Mass surveillance and undermining encryption still on table in EU Council

Dear Justice and Home Affairs Ministers and Ministries of the EU Member States,
Dear Permanent Representatives (Ambassadors) to the EU,
Dear Representatives of the EU Member States in the Law Enforcement Working Party (LEWP),

17 April, 2024

As a coalition of 50 civil society organisations and 26 individual experts, we are writing to call on you not to agree to the EU Council position on the Child Sexual Abuse (CSA) Regulation whilst so many critical issues remain. The fundamental flaws of the Commission's draft law and previous Council texts - including of mass surveillance and serious threats to encryption - have not been resolved by the latest texts from the Belgian Presidency.

In the course of this EU legislative proposal, major concerns have been raised by thousands of experts across human rights law, cybersecurity, children's (digital) rights, child protection hotlines, police forces, data protection and more.

These concerns have been listened to by governments including of Germany, Poland, France, Austria, the Netherlands, Estonia and Finland, who have all reportedly taken a stand against various of the proposal's major legal and technical flaws. However, we warn that these critical issues are still very much present in the new approach.

In particular, the new proposal does not make significant or meaningful changes from a fundamental rights perspective. It can still force providers to undermine the end-to-end encryption of their services in order to comply with a detection order, and can still require them to surveil users with no link to the crime of online CSA.

This is a question of upholding the essence of rights to privacy, data protection, free expression and the presumption of innocence of people across the EU and beyond.

Despite some nominal changes to the risk categorisation framework, the new proposal still allows detection orders to be applied broadly and without targeting (in the meaning of a direct or indirect link, as interpreted by the Court of Justice of the EU (CJEU)[1]).

The concerns raised previously by the EU Council Legal Service, of incompatibility with human rights case law prohibiting general monitoring, firmly remain. Detection orders therefore continue to be vulnerable to being annulled at the CJEU.

1 See paragraph 111 of the Tele 2 judgment of the CJEU (joint cases C-203/15 and C-698/15).

This is a matter of not undermining one of the most important tools to protect digital communications that we have in the world, end-to-end encryption.

Whilst the new proposal makes some nods to the need to protect encryption, it only prevents providers from being forced to "alter" or "decrypt" encrypted communications. It keeps the use of Client-Side Scanning (CSS) techniques on the table, and doesn't stop providers from being forced to generally weaken or undermine the security or integrity of their service.

Earlier this year, the European Court of Human Rights (ECtHR) issued a landmark judgment, emphasising the importance of encryption in the protection of the right to privacy.[2] This important consideration is not reflected in the new Council approach – which would therefore likely also fall foul of the ECtHR in addition to the CJEU.

This is about ensuring that those whose safety relies on secure online communications are not unduly impacted, no matter how important the goal of the law.

From journalists, to youth activists, to people seeking sexuality or reproductive healthcare information: they must be considered, too. Yet the latest proposal and its supporting annex continue to mandate risky age verification tools and encourage other forms of widespread and invasive personal data disclosure. Together, these would render online anonymity close-to impossible, which can have serious consequences on people's digital freedoms and safety.

What's more, the new proposed risk categories will mean that the services which protect the privacy and security of their users will be considered high risk. Conversely, those whose business models rely on exploiting and monetising their users' data, and who do not offer secure communications channels, will by default be considered less risky. This runs contrary to the principles of privacy by design and by default as established in the General Data Protection Regulation (GDPR).

As recently emphasised by the European Data Protection Supervisor, the CSA Regulation risks the EU crossing the rubicon. With this latest attempt from the Presidency in order to unblock negotiations, the Council would be endorsing general monitoring and encryption-threatening measures that no doubt will be felt across the world.

We, the undersigned, call on you as representatives of your country to protect our rights and freedoms by rejecting this new Council General Approach.

