POSITION PAPER

Rejecting suspicionless scanning: the ePrivacy derogation and the defence of encryption in Europe

ALT-TEXT's position on the revival of "Chat Control 1.0" and the path to a rights-compliant Child Sexual Abuse Regulation

In brief

- On 9 July 2026 the European Parliament brought back "Chat Control 1.0", a law that lets messaging and email providers scan private communications for child sexual abuse material (CSAM).
- It returned even though more Members voted against it than for it. The procedure meant that stopping the law needed an absolute majority of the whole Parliament, 361 votes, not just a majority of those present. The opposition reached 314 and fell 47 short, so the law returned by default.
- This is the narrower, temporary law: it permits scanning but does not force it, and it does not properly reach end-to-end encrypted (E2EE) services such as Signal or WhatsApp.
- The far more dangerous law, the permanent regulation that would force detection and could break encryption through "client-side scanning", will continue being negotiated when the Parliament returns in September 2026.
- ALT-TEXT's position: mass scanning is the wrong tool. It is unreliable, treats the whole population as suspects, weakens the security everyone depends on, and was revived through a procedural manoeuvre that sidestepped scrutiny.
- We call for encryption to be protected in law, for investigations to be targeted and judicially authorised, and for public money to fund European, open-source, privacy-respecting communication tools. The real fight is in September.

Executive summary

On 9 July 2026 the European Parliament allowed the temporary ePrivacy derogation, often known as Chat Control 1.0, to be revived until April 2028. The vote count and the procedural mechanics are set out in section 3; what matters at the outset is that a measure a majority of participating legislators rejected became law by procedural default.[1][2]

ALT-TEXT's position is clear. We oppose the suspicionless, generalised scanning of private communications as incompatible with Articles 7 and 8 of the Charter of Fundamental Rights, and we oppose the political manoeuvre by which this text was revived. The derogation is a threat to privacy; the process is a threat to democratic processes. Our central demands are the protection of E2EE in law, a shift to targeted and judicially authorised investigation, and dedicated public funding for the open-source, interoperable communications infrastructure on which the European priority of digital sovereignty depends.

---

[1] European Parliament, press release, "Combating child sexual abuse online: support for a more limited ePrivacy derogation", 9 July 2026. https://www.europarl.europa.eu/news/en/press-room/20260706IPR46318/combating-child-sexual-abuse-support-for-a-more-limited-eprivacy-derogation

[2] HowTheyVote.eu, roll-call record for the vote of 9 July 2026 (607 Members voting, 112 not voting). https://howtheyvote.eu/votes/195775

1. The core tension

The protection of children from abuse is urgent. No one would contest that. However, there is a false tension between child protection on the one hand and privacy on the other. The theory of those behind Chat Control is that scanning the private messages of the entire EU population will surface enough offending material to justify the intrusion. On the other hand, we have those who believe that CSAM is best addressed through targeted investigations, judicial oversight and well-resourced law enforcement. This argument maintains that mass scanning corrodes the security infrastructure that protects victims and vulnerable people and the channels for reporting violations.

Thus far, the evidence does not corroborate the first theory. A complementary impact assessment prepared for the European Parliament's LIBE committee concluded that detecting known material with established hash-matching technology can be done with relatively high accuracy, whereas deploying currently available technologies to detect previously unknown material on a large scale would result in high error rates and false positives.[3] According to German Federal Criminal Police Office reports, 48% of incoming alerts are not criminally relevant.[4] So while reporting looks voluminous, this is not equivalent to impact and investigators experience bottlenecks whilst moderating and sorting irrelevant content. As the former MEP and digital-rights campaigner Patrick Breyer put it after the vote, trying to protect children with suspicionless mass surveillance is like mopping the floor while the tap is still running.[5]

The gap between the official accuracy claims and reality is well documented. Data obtained by the Irish Council for Civil Liberties on the referrals An Garda Síochána received from the US National Center for Missing and Exploited Children in 2020 shows the pattern: of 4,192 referrals, at least 471 (more than one in ten) were verified as not depicting abuse material at all, examples given by the force included children playing on a beach, topless content and nudist content, while fewer than one in ten referrals (409) were ultimately deemed actionable.[6] Set against the European Commission's claim that detection is 99.9 per cent accurate, with false positives at only one in fifty billion, these figures do not hold up. Worse still, the authority retained the email addresses, screen names and IP addresses of people it had already cleared, and its own data protection unit conceded there may be no legal basis to hold on to that data.[7] This is the surveillance machine that the derogation permits, generating false suspicion against ordinary people and then keeping files on them after they have been cleared.

