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

Executive summary

On 9 July 2026 the European Parliament allowed the temporary ePrivacy derogation, widely known as Chat Control 1.0, to be revived until April 2028. This vote happened despite a majority of voting Members opposing it. Of 607 Members voting, 314 voted to reject the Council's position and 276 voted against rejection, with 17 abstentions. Because the file was handled as a second reading, rejection required an absolute majority of the full chamber, 361 votes, rather than a majority of those voting. The opposition fell 47 votes short. A measure that a majority of participating legislators rejected therefore became law by procedural default.

ALT-TEXT's position is definitive. 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 end-to-end encryption (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. The core tension

The protection of children from sexual abuse is an urgent concern. No one would contest that. The tension does not lie between child protection and privacy; it lies between two theories of how protection can be achieved. The first says that scanning the private messages of the entire population will surface enough abuse material to justify the intrusion. The second maintains that abuse is best addressed through targeted investigation of suspects, judicial oversight, and properly resourced law enforcement, and that mass scanning corrodes the actual security infrastructure that protects victims, survivors and reporting channels.

The evidence does not favour the first theory. The European Parliament's own study concluded that while detecting known material with established hash-matching technology is practical and reasonably accurate, no reliable method exists to detect previously unknown material without high error rates. Investigators are already overwhelmed: the German Federal Criminal Police Office reports that a large share of incoming alerts are not criminally relevant. Report volume is being

used as a proxy for impact, when the operational bottleneck is triage, not detection. 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.

The gap between the official accuracy claims and reality is 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 only 265 files (6.3 per cent) were ultimately completed. Set against the European Commission's public claim that detection is 99.9 per cent accurate, with false positives at one in fifty billion, these figures do not hold up. Worse still, the force 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 that data on the innocent. This is the machinery the derogation authorises, generating false suspicion against ordinary people and then keeping files on them after they have been cleared.

2. ALT-TEXT's position

ALT-TEXT maintains that the confidentiality of private communications is a structural precondition for a free society, not an optional convenience to be traded against each successive emergency. Encryption is what allows journalists to protect sources, lawyers to advise clients, survivors to contact helplines from trusted devices, and citizens to organise, practice dissent and create without a silent watchful eye in the middle. If Europe normalises the scanning of private messages, even voluntarily, we build a blueprint for authoritarian governments elsewhere to adopt without Europe's trias politica.

We therefore reject the framing that pits safety against freedom. That framing is false on its own terms: a communications system with a built-in inspection point is less safe for everyone, because the inspection point becomes an attack surface. The central matching database becomes a high-value target, comparable to the key databases of a key-escrow system. Introducing a systemic weakness to catch a minority of bad actors hands that same weakness to every other bad actor, from criminal networks to hostile states.

3. What was actually decided, and what was not

Precision matters here, because the headline “Parliament voted for Chat Control” understates how contested the outcome was and obscures where the real fight now lies. The revived measure is the temporary ePrivacy derogation, Chat Control 1.0. It permits, but does not require, providers to scan unencrypted or server-side-encrypted services for known CSAM. The platforms in scope are services such as Gmail, Instagram direct messages, Discord, Snapchat, Skype, Xbox messaging and iCloud Mail. Genuinely end-to-end encrypted services such as Signal, WhatsApp and iMessage were already outside its practical reach.

Parliament adopted an amendment explicitly excluding end-to-end encrypted communications from the law's scope. 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. The genuinely dangerous instrument, the permanent Child Sexual Abuse Regulation that would introduce mandatory detection orders and reach for client-side scanning of encrypted services, remains in trilogue and returns to the table in September. The 9 July vote is a holding pattern, not a resolution.

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 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 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, the file moves to conciliation.
September 2026	Trilogue negotiations on the permanent CSAR (“Chat Control 2.0”) resume under the Irish Council Presidency.

4. The procedural objection

ALT-TEXT objects to the manner of this revival as strongly as to its content. The Parliament rejected the derogation in March. A rejected, expired file was then reissued with materially the same content and pushed through under the Rule 170 urgent procedure on the last sitting day before the summer recess, when many Members had already departed. The urgent procedure inverted the ordinary burden: instead of supporters needing to win a vote, opponents needed an absolute majority of the entire chamber to stop it, so that every absence and every abstention 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. Breyer's assessment of the outcome was blunt: that a measure moving forward against the will of the majority of voting MEPs is, in his words, a farce that damages democracy.

