Microsoft Recommendations on the EU Proposed Regulation Laying Down Rules to Prevent and Combat Child Sexual Abuse

February 2024

Microsoft has a long-standing commitment to online child safety and recognizes the responsibility online service providers have to prevent harm while respecting human rights including privacy and freedom of expression. As such, we welcome the Commission's Proposal for a Regulation laying down rules to prevent and combat child sexual abuse ('The Proposal').

While we welcome the 2022 Proposal's risk-based approach we remain **concerned** that both the Commission's and Parliament's positions propose a mandatory-only approach to detection orders that would **unduly restrict companies' ability to prevent harm of child sexual abuse and exploitation**.

In this context, Microsoft **welcomes** the **Polish Presidency's compromise text (28/01/25)** and its approach to **voluntary detection, for three reasons**:

1. The Polish Presidency's permanent extension of the ePrivacy derogation will ensure that Interpersonal Communication Services (ICS) providers can continue to deploy tried and tested detection technologies that are central to the prevention and detection of child sexual abuse and exploitation.

In 2009, Microsoft created in partnership with Dartmouth University, PhotoDNA, a robust hash-matching technology that identifies duplicates of known child sexual abuse imagery in order to detect, remove, and report this heinous content. PhotoDNA, as well other technological means of detecting child sexual abuse material within ICS, account for the tens of millions of reports of child sexual abuse material (CSAM) made to authorities every year. **At Microsoft, 99% of the child sexual abuse and exploitation imagery actioned on our services was detected through the voluntary application of detection technologies**. Technology is critical to address this harm at scale. Putting the ePrivacy derogation through a long-term legal regime will offer welcome legal clarity to providers that deploy technology to reduce the harm on their services. Microsoft therefore welcomes the Polish Presidency's proposal to enable continuing voluntary detection measures.

2. The additional privacy and transparency safeguards and conditions will ensure that voluntary detection is not deployed at the expense of the fundamental right to privacy.

Microsoft also welcomes the proposed additional safeguards and accountability required for providers to take voluntary steps to protect their services. The additional data protection requirements, including a data protection impact assessment, consultations with stakeholders, and transparency measures will all serve to facilitate trust and confidence in industry practices.

3. Voluntary detection, in tandem with additional safeguards, will serve to promote Trust & Safety innovation.

By maintaining the legal basis for voluntary detection of known CSAM, new CSAM and the solicitation of children, the Polish Presidency text will also support an environment that promotes continued technological innovation. The nature of this harm means that perpetrators are always seeking to circumvent tooling designed to protect children.

Moreover, we are in an environment where artificial intelligence is driving significant advancements in a range of fields, including trust and safety. Ensuring that the voluntary framework allows for innovation, by including requirements for high-risk services to contribute to the development of detection technologies, will ultimately promote innovation in this field, and raise the bar for child protection across the eco-system.

Microsoft recommends, where possible, that the processes around risk categorization are made as efficient as possible. As written, the process of risk categorization (and possibly, recategorization) is lengthy and creates significant red-tape for service providers, the EU Centre, and the Coordinating Authority. In the event a service labels itself or is labelled high-risk, it may be subject to additional prevention measures, inform its users of the risk, undertake engineering cycles to showcase reduced risk and report on such, and contribute to the operational, financial and technical development of detection tooling.

Not only that, but the Centre and Coordinating Authorities will also have to remain available to comb through thousands of risk assessments, the possibility for new categorizations, privacy impact assessments, and the success of any new mitigation measures introduced. To optimize the time of all stakeholders involved, and ensure the best result is driven from these procedures, **we recommend that the risk assessments be mandated only to ICS providers, and made optional for hosting providers**.

We recognize that in a voluntary-only regime, checks and balances must be implemented to ensure all players are measured against the same bar. However, we recommend considering ways in which the process can be streamlined for providers undertaking good faith efforts to address CSAM risks on their services.

We **also recommend** that provisions related to age verification are put aside for this specific regulation and consulted on separately. While age assurance remains one of the many ways in which children can be better protected only, this technical solution warrants to be examined specifically, following extensive multi-stakeholder consultation. A variety of workstreams are also seeking to develop a harmonized EU approach to age verification, notably through the Digital Services Act's Article 28 – which take into account its technical overlap with the eIDAS Regulation. We recommend that, to avoid conflicting or repetitive rules, the CSAM Regulation only propose age assurance, or verification, as possible mitigation measure – as opposed to an obligatory provision specific to app stores.

In conclusion, in the context of this continued deadlock in Council, and the pressing deadline for the expiration of the ePrivacy derogation (April 2026) Microsoft recommends that **co-legislators strongly consider the approach** put forth by the Polish Presidency. The proposal advances privacy and safety protections for Europeans by providing a clear legal framework and ensures the benefits of time-tested voluntary detection remains in companies' toolkits. Microsoft welcomes the opportunity to provide feedback to this important topic. We remain ever committed to the whole-of-society fight against child sexual exploitation and abuse and available to discuss any questions you may have.