2. ALT-TEXT's position

Suspicionless scanning of citizens' private communications represents a dangerous precedent. Although the derogation permits email and chat providers to voluntarily detect, report and remove

---

[3] European Parliament, European Parliamentary Research Service (EPRS), 'Proposal for a regulation laying down the rules to prevent and combat child sexual abuse: complementary impact assessment', PE 740.248, April 2023, prepared for the LIBE committee. https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf

[4] Patrick Breyer, "EU Parliament greenlights Chat Control 1.0 – Breyer: 'Our children lose out'", 9 July 2026. https://www.patrick-breyer.de/en/eu-parliament-greenlights-chat-control-1-0-breyer-our-children-lose-out/

[5] Breyer, ibid.

[6] Irish Council for Civil Liberties, "An Garda Síochána unlawfully retains files on innocent people…" Source of the 2020 NCMEC-referral figures and the retention of data on cleared individuals. https://www.iccl.ie/news/an-garda-siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing-of-child-sex-abuse-material/

[7] ICCL, ibid.

CSAM material on non-encrypted applications, we see this as an unnecessary invasion of privacy, and a slippery slope step towards breaking encryption.

The security of our private communications is a structural precondition for our freedom and is not to be traded in with every successive crisis. Encryption allows journalists to protect sources, lawyers to advise clients, survivors to contact helplines, and citizens to organise and express dissent without the threat of surveillance. Normalising the scanning of private messages – even on a voluntary basis – creates a dangerous blueprint for authoritarian regimes to exploit outside the framework of European democratic checks and balances.

ALT-TEXT rejects the framing that puts safety at odds with freedom. This dichotomy is fundamentally false: a communications infrastructure with a built-in inspection point is inherently less safe for everyone. Building a mechanism to scan messages is the digital equivalent of forcing citizens to leave a copy of their house keys in a central database. If that vulnerability exists, it will eventually be found and exploited. Introducing a systemic weakness to target specific criminals inadvertently compromises the entire network, leaving every user exposed to exploitation by criminal networks and hostile states.

3. What was decided, and what was not

The July 9 vote is a temporary provision in lieu of a resolution on the permanent Child Sexual Abuse Regulation (CSAR) which would introduce mandatory detection orders and scope for client-side scanning of encrypted services. The CSAR remains in trilogue and will return to the table in September.

The platforms in scope of the temporary ePrivacy derogation include services like Gmail, Instagram direct messages, Discord, Snapchat, Skype, Xbox messaging and iCloud Mail. These services are not E2EE, being either unencrypted or server-side encrypted. Genuine E2EE services such as Signal, Whatsapp and iMessage are outside the derogation's practical reach and the Parliament adopted an amendment explicitly excluding E2EE services.[8]

This is welcome in principle, but its practical effect is limited, since such traffic cannot be inspected in transit in any case, and its legal survival is uncertain: the amendment now returns to the Council, which has until approximately 9 October 2026 to accept or reject it and may well reject it as inconsistent with the logic of the file.

Timeline of the file

Date	Event
August 2021	The ePrivacy derogation, Regulation (EU) 2021/1232, enters into force as a temporary measure permitting providers to voluntarily scan private communications for CSAM.
2022 onwards	The Commission proposes a permanent Child Sexual Abuse Regulation (CSAR), the file civil society names "Chat Control 2.0", introducing mandatory detection orders. Five trilogue rounds fail to reach agreement.
26 March 2026	Parliament rejects extending the temporary derogation: 311 against, 228 in favour, 92 abstentions. The interim law lapses on 3 April 2026.
Late June 2026	Parliament President Roberta Metsola reopens the file. Member states reinstate the

[8]European Parliament press release, 9 July 2026, op. cit.

	Council's second-reading position with the Commission's original, unrestricted text.
7 July 2026	The EPP invokes the Rule 170 urgent procedure to fast-track the file to the plenary, bypassing committee scrutiny. The urgency motion passes 331 to 304, with 11 abstentions.
9 July 2026	At second reading, 314 MEPs vote to reject, 276 against rejection, 17 abstentions. Rejection required an absolute majority of 361. The motion falls 47 votes short and the derogation is revived until April 2028.
By ~9 October 2026	The Council must accept or reject Parliament's end-to-end encryption exemption amendment. If it rejects it, then the file moves to conciliation.
September 2026	Trilogue negotiations on the permanent CSAR ("Chat Control 2.0") will resume under the Irish Council Presidency.

