Microsoft
Corporate, External & Legal Affairs
Rue Montoyer 51
B-1000 Brussels

Microsoft

Privileged and Confidential

President von der Leyen, Commissioner Johansson, Commissioner Breton
European Commission
Rue de la Loi 200
B-1049 Brussels

Brussels, 2 September 2020

Dear President von der Leyen, dear Commissioners,

We are writing in the context of your recently published EU Strategy for a more effective fight against child sexual abuse (the "Strategy"). We very much welcome the Strategy and its holistic approach to reenforce and increase efforts against these horrendous crimes, which target the most vulnerable. We stand ready to support the Commission's objective with this Strategy, both as industry's representative to the Policy Board of the WePROTECT Global Alliance and as a member of the EU Internet Forum.

With this letter, we would like to emphasize the urgency of the action item referenced below to avoid preventing providers of electronic communications services from detecting child sexual exploitation and abuse imagery on their platforms and services.

In a first stage, as a matter of priority, the Commission will propose the necessary legislation to ensure that providers of electronic communications services can continue their current voluntary practices to detect in their systems child sexual abuse after December 2020.

In 2009, in cooperation with Dartmouth College and Dr. Hany Farid, Microsoft created PhotoDNA, a tool described by some as the single, most-significant technology contribution to-date in the fight against the online proliferation of child sexual abuse imagery. PhotoDNA can be used to find copies of an illegal image with incredible accuracy across the billions of images shared online every day – even when the photos themselves have been altered. Later that year, Microsoft donated PhotoDNA to the U.S. National Center for Missing and Exploited Children (NCMEC), and now licenses it for free to some 175 companies and organizations around the world, including government agencies, domestic and international law enforcement, and many in industry. We continue to use PhotoDNA on our services at Microsoft, including OneDrive,

Xbox, and Skype. In addition, a few years ago, we made a version of PhotoDNA available as a cloud service to our qualified enterprise customers. PhotoDNA Cloud Service enables businesses to protect their assets, interests, and customers by automatically detecting and reporting the distribution of child sexual exploitation and abuse imagery.

As comprehensively described in your strategy, as of December 2020, the ePrivacy Directive will equally apply to so-called over-the-top communication providers ("OTTs") due to the European Electronic Communications Code. [redacted]

While this unintended consequence has been discussed during Council negotiations on the ePrivacy Regulation, it is imperative to solve the issue now – that is, before the EECC enters into force on 21 December 2020 – in order to avoid legal obstacles that would hinder OTTs from continuing to detect and prevent this type of illegal activity.

As you also outlined in your strategy, online child sexual exploitation and abuse has evolved well beyond the simple sharing of illegal images. The grooming of children for sexual exploitation in chat conversations; the live, on-demand streaming of child sexual abuse; and the availability of instructional, "how-to" manuals for sexual torture are just a few ways in which these horrific crimes have expanded online in recent years. To help prevent and to fight back against this illegal content and activities, Microsoft, in conjunction with others in industry, recently developed and released a new technique for detecting child online grooming for sexual purposes in historical text-based message conversations. (More information is available here.) Industry and other partners also seek to do more to combat the complex and complicated issue of the live-streaming of child sexual abuse, and we are always looking to train and test innovative technologies to help identify new, never-before-hashed imagery via artificial intelligence and machine learning.

All of these efforts are aimed at advancing child safety online. Technology is continually evolving, as are the methods by which criminals are abusing online platforms and services. In this regard, any regulation that seeks to ensure both privacy and online child protection needs to be future-proofed.

In brief, the fight against sexual child exploitation and abuse online requires the ability of providers to lawfully and actively:

- **Detect, disrupt, remove, and report** illegal child sexual exploitation and abuse imagery and related activity taking place through electronic communications on our platforms and services;
- Leverage both **automated tools and human moderators** to detect, disrupt, remove, and report such content and activity to the U.S. National Center for Missing and Exploited Children (NCMEC); and
- Innovate and **create new tools and techniques** to not just detect and combat known imagery, but also other forms of child sexual exploitation and abuse such as online grooming, live-streamed abuse, and new never-before-hashed imagery.

We welcome the Commission's intention to bring forward a targeted legislative solution to allow current voluntary activities to continue after 21 December 2020. As noted in your Strategy, such a solution would allow to bridge the time necessary for the adoption of a new longer-term legal framework.

Yours sincerely,

[redacted]

[redacted]

[redacted]

[redacted]

Vice President
European Government Affairs

Chief Digital Safety Officer

Cc:
Vice President Šuica
Vice President Vestager
Vice President Jourova
Commissioner Reynders