Ms Ursula von der Leyen, President of the European Commission
Ms Margrethe Vestager, Executive Vice-President for A Europe Fit for the Digital Age
Mr Didier Reynders, Commissioner for Justice
Ms Valerie Setti, European Commission Coordinator for the Rights of the Child

xx September 2020

Dear President von der Leyen, Vice-President Vestager, Commissioner Reynders, and Coordinator Setti:

Technical solutions to detect child sexual abuse in end-to-end encrypted communications

We, the undersigned civil society organizations and experts, are writing to express our deep concern about measures that may be under consideration by the Commission to enable end-to-end encrypted (E2EE) communications to be scanned for child sexual abuse material (CSAM). Despite their good intentions, these measures would constitute a veiled form of mass surveillance, which is incompatible with the fundamental human right of privacy as guaranteed by Articles 7 and 8 of the EU Charter of Fundamental Rights, as well as Article 8 of the European Convention on Human Rights. We further believe that the impact of these measures, if adopted, will be to undermine the security and safety of adults and children alike, while failing to deter abusers from sharing such images by other means.

Although our concerns have been animated by the recent release of a leaked expert technical paper to the Commission[1] on this topic, the fact that the Commission had commissioned this expert study is in the public domain,[2] and the parameters of the solutions being considered have also been previously discussed.[3] In short, it is common to all shortlisted proposals that the confidentiality of image and video content on an end-user's device will be compromised to enable surveillance of that content. Even though the expert report suggests that these measures would only be deployed only for the detection of CSAM, there is no technical reason why the same technologies could not be used to detect other unlawful, or indeed, lawful, content.

In two of the shortlisted options, the user's Internet-connected device will first convert the content into hash values that uniquely identify it, and these will be sent to their electronic service provider (ESP) for analysis. In the event that a match against known CSAM images is reported by ESP server, the device will then send full image and video content to the ESP, completely bypassing encryption. In the third shortlisted option, full image and video content

[1] Technical solutions to detect child sexual abuse in end-to-end encrypted communications, available at: https://t.co/9A2NoGKCv3?amp=1 [accessed 24 September 2020]
[2] European Union: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on EU strategy for a more effective fight against child sexual abuse, 24 July 2020, COM(2020) 607 final, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf [accessed 14 September 2020].
[3] Matthew Green, "Can End-to-End Encrypted Systems Detect Child Sexual Abuse Imagery?" (8 December, 2019), available at: https://blog.cryptographyengineering.com/2019/12/08/on-client-side-media-scanning/ [accessed 14 September 2020].

will be sent in the first instance, again completely bypassing encryption, where it will be analyzed in a "secure enclave" to which the ESP putatively would not have direct access.

The protection of children from sexual abuse, including the distribution of images of such abuse, is a vital responsibility for governments to undertake in concert with stakeholders from the private sector and civil society. As such we strongly support the Commission's undertaking to make the fight against child sexual abuse a priority for the EU.[4] However, just as child sexual abuse is not primarily a technological problem but a social one, so too the EU must look beyond purely technical solutions to address it. Indeed, as the Commission has acknowledged, this fight requires coordinated multi-stakeholder action in relation to prevention, investigation, and assistance to victims. The proposals in this technical paper do not reflect this balanced approach.

This reflects one of the technical flaws in the paper. In all of the scenarios illustrated in the paper, the result is said always to be that the recipient receives and decrypts an end-to-end encrypted message, even in cases where law enforcement was given exceptional access. Such access is inconsistent with a communications system that is fully secured with end-to-end encryption. Any "solution" that would weaken end-to-end encryption by requiring images and videos, or unique representations of them, to be shared with an intermediary is no solution at all. It undermines the fundamental feature of end-to-end encryption: that only the sender and the recipient will be able to understand the contents of a communication.

The paper uses "privacy" as a metric against which different approaches are measured, but it never defines the term. This shows a lack of technical rigor, and it has resulted in an inadequate assessment of privacy risks. Among the many unacceptable privacy risks that these "solutions" present, an ESP server, secure enclave, or CSAM hash database could be compromised to return a match for non-CSAM images or videos, thereby identifying individual users who possess those files. Similarly, once built into devices under a government mandate, this "solution" can be abused. A repressive government could order an ESP to use this technology to track files shared by whistleblowers and dissidents. A security hole in this complex "solution" could instantly transform millions of devices into unrestricted spying tools.

Even if each of these known and unknown vulnerabilities could somehow be identified and eliminated, the resulting surveillance regime still would not achieve the desired objective, as abusers would only have to shift away from European platforms to the many other E2EE encryption apps and services that are already freely available, in order to bypass the surveillance of their communications.

As a paper by Unicef has stressed, domestic laws on surveillance must comply with international human rights norms, including the right to privacy[5]. In practice, this means that government requests for communications data should be judicially authorized, narrowly targeted, based on reasonable suspicion, and necessary and proportionate to achieve a legitimate objective. Under international human rights law, measures that would restrict the

[4] Supra note 1.
[5] See 'Privacy, protection of personal information and reputation' by Unicef 2017.

use of encryption are deeply problematic as is the mass interception and blanket retention of communications data[6].

We respectfully urge the Commission to abandon this ill-fated approach, and instead to prioritize measures to address the many existing shortfalls and gaps that the Commission has already identified in the EU's response to child sexual abuse, including investment in interventions to prevent would-be perpetrators from offending to begin with.

Yours sincerely,

Article 19
Bits of Freedom
Center for Democracy & Technology
European Digital Rights (EDRi)
Global Partners Digital
Hermes Center
Internet Society
IT-Pol
Prostasia Foundation

[List in formation]

[6] See Report on encryption, anonymity, and the human rights framework, by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, May 2015.