on 26. March 2026 0

End of “Chat Control”: EU Parliament Stops Mass Surveillance in Voting Thriller – Paving the Way for Genuine Child Protection!

EUROPEAN PARLIAMENT FREEDOM, DEMOCRACY AND TRANSPARENCY

The controversial mass surveillance of private messages in Europe is coming to an end. After the European Parliament had already rejected the indiscriminate and blanket Chat Control by US tech companies on 13 March, conservative forces attempted a democratically highly questionable maneuver yesterday to force a repeat vote to extend the law anyway.

However, in a true voting thriller today, the Parliament finally pulled the plug on this surveillance mania: With a razor-thin majority of just a single vote, the Parliament first rejected the automated assessment of unknown private photos and chat texts as “suspicious” or “unsuspicious”. In the subsequent final vote, the amended remaining proposal clearly failed to reach a majority.

This means: As of 4 April, the EU derogation will expire for good. US corporations like Meta, Google, and Microsoft must stop the indiscriminate scanning of the private chats of European citizens. The digital privacy of correspondence is restored!

The Myth of a Legal Vacuum

This does not create a legal vacuum—quite the opposite. Ending indiscriminate mass scanning clears the path for modern, effective child protection. Fearmongering that investigators will be “flying blind” is unwarranted: Recently, only 36% of suspicious activity reports from US companies originated from the surveillance of private messages anyway. Social media and cloud storage services are becoming increasingly relevant for investigations. Targeted telecommunications surveillance based on concrete suspicion and a judicial warrant remains fully permissible, as does the routine scanning of public posts and hosted files. User reporting also remains fully intact.

Digital freedom fighter and former Member of the European Parliament Patrick Breyer (Pirate Party) commented on today’s historic victory:

> *“This historic day brings tears of joy! The EU Parliament has buried Chat Control – a massive, hard-fought victory for the unprecedented resistance of civil society and citizens! The fact that a single vote tipped the scales against the extremely error-prone text and image search shows: Every single vote in Parliament and every call from concerned citizens counted!*
>
> *We have stopped a broken and illegal system. Once our investigators are no longer drowning in a flood of false and long-known suspicion reports from the US, resources will finally be freed up to hunt down organized abuse rings in a targeted and covert manner. Trying to protect children with mass surveillance is like desperately trying to mop up the floor while leaving the faucet running. We must finally turn off the tap! This means genuine child protection through a paradigm shift: Providers must technically prevent cybergrooming from the outset through secure app design. Illegal material on the internet must be proactively tracked down and deleted directly at the source. That is what truly protects children.*
>
> *But beware, we can only celebrate briefly today: They will try again. The negotiations for a permanent Chat Control regulation are continuing under high pressure, and soon the planned age verification for messengers threatens to end anonymous communication on the internet. The fight for digital freedom must go on!”*

The Next Battle: The Return of Chat Control and Mandatory ID

Despite today’s victory, further procedural steps by EU governments cannot be completely ruled out. Most of all, the trilogue negotiations on a permanent child protection regulation (Chat Control 2.0) are continuing under severe time pressure. There, too, EU governments continue to insist on their demand for “voluntary” indiscriminate Chat Control.

Furthermore, the next massive threat to digital civil liberties is already on the agenda: Next up in the ongoing trilogue, lawmakers will negotiate whether messenger and chat services, as well as app stores, will be legally obliged to implement age verification. This would require users to provide ID documents or submit to facial scans, effectively making anonymous communication impossible and severely endangering vulnerable groups such as whistleblowers and persecuted individuals.

Background: What exactly expires on 3 April

An EU interim regulation (2021/1232), set to expire on 3 April, currently permits US corporations such as Meta to carry out indiscriminate mass scanning of private messages on a voluntary basis. Three types of chat control are authorised: scanning for already known images and videos (so-called hash scanning, which generates over 90% of reports); automated assessment of previously unknown images and videos; and automated analysis of text content in private chats.

The AI-based analysis of unknown images and texts is extremely error-prone. But the indiscriminate mass scanning for known material is also highly controversial, too: beyond the unreliability of the algorithms documented by researchers, these scans rely on opaque foreign databases rather than European criminal law. The algorithms are blind to context and lack of criminal intent (e.g. consensual sexting between teenagers). As a result, vast numbers of private but criminally irrelevant chats are exposed.

New Study Proves: Chat Control Software is Flawed

The fact that today’s decision by the EU Parliament was also technically imperative is proven by a newly published scientific study. Renowned IT security researchers analyzed the standard algorithm “PhotoDNA”, which is used by tech companies for Chat Control. Their damning verdict: The software is “unreliable”. The researchers proved that criminals can render illegal images invisible to the scanner through minimal alterations (e.g., adding a simple border), while harmless images can be easily manipulated so that innocent citizens are falsely reported to the police.

The Hard Facts: Why Chat Control Has Failed Spectacularly

The EU Commission’s 2025 evaluation report on Chat Control reads like an admission of complete failure:

- **Data Giant Monopoly:** Roughly 99% of all chat reports to police in Europe come from a single US tech corporation: Meta. US companies acted as a private auxiliary police force—without effective European oversight.
- **Massive Police Overload from Junk Data:** The German Federal Criminal Police Office (BKA) reports that a staggering **48% of the disclosed chats are criminally irrelevant**. This flood of junk data ties up resources that are urgently needed for targeted investigations.
- **Criminalization of Minors:** According to crime statistics, around 40% of investigations in Germany target teenagers who thoughtlessly share images (e.g., consensual sexting).
- **An Obsolete Model Due to Encryption:** Because providers are increasingly transitioning to end-to-end encryption for private messages, the number of chats reported to the police has already dropped **by 50%** since 2022.
- **Failure in Child Protection:** According to the Commission’s report, there is no measurable correlation between the mass surveillance of private messages and actual convictions.

