshold of illegality for grooming (and thus would not be covered by the definition of solicitation of children under Article 2(o) of the Regulation). We are therefore concerned that the Regulation may have the unintended consequence of significantly inhibiting service provider efforts to detect and report risky behavior that may not meet EU criminal thresholds but that nonetheless breach a service's terms of use. As outlined earlier in this paper, there is a consequential risk that the amount of OCSEA detected in the EU could be significantly reduced.

9. Clarify the scope of obligations to ensure they are proportionate

Although we recognize the care that has gone into articulating many of the terms and provisions set out in the Regulation, others would benefit from greater clarity and precision.

In particular, Article 4(3) requires IPCS providers to conduct age verification if there is "a risk of use of their services for the purpose of solicitation of children." Because this provision fails to articulate any quantum of risk (e.g., "substantial risk"), it could in practice require all such providers to take these measures, which would be inconsistent with principles of data minimization and disproportionate (particularly in the case of services that permit anonymous use, which are of vital importance for many marginalized or minority communities).

The Regulation also empowers the EU Centre to "conduct searches on hosting services" (Art. 49(1)). It does not, however, provide clarity or limits on what constitutes a "search," and imposes no safeguards around such searches, with respect to the interests of either providers or users of covered services. To remedy this, we urge policymakers to require the EU Centre to obtain an order from a judicial authority, subject to the protections set out in EU and Member State law, before conducting any search of the provider's services. We also recommend providing further clarity in the Regulation on what would constitute a "search" in this context, especially given our

earlier points on the need to clarify obligations for enterprise service providers and to ensure that these are proportionate.

* * * * *

Microsoft appreciates the opportunity to share these views on the proposed Regulation. We look forward to further discussions with policymakers and other stakeholders on this important initiative.