27 October 2020

Open Letter: Civil society views on defending privacy while preventing criminal acts

Dear European Commission President Ursula von der Leyen,

Dear Commissioner Ylva Johansson,

Dear Commissioner Thierry Breton,

CC: Commission President Head of Cabinet Bjoern Seibert, Commission President Digital Adviser Anthony Whelan; Commissioner Breton Head of Cabinet Mr. Moutarlier; Commissioner Johansson Head of Cabinet Åsa Webber and Deputy Head of Cabinet Tom Snels.

We, the undersigned organisations, would like to share with you our views on the Communication on an EU strategy for a more effective fight against child sexual abuse material (CSAM) and the proposals deriving from it, including the interim Regulation amending the ePrivacy Directive and the internal discussion document "Technical solutions to detect child sexual abuse in end-to-end encrypted communications". In this letter we want to highlight **our concerns with some of the proposals** and request you to **ensure that privacy, data protection and other fundamental rights are respected in any policy initiative deriving from these documents and to ensure meaningful participation of civil society**, through public consultations and open meetings.

The signatories share the European Commission's goal to protect children. Child sexual abuse is a serious crime with extremely serious consequences for victims. **All forms of violence against children online and offline must be effectively eliminated**. Many effective measures to achieve that goal may be found outside of technology, ranging from public education and victim support to improved cross-border police cooperation. We welcome the Commission's work programme to secure Member State compliance with the many aspects of Directive 2011/92/EU. Many CSA websites are now hosted in Europe and we suggest that the Commission prioritise this non-technical work, and more rapid take-down of offending websites, over client-side filtering.

We want to highlight **five sets of fundamental rights problems posed by the three aforementioned documents**:

Lack of clarity of services covered and the legal basis for current practices

We welcome recital 11 of the interim Regulation which states that technologies used should be the "least privacy-intrusive in accordance with the state of the art in the industry and should not include systematic filtering and scanning of communications containing text but only look into specific communications in case of concrete elements of sus-

picion of child sexual abuse." However, it is not entirely clear which specific services, platforms, applications and technologies the Commission is referring to when stating that the scope will include "technologies for the processing of personal and other data" to detect CSAM, and under which legal basis (if any) the companies that offer services, platforms, applications and technologies are currently performing these practices.[1]

Lack of impact assessment and key consultations

We regret the complete lack of public consultations, impact assessments and solicitation of expert opinions from the Fundamental Rights Agency (FRA), the European Data Protection Supervisor (EDPS) and human rights organisations. The current justification of a rushed timeline given the entering into force of the European Electronic Communications Code is not acceptable given the potential impact on fundamental rights.

Normalisation of exceptional measures

We acknowledge the claim that the measures of the interim Regulation are of a temporary nature. However, we note that the period of application of the interim Regulation will continue until 2025 and we fear that, once adopted, the temporary measures it encourages will become accepted practice that will be renewed uncritically as a *fait accompli*. There are serious risks that this legislation of exception becomes the new accepted norm.

Empowerment of big tech companies

Some of the measures proposed in these documents would put private companies in charge of surveillance and censorship mechanisms that, because of their impact on fundamental rights, should be the responsibility of public authorities. In this regard, we encourage the Commission to carefully consider the impact on human rights of any filtering mechanism, including hash-matching technology to detect CSAM. **Any future initiative that uses hash databases to detect illegal material must be pursued within a strong rule-of-law framework that includes safeguards for fundamental rights; this would include ensuring any such database operates with open source software, is controlled by public independent institutions, and operates under full public scrutiny**[2] rather than relying on US technologies and databases handled by US organisations.[3]

1 The interim Regulation does refer in recital 2 to "voice over IP, messaging and web-based e-mail services" but there is no comprehensive annex of specific platforms, services, applications and companies affected by the interim Regulation (or exempted) that would clarify the actual impact of the measures. For example, we would benefit from a more detailed description of what Article 3 of the interim Regulation refers to when mentioning under the scope "*well-established technologies regularly used by providers of number-independent interpersonal communications services for that purpose before the entry into force of this Regulation, and that are in accordance with the state of the art used in the industry and are the least privacy-intrusive*".

2 This would require the preparation of data protection and human rights impact assessments, public consultations, opinions by key actors such as the Fundamental Rights Agency, the European Data Protection Supervisor, Data Protection Authorities, civil society groups and academics. The Commission should impose regular revision of the databases, external audits on the software and revision of practices by member states at least annually.

