Brussels, 22 February 2021

Dear Honorable Member of the European Parliament,

We welcome the collective efforts of the EU institutions on the proposal for a temporary derogation from certain provisions of the e-Privacy Directive for combatting child sexual abuse material online (the "interim derogation"). We care deeply about the safety of children online, and we invest heavily in industry-leading tools that help prevent, detect, and report abusive behaviour relying on traffic and content data. We believe the proposed interim derogation could support our efforts to help keep children safe.

We are grateful for the effort made by all parties in finding a path forward and, in particular, the provisional compromise reached to move away from a one-in-50-billion error rate in favour of a more pragmatic approach that requires limiting the rate of error "as much as possible" and rectifying any such errors promptly. A requirement of a specific and unrealistic error rate would exclude all current technology used to detect child sexual abuse material (CSAM) as no technology in use today by any company operates to that level of accuracy. Moreover, we are unaware of any peer-reviewed evidence attesting to the fact that any technology in use meets this bar. Establishing such an unrealistic threshold would preclude any company from continuing to detect child sexual abuse material and activity.

There are, however, further issues still to be agreed that, if not resolved, could significantly hinder our ability to continue to fight child sexual abuse and exploitation online, putting children and the prosecution of offenders at risk.

The elements in question are:

- Reporting to the competent national law enforcement authorities
- Retention of content data for a period no longer than three months
- Coherence and consistency with existing frameworks
- Concrete elements of suspicion
- Information requirements for positive hits of CSAM, and
- Local age of consent and Professional privilege.

We address our chief concerns with each of these elements immediately below.

Reporting to the competent national law enforcement authorities
In its amendment 28, the European Parliament proposes in Article 3(1) sub (ea) that *"Every case of a reasoned and verified suspicion of online child sexual abuse is immediately reported to the competent national law enforcement authorities."* Under the current system, U.S. providers are legally required to report child sexual abuse content to the National Centre for Missing and Exploited Children's (NCMEC) CyberTipline. NCMEC has an international hub function - it receives all such referrals and subsequently triages and passes that information to law enforcement authorities all over the world, including to law enforcement agencies in Europe. This happens either directly or through a clearinghouse. The proposed amendment undermines the existing effective global system of reporting by creating a parallel and duplicative reporting structure, opening the system to fractured efforts and potential errors. This would challenge the well-established and functioning international system that has delivered numerous positive

outcomes for law enforcement agencies around the world. Significant changes to the existing reporting system could result in important unintended consequences and require careful consideration about design and resources that cannot be addressed by an interim regulation and are currently being debated as part of the wider EU CSAM strategy.

Retention of content data for a period no longer than three months
The European Parliament's provision in Article 3(1) sub (db) and its data retention "hard stop" of three months conflicts with requirements on U.S. providers, which are subject to preservation obligations of 90 days and potential extensions. Such a finite period seriously runs the risk of undermining ongoing investigations by global law enforcement. The current system relies on targeted preservation of data to ensure critical evidence remains available and can be leveraged to bring offenders to justice.

Coherence and consistency with existing frameworks
The amendments currently being debated include an obligation for providers to priorly consult with the Data Protection Authorities (DPAs) for technologies within the scope of the interim regulation. This requirement deviates from GDPR principles (e.g., risk-based approach), which only requires this consultation if the data protection impact assessment suggests that the risk of processing data is high and cannot be otherwise mitigated. The text of the derogation should follow this same principle. Further, the general approach on the ePrivacy Regulation proposal adopted by the Council's draft adopted on 10 February does not require a prior consultation when the provider is accessing communication content, but maintains the risk-based approach (art.6a (2)). The interim derogation should do the same.

Concrete elements of suspicion
Recital 11 includes a reference to the need to look only into specific communications in cases of concrete elements of suspicion of online child sexual abuse. This requirement appears to be based on a misunderstanding of how the technologies for the detection of CSAM actually operate and can impact providers' ability to detect such content at scale. CSAM detection technology looks for matches of content previously identified as child sexual exploitation and abuse material, helping to pinpoint the elements of suspicion. Therefore, it is only by applying the available technology that we can form a concrete suspicion of activity related to child sexual exploitation and abuse.

Information requirements for positive hits for CSAM
The European Parliament's amendment 28 in Article 3(1) sub xii requires providers to disclose information to a user in the event of a "positive hit for online child sexual abuse material" unless doing so would be prejudicial to an ongoing investigation. This provision is practically impossible for providers as we cannot determine at scale when an investigation may be commenced, when it is concluded, or under what circumstances disclosure would or would no longer interfere with an ongoing investigation by law enforcement. Moreover, notices to users, who may be subject to a law enforcement investigation, would likely result in a range of adverse outcomes, including, but not limited to, destruction of evidence, self-harm, and violence directed at others, including the child victims of these crimes. The proposed revised text fails to address these concerns.

Local age of consent rules
The European Parliament's amendment on Recital 4a, talks about the need to take into account localised age of consent rules and barring reporting of imagery when the subjects are over the age of consent. This requirement assumes providers have information about users that are not actually known in practice, and thus places an unreasonable burden on industry to determine a country of origin and unattainable precise age-markers.

Professional privilege
The European Parliament's amendment 28 in Article 3(1) sub xiii excludes communications protected by professional privilege (e.g., attorney/client and doctor/patient). However, it is technically impossible for service providers to determine whether such a privilege exists or not. Even if providers were to permit users to self-designate privileged communications, there would be no ability to verify this designation, and it could create a dangerous loophole that would allow child predators to opt into shielding their communications from CSAM detection.

We do not tolerate child sexual abuse and exploitation on our services and have over many years worked diligently to develop the appropriate technologies to achieve this aim. Having an enabling legal framework for providers is essential for the continuation of our efforts to detect and remove child sexual exploitation and abuse material from our services. While a longer-term solution is being debated as part of the wider EU strategy for a more effective fight against this crime, we encourage EU lawmakers to agree a workable interim solution that urgently addresses the current ambiguity and uncertainty.

We also wish to highlight our collective commitment to ensure private and safe communications for our users and welcome the European Parliament's recognition of the role that encryption plays in supporting this aim. We believe a workable derogation that balances core privacy interests and allows for existing CSAM prevention, detection, and reporting efforts to continue is achievable by addressing the issues outlined above.

We look forward to our continued dialogue on this important matter. We stand ready to answer your questions and to support you with the information needed to progress this file.

Yours sincerely,

Cornelia Cornelia Kutterer, Senior Director, EU Government Affairs, **Microsoft**

Remy Malan, Vice President of Trust and Safety and Chief Privacy Office, **Roblox**

Marc-Antoine Durand, Chief Operating Officer, **Yubo**

François-Xavier Dussart, Senior Director, EU Public Policy, **Verizon Media**

Aura Salla, Public Policy Director, Head of EU Affairs, **Facebook**

Karen Massin, Director, Government Affairs and Public Policy, European Institutions, **Google**

Jean Gonié, Director Europe Public Policy, **Snap Inc.**