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 inspection to the one place the user believed was private. The Global Encryption Coalition is explicit that client-side scanning and server-side methods are not alternatives to backdoors, they are backdoors.

The market consequence is definite. 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. 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.

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 share a commercial interest in 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, ring-fenced funding within the next Multi-Annual Financial Framework for open-source, local-first and interoperable communications infrastructure, for the digital commons, and for the independent civil-society organisations that provide technical oversight of these files. Open standards and interoperability are the durable structural remedy to platform monopoly: 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. The Cyber Resilience Act's security-by-design logic is fundamentally incompatible with a legal mandate to insert scanning backdoors, and that contradiction should be surfaced in every consultation.

The scanning agenda also contradicts the EU's own settled law. The Digital Services Act, adopted only 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. 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 of the Charter. 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 engineer it in another. This is precisely the incoherence ALT-TEXT tracks under the Digital Omnibus, where each new file is treated in isolation and the cumulative erosion of safeguards goes unexamined.

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

The costs of this regime do not fall 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 of the most vulnerable children out of the services they rely on to reach family, support workers or legal advice. Age assurance built on biometric processing compounds the harm by normalising the systematic handling of children's most sensitive data.

The regime also criminalises the ordinary. 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 that falls hardest on LGBTQ+ young people exploring their identity, sometimes in unsupportive homes. Beyond any specific case, the knowledge that private messages may be scanned exerts a chilling effect on expression. That effect is felt most acutely by those who hold power to account: journalists protecting confidential sources, whistleblowers, human-rights defenders and activists. This engages the European Media Freedom Act directly, since confidential source protection is a precondition of a free press, and a communications environment subject to standing inspection cannot honour it. A tool sold as child protection would quietly degrade the conditions for democratic scrutiny itself.

8. The citizenship dimension

This file is also a test of democratic and media literacy. 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 “protection” is packaged as surveillance, 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.

- **First, 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.
- **Second, 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.
- **Third, resource 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.
- **Fourth, 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.
- **Fifth, defend the 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.
- **Sixth, fund the alternative.** 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 a warning rather than a full on defeat. Its practical reach is narrow, but its precedent is not, and the permanent regulation it holds a place for is far more dangerous. The lesson of 9 July is that substance and procedure must be defended together, and that opposition alone is insufficient. The European Union should reject suspicionless scanning, protect encryption without exception, and invest in the public-interest infrastructure that makes trustworthy communication a durable European asset. The next decisive moment is September. ALT-TEXT intends to engage the permanent regulation on those terms.

References

The vote figures, procedural mechanics and timeline in this paper are drawn from the European Parliament's own record. Where a claim rests on a specific external source, it is listed below.

1. European Parliament, press release, "Combating child sexual abuse online: support for more limited ePrivacy derogation", 9 July 2026. Confirms the vote sequence (314–276–17), the second-reading absolute-majority requirement, the encryption-exclusion amendment, and the three-month referral to the Council. 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
3. Patrick Breyer, "EU Parliament greenlights Chat Control 1.0 – Breyer: 'Our children lose out'", 9 July 2026. Source of the quoted remarks and of the Commission and BKA effectiveness figures referenced above. https://www.patrick-breyer.de/en/eu-parliament-greenlights-chat-control-1-0-breyer-our-children-lose-out/
4. 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/
5. 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; concludes 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
6. European Commission, "Strengthening Europe's tech sovereignty", 3 June 2026. The European technological sovereignty package, comprising the Chips Act 2.0, the Cloud and AI Development Act, the open source strategy and an energy-digitalisation roadmap. https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_en
7. European Digital Rights (EDRi) and partners, "A safe internet for all: upholding private and secure communications", network position paper on the CSA Regulation. Companion analysis; source for the discussion of disproportionate harm to marginalised communities and of age-verification and identity risks. https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

Version control: July 2026
ALT-TEXT ASBL — Imagining a digital alternative