Monday 23 February 2026

Civil society open letter to Members of the European Parliament

We say no to Big Tech mass snooping on our messages!

The European Parliament is currently deciding its position on the proposed second extension of the 'temporary' **interim ePrivacy derogation** 2025/0429(COD), with trilogues expected to start in early Spring 2026. **It is vital that the Parliament acts now to rule out mass snooping on our private messages.**

This controversial law was already criticised strongly by many in the Parliament when it was first extended by the Commission, leading to a Parliament position which stated that after the first extension, the derogation "shall elapse permanently". The derogation is sometimes referred to as "Chat Control 1.0" because it suspends the fundamental right to privacy enshrined in EU primary and secondary law. **This right is supposed to keep us all safe from arbitrary or untargeted snooping in our digital and physical private lives**.

The proposed extension of this law would **allow Big Tech companies to continue to scan billions of private messages (chats), emails and social media posts** of people across the EU, and report them to a US center in case they suspect abuse material is being shared. The US center then forwards material on to US and EU law enforcement agencies.

As emphasised by the European Data Protection Supervisor, the law lacks a proper legal basis - with governments like Germany telling local companies that as a result, it would be illegal for them to do such scanning (p.11). It also contains very few safeguards despite putting a serious limitation on the right to privacy of millions of people. Of the safeguards that exist, they are not followed: EU Member States and the Commission have been late and incomplete in reporting data.
The latest Commission implementation report shows a concerning lack of proportionality - with **only 0.000002735% of scanned content in the data provided actually constituting illegal material**, and even less than this coming from the EU.[1] It equally shows **very high levels of errors**, with even supposedly leading-edge scanning tech getting it wrong between 13 and 20% of the time (p.8). With such a huge amount of content being scanned, **this is an huge and unacceptable margin of error**.

While the issue of tackling the spread of child sexual abuse material is of vital importance, its pursuit must still respect privacy, free expression, and the presumption of innocence. Law enforcement agencies should use their full democratically-agreed powers to pursue and convict

1 According to page 4 of the 2025 implementation report (COM(2025) 740 final), the scanning done by Microsoft in 2023 found 32,000 global items of CSAM out of 11.7 billion scanned, for example. Therefore only 0.000002735% globally was CSAM, and even less was CSAM from the EU - just 0.00000077%.

perpetrators of this horrific crime.

Innocent people, however, must not have their private communications scanned and reported to a US government-affiliated agency. This can lead to grave consequences for wrongly-accused people, can have a chilling effect on free speech, creates huge possibilities for abuse (such as the use of scanned information for advert targeting) and can violate professional confidentiality for lawyers, doctors and therapists.

This is the position that the European Parliament took in its 2023 report by MEP Javier Zarzalejos on the Regulation laying down rules to prevent and combat child sexual abuse, which unlike the interim derogation, has the potential to create a genuinely proportionate and legally-sound long-term approach to the scourge of CSAM online.

We urge Members of the European Parliament to reject any extension of the interim ePrivacy derogation unless it explicitly rules out mass surveillance (meaning no indiscriminate or untargeted scanning); requires a high standard of accuracy (meaning no scanning for 'new' or 'unknown' material); and is clearly time-bound to a maximum of 1 year.

Signed,

Civil society organisations:

- 101.CY
- Alternatif Bilişim (Alternative Informatics Association)
- ANSOL - Associação Nacional para o Software Livre
- Asociația pentru Tehnologie și Internet (ApTI)
- Bits of Freedom
- Bundesrechtsanwaltskammer
- Centre for Democracy & Technology Europe (CDT Europe)
- Chaos Computer Club
- D3 - Defesa dos Direitos Digitais
- D64 – Center for Digital Progress
- Danes je nov dan, Inštitut za druga vprašanja
- Dataföreningen Västra (Swedish Computer Association West)
- Datenpunks Bremen
- Datenpunks e. V.
- Defend Democracy
- Digital Rights Ireland
- Digitalcourage
- Digitale Gesellschaft (CH)
- Digitale Gesellschaft (Germany)
- Electronic Frontier Norway
- epicenter.works
- ESWA (European Sex Workers Rights Alliance)
- European Digital Rights (EDRi)
- Giordano-Bruno-Stiftung
- INSPIRIT Creatives UG NGO
- Internet Society Catalan Chapter (ISOC-CAT)
- Irish Council for Civil Liberties
- IT-Pol Denmark
- IuRe (Iuridicum Remedium)
- Kleindatenverein
- Osservatorio Nessuno OdV
- Politiscope
- Privacy First
- SekswerkExpertise, platform for the enhancement of sex worker rights
- Selbstbestimmung Selbstgemacht e.V.
- Statewatch
- Stichting Data Bescherming Nederland (SDBN)
- Whistleblower-Netzwerk e.V.
- Xnet, Institute for Democratic Digitalisation

- Bangladesh NGOs Network for Radio and Communication(BNNRC)

Individuals:

- Anne Roth, Senior Policy Advisor on digital policy, 'Die Linke', German Bundestag
- Prof. Carmela Troncoso, MPI-SP & EPFL
- Prof. Bart Preneel
- Matthias Pfau, Cryptography Expert
- Arne Möhle, Cryptography Expert at Tuta
- Runa Sandvik, Digital Security Expert
- Assoc. Prof. Asli Telli, Research Associate at University of Cologne
- Prof. Diego F. Aranha, Aarhus University
- Professor Kimmo Halunen
- Peter Schwabe, MPI-SP & Radboud University
- Dr. Eyal Ronen, School of Computer Science, Tel Aviv University
- Dr. Patrick Breyer