4. The procedural objection

After the EP rejected the derogation in March, the file was reissued with much the same content and pushed through via the Rule 170 urgent procedure on the last sitting day before the summer recess, after many MEPs had already left Brussels. The parameters of the urgent procedure meant that opponents of Chat Control would need an absolute majority of the entire chamber (361 votes) to stop it from passing, meaning that every absence and abstention was counted, in effect, as support.

A procedure designed for genuine emergencies was used to escape scrutiny, including the opinion of the European Data Protection Supervisor (EDPS) and a fundamental-rights impact assessment. When a chamber can be made to vote on the same question repeatedly, under progressively less favourable rules, until it yields the desired answer, the democratic value of the vote is hollowed out.

We believe this to be a governance failure where procedural "simplification" and urgency become instruments for weakening safeguards rather than improving lawmaking.

5. Why client-side scanning is not a compromise

The permanent regulation's proponents present client-side scanning as a way to preserve encryption while still detecting material. Scanning content on the device before it is encrypted does not preserve confidentiality; it relocates the point of scanning to the user's phone. The Global Encryption Coalition is explicit that client-side scanning is not an alternative to creating a backdoor - it is a backdoor.

Furthermore, there are consequences for the EU market. Providers of genuine E2EE have stated they will withdraw from the EU rather than ship what would, in effect, be state-mandated malware on their users' devices. Signal's representatives have argued that privacy can scale without surveillance capitalism, and that a mandate to scan would force them to exit.[9] The result would be a European market poorer in trustworthy tools, pushing security-conscious users towards subpar alternatives and undermining the Union's own objectives under NIS2, eIDAS 2.0 and the European Digital Identity Wallet, which all depend on communications the public can trust.

---

[9] Signal, "For a future with privacy, not mass surveillance, Germany must stand firmly against client-side scanning in the Chat Control proposal", October 3 2025. lhttps://signal.org/blog/pdfs/germany-chat-control.pdf

6. The structural remedy: sovereignty, open source and public funding

The deeper problem is that Europe's private-communications layer rests largely on a handful of non-European platforms operating, until this vote, in a legal grey zone. The scanning debate is therefore also a digital sovereignty debate. Detection-technology vendors and large US-based platforms all share a preference for a stable legal framework for scanning; the "regulatory gap" framing that drove the urgency serves that constituency as much as it serves child protection. A rights-respecting response does not simply block bad law; it builds the public-interest alternative.

ALT-TEXT calls for dedicated funding within the next Multi-Annual Financial Framework for open-source, local-first and interoperable communications infrastructure. Ring-fenced funding would help preserve an Internet built for everyone. Open standards and interoperability are a structural remedy for platform monopolies: they let Europeans move to trustworthy tools without losing their networks, and they distribute security expertise rather than concentrating it. Under the European Technological Sovereignty Package, the Cloud and AI Development Act's criteria for trusted providers and the EU Open Source Strategy should be read together as the constructive counterpart to the defensive fight over encryption.[10] The Cyber Resilience Act's security-by-design logic is fundamentally incompatible with a legal mandate to adopt encryption-breaking backdoors, and that contradiction should be recognised in every consultation.

Suspicionless scanning also contradicts the EU's own law. The Digital Services Act, adopted in 2022, reaffirms in Article 8 the prohibition on general monitoring obligations: providers may not be compelled to actively search all the content their users share.[11] This is not an incidental rule but a core protection against censorship, and it aligns with consistent case law of the Court of Justice, which has held that generalised access to the content of communications compromises the essence of the right to privacy under Article 7 and right to personal data protection under Article 8 of the Charter.[12] Generalised scanning, whether imposed by a detection order or pressed on providers through open-ended risk-assessment duties, runs directly against that prohibition. The Union cannot coherently forbid general monitoring in one instrument and push for it in another. Treating legislation in isolation makes for an incoherent set of rules which can be undermined and lead to an erosion of safeguards.

7. Who is harmed: marginalised communities and the chilling of expression

The costs borne by weakening privacy and security are rarely experienced evenly. Age-verification and mandatory digital-identity requirements, presented as safeguards, would make an identity document a precondition for ordinary communication. That would exclude the people least able to absorb it: undocumented people, including undocumented children who have fled persecution; Roma and Sinti communities; homeless people; and anyone without the requisite papers. A measure justified as protecting children would in practice lock some off the most vulnerable children out of

[10] European Commission, "Strengthening Europe's tech sovereignty", 3 June 2026. https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_en

[11] European Parliament, Answer given by Executive Vice-President Virkkunen on behalf of the European Commission, 21 January 2025
https://www.europarl.europa.eu/doceo/document/E-10-2024-002041-ASW_EN.html

