EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY
Digital Society, Trust and Cybersecurity
Cybersecurity and Digital Privacy Policy

Brussels,
cnect.ddg1.h.2(2020)5166553/AP

Mr. Jeremy Malcolm
Executive Director
Prostasia Foundation

E-Mail: jeremy@prostasia.org

Dear Mr. Malcolm,

Thank you for your email of 2nd October 2020 sent to European Commission President Ursula von der Leyen, where you express your concern about possible methods to detect child sexual abuse in end-to-end encrypted communications. Ms. von der Leyen asked me to reply on her behalf.

I agree that the fight against child abuse is a priority for the European Union. On 24 July 2020, the Commission adopted an EU strategy for a more effective fight against child sexual abuse, which sets out eight initiatives to implement and develop the legal framework, strengthen the law enforcement response and catalyse a coordinated multi-stakeholder action in relation to prevention, investigation and assistance to victims. In particular, the Commission will propose in the second quarter of 2021 sector-specific legislation to tackle child sexual abuse online more effectively.

I am aware that certain providers of number-independent interpersonal communications services are already using specific technologies to detect and report child sexual abuse online and remove child sexual abuse material on their services, and that these services will fall within the scope of the ePrivacy Directive on 21 December 2020. Following the strategy, the Commission recently proposed a Regulation with the sole objective of enabling providers of number-independent interpersonal communications services to continue their current voluntary practices to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material in their systems after December 2020, pending adoption of the announced long-term legislation.

The proposed Regulation respects fundamental rights, including the rights to privacy and protection of personal data. It provides for a series of safeguards to ensure that providers of number-independent interpersonal communications services deploy the types of technologies that are the least privacy-intrusive in accordance with the state of the art in the industry.

Providers of certain online services are well placed to help prevent, detect and report child sexual abuse that occurs on their own infrastructures. The National Centre for Missing and Exploited Children (NCMEC) in the US received almost 17 million referrals of child sexual abuse from these companies in 2019. These reports have been instrumental in rescuing children from ongoing abuse in the EU and globally, often providing the only lead to law enforcement to start an investigation in cases which would otherwise have gone unreported.

Moreover, the sharing of material that evidences this sexual abuse taking place in the real world continues to perpetuate the harm caused to the victims and helps to fuel the demand for more and new material.

I also would like to stress that encryption is an important means of protecting confidentiality and is widely recognised as an essential tool for security and trust in open networks. However, the use of encryption should be without prejudice to the powers of competent authorities to safeguard national security and to prevent, investigate, detect and prosecute criminal offences, in accordance with the procedures, conditions and safeguards set forth by law and in compliance with Fundamental Rights.

I hope you find this information useful.

Yours sincerely,

(eSigned)
Jakub Boratyński
Head of Unit