

From: [REDACTED] <[REDACTED]@edri.org>
Sent: vendredi 22 avril 2022 13:07
To: EC PRESIDENT VDL
Cc: SEIBERT Bjoern (CAB-VON DER LEYEN); WHELAN Anthony (CAB-VON DER LEYEN); [REDACTED]
Subject: Re: Open letter: Protecting digital rights and freedoms in the legislation to effectively tackle child abuse

Dear European Commission President Ursula von der Leyen,

cc: Commission President Head of Cabinet Bjoern Seibert and Commission President Digital Adviser Anthony Whelan;

We are writing to follow up on [the civil society open letter that we sent you last month](#) about the upcoming 'Legislation to effectively tackle child sexual abuse'. **The letter has now been signed by a total of [45 organisations](#)** working for rights and freedoms across Europe and beyond, with support continuing to grow.

We urge you to pay attention to the concerns that we raise, and to use your executive powers to ensure that the Commission does not put forward a proposal that would undermine the CJEU prohibition of general monitoring or subject Europeans to monitoring that would turn their devices into spyware.

In particular, we would like to highlight that since we sent you our letter, the [leaked Opinion of the Regulatory Scrutiny Board \(RSB\)](#) revealed the shocking news that the upcoming proposal seeks to mandate generalised scanning, even in encrypted environments. The method that will be used for such detection is 'Client-Side Scanning' (CSS), a fundamentally flawed method which experts agree undermines encryption:

- In this paper, 14 of the world's leading cybersecurity experts explain how CSS leaves every person's devices vulnerable to hackers, criminals and other malicious actors: <https://arxiv.org/abs/2110.07450>
- In this article, two Princeton computer scientists explain that CSAM scanning in encrypted environments is fundamentally and unmitigably technically flawed: <https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/>

- In this article, security experts at EFF explain further risks of CSS:
<https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption>

Furthermore, the RSB Opinion revealed that 'unknown' content would also be in scope of these rules. **We remind you that AI tools are notoriously inaccurate at such tasks, and poor at interpreting context.** Such requirements would not only be very invasive, but would expose people to large numbers of erroneous reports. For example, [in a period of just 53 days in 2021, Meta found that their systems had wrongly flagged at least 207 people](#) of exchanging CSAM in the EU, with an additional 4,500 people lodging complaints.

Scaled up across time and multiple services/platforms, this volume of wrongful accusations could amount to a vast number of falsely-accused people. Because of the scale of private messaging in the EU, this is the case even if - as some providers of such technologies claim - their systems have a high theoretical accuracy. However, we have many reasons to doubt this claim of high accuracy. **In 2021, for example, [LinkedIn found that only 31 of the 75 files identified by PhotoDNA as CSAM were actually CSAM](#); meaning the rate of accuracy was only 41%.**

We believe that if the upcoming legislation mandates generalised scanning, the Legislation to effectively tackle child sexual abuse will not be fit for purpose, and will further be vulnerable to legal challenge. If the European Commission decides to propose a long-term derogation of the ePrivacy Directive, it needs to ensure that highest standards of necessity and proportionality. Furthermore, current "voluntary" practices by providers should be revised by data protection authorities (DPAs) under guidance of the European Data Protection Board (EDPB) and the European Data Protection Supervisor. If data protection authorities consider these current practices legal, they should be limited to scan for known images, with seriously enhanced mechanisms for transparency, accountability, oversight and human rights safeguards compared at least to the interim Regulation.

We are at your disposal to meet should you wish to further discuss what a fundamental rights-compliant approach to this important issue could look like.

Kind regards,



--



EUROPEAN DIGITAL RIGHTS

www.edri.org

On 16/3/22 19:18, [REDACTED] wrote:

17 March 2022

Dear **European Commission President Ursula von der Leyen**,

Dear **Executive Vice-President Margrethe Vestager**,

Dear **Vice-President Věra Jourová**,

Dear **Vice-President Dubravka Šuica**,

Dear **Commissioner Ylva Johansson**,

Dear **Commissioner Thierry Breton**,

Dear **Commissioner Margaritis Schinas**,

cc: Commission President Head of Cabinet Bjoern Seibert and Commission President Digital Adviser Anthony Whelan; Executive Vice-President Vestager Head of Cabinet Kim Jørgensen and Deputy Head of Cabinet Christiane Canenbley; Vice-President Jourová Head of Cabinet Renate Nikolay and Deputy Head of Cabinet Daniel Braun; Vice-President Šuica Head of Cabinet Colin Scicluna and Deputy Head of Cabinet Deša Srsen; Commissioner Johansson Head of Cabinet Åsa Webber and Deputy Head of Cabinet Tom Snels; Commissioner Breton Head of Cabinet Valère Moutarlier and Deputy Head of Cabinet Lucía Caldet; Commissioner Schinas Head of Cabinet Despina Spanou and Deputy Head of Cabinet Natasha Bertaud

Re: Protecting digital rights and freedoms in the Legislation to effectively tackle child abus

Tackling the online dissemination of child sexual abuse and exploitation material (CSAM) is an important part of the broader global fight to protect young people from sexual abuse and exploitation. In particular, this fight requires a

comprehensive approach by governments and companies to prevent such egregious crimes before they happen. In the context of **the upcoming EU legislation to effectively tackle child abuse**, we urge the Commission to ensure that people's private communications do not become collateral damage of the forthcoming legislation.