3 In the United Stated the technology used to detect CSAM (PhotoDNA) is developed by Microsoft and the hashed database of CSAM handled by the National Center for Missing and Exploited Children (NCMEC)

Potential attack on encryption

As studied by Der Spiegel,[4] some of the proposals that are recommended in that "Technical Solutions" discussion paper *de facto* amount to breaking end-to-end encryption, as they consist in pre-filtering of the messages on users' end devices with the help of an external server before these messages are encrypted and sent. This undermines the crucial technological safeguard of encryption, as EDRi has expressed in previous dedicated papers and in its recent letter to the German Presidency.[5] This is a slippery slope in a context of degrading rule of law and democratic principles in the EU.

In particular, the Technical Solutions paper is technically flawed in at least two ways. First, it measures different technical solutions against "privacy," but fails to define the term. Second, the favoured solutions the paper identifies all involve the result of law enforcement gaining exceptional access to content, while purporting to achieve the result that the recipient receives and decrypts a communication that was encrypted end-to-end. These two results are at odds: a service is not fully protected by end-to-end encryption unless only the sender and the recipient of a communication shared over the service can access its contents.

We urge the European commission to consider the full range of children's rights, including the right to privacy, freedom of expression, and to access to effective remedies for violation of these rights.

Encryption benefits children by ensuring the protection of their sensitive information. As UNICEF recognises, improving privacy and data protection for children is essential for their development and for their future as adults. UNICEF calls for any monitoring tools to "bear in mind children's growing autonomy to exercise their expression and information rights".[6] Weakening encryption and security for electronic communications services used by the general public is unlikely to be an effective measure in the fight against organised distribution of CSAM.[7] As Unicef has also stressed, domestic laws on surveillance must comply with international human rights norms, including the right to privacy. 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

4 https://www.spiegel.de/netzwelt/netzpolitik/eu-kommission-gegen-kindesmissbrauch-verschluesselung-bitte-nur-fuer-gute-menschen-a-8db88bf2-29c8-495c-83e9-818bf05d7d85

5 Specifically, we find it problematic that the "technical solutions" paper suggests as one of the possibilities covertly inserting a government participant in apparent "secure" chats, scanning content on user devices before the content is shared or directly allowing access to device encryption by governments. More generally, the paper introduces new avenues for access which directly undermine trust by introducing real-time censorship into communications that users expect to be private. By suggesting legal cover for client-side censorship, the Commission risks creating a precedent for introducing further restrictions upon the request under member state laws.

6 UNICEF's Toolkit on Children's privacy and freedom of expression: https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

7 There could be unintended consequences as well: Criminal actors could quickly switch to services without encryption backdoors, while ordinary citizens will lose critical protection against cybercrime and unlawful mass surveillance by intelligence services or private companies. Furthermore, we would like to recall how the Snowden revelations showed cases of the British intelligence service GCHQ, as well as other services around the world, harvesting intimate video chats in the context of "national security". Europe should at all costs forbid these types of general monitoring activities by public or private actors.

achieve a legitimate objective. Under international human rights law, measures that would restrict the use of encryption are deeply problematic, as is the mass interception and blanket retention of communications data.

For a meaningful impact on children's rights, we call for the debate on these proposals to be informed by opinions from the **European Data Protection Supervisor (EDPS)** and the **Fundamental Rights Agency (FRA).** In addition a public debate we call for the preparation of **public consultations** as well as adequate **impact assessments** on the different proposals that will derive from the documents discussed in this letter. Finally, **civil society groups, especially children rights' groups but also human and digital rights organisations, need to be involved and work together to find acceptable legal solutions**. Anything less will not necessarily protect children, but most likely make private communications for all, including children, subject to mass surveillance.

We look forward to discussing with you the issues covered in this letter.

Sincerely,
Diego Naranjo
Head of Policy
European Digital Rights (EDRi)
diego.naranjo@edri.org

List of organisations signing:

Advocacy for Principled Action in Government
Article 19
CDT- Center for Democracy and Technology
Civil Liberties Union for Europe (Liberties) - Europe
Coalizione Italiana per le Libertà e i Diritti civili (CILD) - Italy
Commission for The Disappeared and Victims of Violence (KontraS) – Indonesia
Defend Digital Me – United Kingdom
Democratic Society
Encryption Europe
European Digital Rights (EDRi) - Europe
Fundación Karisma - Colombia
Future of Privacy Forum
Global Partners Digital
Government Accountability Project
Hungarian Civil Liberties Union – Hungary
Internet Society
Irish Council for Civil Liberties (ICCL) – Ireland
Kenya Human Rights Commission (KHRC) – Kenya
Open Media
Peace Institute – Slovenia
Ranking Digital Rights
Xnet - Spain