The Great Fact Check: Disinformation Narratives of Proponents

During the legislative process, foreign-funded lobby groups and authorities tried to pressure the Parliament through fearmongering. A comparison of their claims with reality:

Disinformation 1: “The European Parliament is to blame for the collapse of the trilogue negotiations.”
(Claimed by the lobby alliance ECLAG and US tech companies)

- **Fact:** It was the EU Council of Ministers that deliberately let the negotiations fail. Leaked Council

- cables reveal that EU member states showed no willingness to compromise, fearing that any concession could set a precedent for the permanent Chat Control 2.0 regulation. Parliament's lead negotiator, Birgit Sippel, sharply criticized the Council: *"With their lack of flexibility, Member States have deliberately accepted that the interim regulation will expire."*

Disinformation 2: "Without indiscriminate Chat Control, law enforcement will be flying blind."
(Claimed by authorities including BKA President Holger Münch)

- **Fact:** Targeted surveillance remains allowed. The real problem for authorities is their own refusal to remove material from the internet. The Federation of German Criminal Investigators (BDK) warns that this mass surveillance produces *"a flood of tips… often without any actual investigative lead."* Meanwhile, the BKA systematically refuses to proactively have abuse material removed from the internet, as investigative reporting by ARD has revealed.

Disinformation 3: "The deployed scanning technology is highly precise."
(Claimed by Meta, Google, Microsoft, Snap, TikTok)

- **Fact:** According to an open letter by renowned IT researchers, *"false positives seem unavoidable."* According to an alliance of more than 40 civil liberties organizations (including the Chaos Computer Club), the EU Commission itself documented error rates of the algorithms between 13 and 20 percent. Of billions of scanned messages, only 0.0000027 percent were actually illegal material. Furthermore, the German Data Protection Conference (DSK) warns: *"Indiscriminate surveillance affects the core of the confidentiality of communication."*

Disinformation 4: "The demand comes primarily from victims."
(Implied by the ECLAG campaign)

- **Fact:** Actual survivors are taking legal action against the surveillance. Survivor Alexander Hanff writes: *"Taking away our right to privacy means further harming us."* To preserve safe spaces for victims, a survivor from Bavaria is currently suing Meta. Who truly benefits was exposed in an investigative report by Balkan Insight: The US organization *Thorn*, which sells scanning software, invests massively in EU lobbying, while ECLAG members are funded by tech corporations.

The Way Forward: "Security by Design" Instead of Surveillance Mania

The European Parliament advocates a genuine paradigm shift for future legislation, supported by civil society, survivor networks, and IT security experts:

1. **Strict default settings and protective mechanisms (Security by Design)** to make cybergrooming technically harder from the outset.
2. **Targeted telecommunications surveillance** based on judicially confirmed suspicion.
3. **Proactive search by a new EU Child Protection Center and immediate takedown obligations** for providers and law enforcement on the open internet and darknet – illegal material must be destroyed directly at the source. There must be an end to law enforcement agencies declaring themselves "not competent" for the removal of abuse material.

Bought Fearmongering by the Lobbying Machine

During the legislative process, the massive, questionable lobbying efforts were exposed: The push for Chat Control is heavily driven by foreign-funded lobby groups and tech vendors. The US organization *Thorn*, which sells the exact type of scanning software in question, spends hundreds of thousands of euros lobbying in Brussels. The tech industry officially lobbied side-by-side with certain organizations for a law that does not protect children, but rather secures their own profits and data access.

Patrick Breyer concludes:

> *"Right up to the very end, the US tech industry and foreign- or government-funded lobby groups tried to panic Europe. But flooding our police with false positives and duplicates from mass surveillance doesn't save a single child from abuse. Today's definitive failure of Chat Control is a clear stop sign to this surveillance mania. Negotiators cannot ignore this verdict in the ongoing trilogue negotiations for a permanent regulation. Indiscriminate mass scanning of our private messages must finally give way to truly effective and targeted child protection that respects fundamental rights."*

TAGS: Chatcontrol

back to archive

←

Related topics

26. March 2026

End of "Chat Control": EU Parliament Stops Mass Surveillance in Voting Thriller – Paving the Way for Genuine Child Protection!

EUROPEAN PARLIAMENT

FREEDOM, DEMOCRACY AND TRANSPARENCY

💬 0

24. March 2026

The Battle Over Chat Control: How EU Governments and the Tech Lobby Are Trying to Overturn Parliament's Vote — A Comprehensive Fact Check

FREIHEIT, DEMOKRATIE UND TRANSPARENZ

💬 0

17. March 2026

End of "Chat Control": Paving the Way for Genuine Child Protection!

EUROPEAN PARLIAMENT

FREEDOM, DEMOCRACY AND TRANSPARENCY

💬 0

1 2 … 38 Next page

Interesting too

Kategorien:

ARTIFICIAL INTELLIGENCE

COMMUNICATIONS SCREENING

EUROPAPARLAMENT

EUROPEAN PARLIAMENT

FREEDOM, DEMOCRACY AND TRANSPARENCY

FREIHEIT, DEMOKRATIE UND TRANSPARENZ

JOB OFFERS MEDIA REPORTS

NICHT KATEGORISIERT OTHER

PRESS BRIEFINGS PRESS RELEASES

PRESSEMITTEILUNGEN

PRESSEMITTEILUNGEN (SH)

SONSTIGES

Keep in touch with me!

@patrickbreyer_mep

PIRATE PARTY

- About us
- Pirate Party Germany
- European Pirate Party
- Pirate Party International
- Communal Pirates

All content on this site – unless indicated otherwise – is free to use under a Creative Commons license.

Contact / Privacy Notice