Signed,

2 See *Podchasov v. Russia* (Application no. 33696/19) at the European Court of Human Rights (ECtHR).

Civil society organisations

Pan-European

- European Digital Rights (EDRi)
- The Centre for Democracy and Technology Europe
- European Network for the Promotion of the Rights and Health among Migrant Sex Workers (TAMPEP)
- Access Now
- Civil Liberties Union for Europe
- Defend Democracy
- Wikimedia Europe

Austria

- epicenter.works - for digital rights

Denmark

- IT-Pol Denmark

France

- La Quadrature du Net

Germany

- Digitale Gesellschaft
- Gesellschaft für Informatik e.V. (German Informatics Society)
- Deutsche Vereinigung für Datenschutz e.V. (DVD)
- SUPERRR Lab
- D64 – Zentrum für Digitalen Fortschritt (Center for Digital Progress)
- Digitalcourage

Greece

- Homo Digitalis

Italy

- Comitato per i Diritti Civili delle Prostitute APS

Netherlands

- Bits of Freedom
- Privacy First
- PIC

Portugal

- AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação
- ISOC Portugal
- ANSOL - Associação Nacional para o Software Livre
- D3 - Defesa dos Direitos Digitais

Slovenia

- Državljan D / Citizen D

Spain

- Xnet, Institute for Democratic Digitalisation (Spain)

Sweden

- Red Umbrella Sweden

International/global

- Electronic Frontier Foundation (EFF)
- Fundación Cibervoluntarios
- Internet Society
- The Tor Project
- Aspiration
- ARTICLE 19
- Committee to Protect Journalists (CPJ)

International – countries and regions

- Internet Society Catalan Chapter (ISOC-CAT)
- CIPESA (Africa)
- Bangladesh NGOs Network for Radio and Communication(BNNRC)!
- Tech for Good Asia
- Internet Society - Brazil Chapter
- Electronic Frontier Norway
- Fight for the Future (United States)
- Privacy & Access Council of Canada
- JCA-NET(Japan)
- Big Brother Watch (United Kingdom)
- Electronic Frontiers Australia
- Defend Digital Me (United Kingdom)

- STAR - The First Sex Workers Collective in the Balkans (North Macedonia)
- European Sex Workers' Rights Alliance (ESWA) (Europe and Central Asia)
- The Law and Technology Research Institute of Recife (IP.rec) (Brazil)

Expert individuals (academics, researchers, technologists, lawyers etc.)

- Bart Preneel, Professor KU Leuven-COSIC
- Simona Levi, digital rights activist and theatre director, University of Barcelona
- PhD. Jordi Domingo-Pascual, Professor at Universitat Politènica de Catalunya (UPC BarcelonaTECH)
- Brian Byaruhanga, Engineer and Technologist
- Dr. Zdravko Bozakov, Professor at University of Applied Sciences Worms
- Sharon Polsky MAPP, President, Privacy & Access Council of Canada
- Mr Michele Neylon, Technologist
- Runa Sandvik, Founder of Granitt
- Alec Muffett, Security Technologist & Consultant
- Robin Wilton, Technologist & Director, Internet Trust at Internet Society
- Jeremy Harmer LL.M. Ph.D., Independent privacy researcher
- José Legatheaux Martins, Retired professor of Informatics at NOVA School of Science and Technology, Lisbon
- Leo Florea Ph.D., Encryption researcher and cybersecurity expert
- Jorge Pinto, Security Professional
- Riana Pfefferkorn, Research Scholar, Stanford
- Prof. Carmela Troncoso, EPFL
- Jorge Alberto Kobeh Jirash, Technologist
- Charles Mok, Stanford University
- Arne Möhle, Founder of Tuta Mail (Tutanota)
- Matthias Pfau, Founder of Tuta Mail (Tutanota)
- Athena Michalakea, PhD Birkbeck, University of London, Lawyer, Athens Bar Association
- Prof. Dr. Gloria González Fuster, Research Professor at Vrije Universiteit Brussel (VUB)
- Ot van Daalen, Institute for Information Law, University of Amsterdam
- SW Digitaal, Digital Rights Advisor for sexworkers in the Netherlands
- Marjan Wijers, PhD researcher human rights and sex worker rights
- Yigit Aydinalp, University of Sheffield