As the shocking events of the past three weeks have emphasised, **privacy and safety are mutually reinforcing rights**. People under attack depend on privacy-preserving technologies to communicate with journalists, to coordinate protection for their families, and to fight for their safety and rights. Equally in peacetime, people's ability to communicate without unjustified intrusion - whether online or offline - is vital for their rights and freedoms, as well as for the development of vibrant and secure communities, civil society and industry.

We strongly believe that we need to work together to find long-term solutions to the dissemination of CSAM online which are based in evidence and are respectful of all fundamental rights and the rule of law. We believe that resorting to quick 'silver bullet' technological 'solutions' are not only ineffective, but may result in unintended consequences for the privacy and confidentiality of every single person's communications, including those of children and survivors of abuse.

Experts agree that there is no way to give law enforcement exceptional access to communications that are encrypted end-to-end without creating vulnerabilities that criminals and repressive governments can exploit.¹ As the recent Pegasus scandals have shown, the unfettered tapping of people's devices poses huge risks to journalists, politicians, human rights defenders and the preservation of democratic society.

We, the undersigned 35 organisations, therefore call on the European Commission to ensure that the forthcoming legislation respects at a minimum a set of 10 cumulative human rights principles², of which we would like to highlight the following:

1. **No mass surveillance:** There must never be the generalised, automated scanning of everyone's private communications, as this is a practice that is inherently disproportionate under EU law. The Legislation to effectively tackle child sexual abuse must not compel service providers to take steps or to ensure outcomes that would in effect force them to conduct such practices;

2. **Interventions into people’s private communications must be targeted on the basis of individual-level suspicion:** Any intrusion into private communications must be made on the basis of specific, reasonable and individual-level suspicion as prescribed by the law and with judicial oversight in order to be justified;
3. **Measures must be the least privacy-invasive and be limited to detecting CSAM only:** In order to ensure this, the European Data Protection Board (EDPB) should provide guidance on appropriate technologies. Measures which break or undermine encryption (such as Client-Side Scanning); which are experimental or inaccurate; or which create cybersecurity risks will always create far more problems than they can solve.

Civil society organisations have helped to shape the General Data Protection Regulation (GDPR), the upcoming ePrivacy Regulation, and preventing illegal data retention rules. We believe, therefore, that closer collaboration on the forthcoming proposal would help ensure a legislation that is effective, necessary and proportionate for its purpose. This could also help **avoid litigation that could strike down parts of the future Regulation, if it were to compel service providers to intrude on people’s private communications without justifiable suspicion.**

As human rights advocates with expertise in technology, we reiterate the inherent limitations of any tech-based ‘solution’ to complex criminal problems like the dissemination of CSAM, which require a holistic approach. In achieving the goal of protecting children, including preventing the creation of CSAM in the first place, we suggest exploring social and human interventions at least as intensively as technology-based ones.

In a society which respects democracy and the rule of law, governments cannot take measures *at any cost*. **And in a world in which every aspect of our lives is increasingly digital, measures that jeopardise the privacy and confidentiality of communications will only become more dangerous.**

We hope our comments help you in the final steps in the preparation of the legislation. We are at your disposal to provide support and advice on this file.

Signed,

European Digital Rights (EDRi)

ApTI (Romania)

Big Brother Watch (UK)

Bits of Freedom (The Netherlands)

Centre for Democracy & Technology (CDT) (International)

Committee to Protect Journalists (CPJ) (International)

Data Rights (The Netherlands / European)

dataskydd.net (Sweden)

Defend Digital Me (UK)

Deutscher Anwaltverein (DAV) (Germany)

Deutsche Vereinigung für Datenschutz (DVD) (Germany)

Digitalcourage (Germany)

Digitale Gesellschaft (Germany)

Državljan D/Citizen D (Slovenia)

Electronic Frontier Foundation (EFF) (International)

Electronic Frontier Finland (Effi)

Entropia (Germany)

European Center for Not-for-Profit Law (ECNL)

European Sex Workers' Rights Alliance (ESWA)

Foundation for Information Policy Research (FIPR) (UK / European)

Global Voices (the Netherlands / International)

Homo Digitalis (Greece)

Internet Society Catalan Chapter (ISOC-CAT) (European)

ISOC Brazil - Brazil Chapter of the Internet Society (Brazil)

IT-Pol Denmark

LGBT Technology Partnership (International)

Ligue des droits humains (Belgique)

Mnemonic (Germany / International)

Open Governance Network for Europe

Open Rights Group (ORG) (UK)

Privacy and Access Council of Canada

Privacy International (PI)

Ranking Digital Rights (International)

Tech for Good Asia

Vrijdschrift.org (The Netherlands)

[1https://arxiv.org/abs/2110.07450](https://arxiv.org/abs/2110.07450)

[2https://edri.org/our-work/chat-control-10-principles-to-defend-children-in-the-digital-age/](https://edri.org/our-work/chat-control-10-principles-to-defend-children-in-the-digital-age/)

--



European Digital Rights

<https://edri.org>

Bio&Picture:



Tel (mobile): [REDACTED]

Tel (office landline): [REDACTED]

PGP: [REDACTED]

Twitter: [REDACTED]

--

[REDACTED]

EUROPEAN DIGITAL RIGHTS

www.edri.org [REDACTED] [PGP](#)



[Subscribe to the EDRi-gram.](#)