[12] Official Journal of the European Union, Charter of Fundamental Rights of the European Union, 26 October 2012 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT

the services they rely on to reach family, support workers or legal advice. Proof of age built on biometric processing compounds the harm by normalising the systematic handling of children's most sensitive data.[13]

This regime also criminalises everyday use. Teenagers above the age of consent who lawfully exchange intimate images can have those messages flagged, reviewed by moderators and routed to police, a process that is itself intrusive and distressing and often falls hardest on LGBTQ+ young people exploring their identity. Beyond this, when people know they might be watched, they change the way they speak, leading to self-censorship and the chilling of free expression. This chilling effect is felt acutely by those who hold power to account: journalists protecting confidential sources, whistleblowers, human-rights defenders and activists. This directly concerns Article 4 of the European Media Freedom Act[14], since confidential source protection is a precondition of a free press that would be undermined if such communications are subject to surveillance.

8. The citizenship dimension

The public was told a measure had "passed" when a majority of voting representatives had in fact opposed it; the decisive facts were procedural thresholds and scheduling, not a change of political mind. Citizens equipped to read algorithmic and institutional power can see the difference between a substantive democratic decision and an outcome engineered by the rules under which a vote is held. ALT-TEXT frames AI and digital literacy not as an engineering skill but as a civic capability: the ability to recognise when surveillance is being sold as "protection", to interrogate claims of technical necessity, and to demand transparency about who benefits from a given framing. Surveillance and control are frequently presented as safety while reproducing the power structures that silence marginalised communities. It falls to citizens to reject that colonisation of digital space and to insist on infrastructure that empowers expression rather than watching over it.

9. Recommendations

ALT-TEXT urges European policymakers, the LIBE committee, and civil-society coalitions to pursue the following concrete mechanisms.

- Protect encryption in primary law. The end-to-end encryption exemption adopted on 9 July must be retained by the Council and written durably into any permanent regulation, with no carve-out permitting client-side scanning, which is functionally a backdoor.
- Replace suspicionless detection with targeted, judicially authorised investigation. Scanning should be confined to accounts identified by a competent judicial authority on the basis of reasonable suspicion, consistent with the Council Legal Service's own warning that generalised scanning is incompatible with Article 7 of the Charter absent prior authorisation, and with the general-monitoring prohibition in Article 8 of the Digital Services Act.[15]

---

[13] European Digital Rights (EDRi) and partners, "A safe internet for all: upholding private and secure communications", network position paper on the CSA Regulation. https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

[14] Article 4 of the European Media Freedom Act, https://www.media-freedom-act.com/Media_Freedom_Act_Article_4_(Regulation_EU_2024_1083_of_11_April_2024).html

[15] Council of the European Union, Legal Service opinion 8787/23, 26 April 2023 (LIMITE; published via Statewatch). Concerns the permanent 2022 CSA Regulation, not the 2026 derogation; warns that detection orders in interpersonal communications risk compromising the essence of Articles 7 and 8 of the Charter, and that any scanning should be confined to persons in respect of whom there are reasonable grounds for suspicion. https://statewatch.org/wp-content/uploads/2026/04/eu-council-cls-opinion-csam-proposal-8787-23.pdf

- Provide resources for what actually protects children. Redirect funding to law-enforcement triage capacity, victim support, takedown of hosted material, and prevention, rather than to volume-generating scanning that overwhelms investigators with non-actionable alerts.
- Reject mandatory age verification and identity gating. No provision should make an identity document a precondition for private communication, given the exclusion of undocumented people, minoritised communities and vulnerable children, and the disproportionate processing of biometric data this would entail.
- Defend the proper political process. Members should formally contest the use of the Rule 170 urgent procedure to revive rejected files, and demand a full fundamental-rights impact assessment and a fresh EDPS opinion before the permanent regulation advances in the September trilogues.
- Provide funds for the alternatives. Ring-fence MFF streams for open-source, interoperable, local-first communications infrastructure and for independent civil-society oversight, so that European digital sovereignty is built, not merely invoked.

Conclusion

The revival of Chat Control 1.0 is an indication that those in favour of suspicionless scanning of citizens' private messages will aggressively push for more dangerous privacy-eroding provisions in the final text of the CSA Regulation, perhaps even breaking encryption. A warning rather than a full defeat since its reach is narrow, the lesson of 9 July is that substance and procedure must be defended together, and that opposition within the Parliament alone will not suffice. The European Union should take a stance like that of the UN; reject suspicionless scanning, and protect encryption without exception. Furthermore, it is crucial for the EU's future to invest in public-interest infrastructure that makes trustworthy communication a durable European asset. September will be a decisive moment. ALT-TEXT intends to engage the permanent regulation on these terms.