To sign this open letter, please do so here:
https://app.smartsheet.com/b/form/e43080d5ee6646f3bba7f081b440ba87

—-

We, the undersigned civil society organisations, companies and cybersecurity experts, including members of the Global Encryption Coalition, are writing to express our serious concern regarding the stated intention of Ireland's Minister for Justice to introduce domestic legislation that would give Irish police (An Garda Síochána) access to encrypted messaging services.[1]

The text of the proposed *Communications (Interception and Lawful Access) Bill* has yet to be made public, as drafting has not yet begun. The minister has indicated a review of Ireland's existing interception legislation, the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*, is under way, and drafting of the new bill will begin in the coming months.[2]

The announcement follows the publication of Ireland's *Programme for Government* in January, which outlined plans to introduce new data retention and interception laws, including provisions for over-the-top and encrypted services.[3] While the programme is titled "Securing Ireland's Future," these proposals risk achieving the very opposite.[4]

Systemic vulnerabilities
Weakening encryption would put both individuals and businesses at greater risk of scams, fraud, identity theft, and other cybercrime. It would also make sensitive data more vulnerable to foreign cyberattacks and undermine national security. At a time when cybersecurity is central to innovation and competitiveness, any erosion of encryption could have lasting consequences for Ireland's digital future and international standing.

It is a misguided belief that encrypted services can be weakened solely for "good guys" without also creating access pathways for malicious actors, including criminals, hackers and hostile state actors. Encryption is a critical security feature; any deliberate weakening or circumvention of it creates systemic vulnerabilities that would endanger everyone and put Ireland's national security at risk.

Impossible choice for encrypted providers

---

[1] Speech by Minister for Justice, Home Affairs and Migration, Jim O'Callaghan: A Contested Arena: Balancing competing human rights in the area of Justice, Home Affairs and Migration, 16 July 2025, https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/publications/speech-by-minister-for-justice-home-affairs-and-migration-jim-ocallaghan-a-contested-arena-balancing-competing-human-rights-in-the-area-of-justice-home-affairs-and-migration/#access-to-data-for-law-enforcement
[2] Ibid
[3] Programme for Government 2025 Securing Ireland's Future, p.121, January 2025, https://assets.gov.ie/static/documents/programme-for-government-securing-irelands-future.pdf
[4] Programme for Government 2025 Securing Ireland's Future, January 2025, https://assets.gov.ie/static/documents/programme-for-government-securing-irelands-future.pdf

If Ireland passes a law giving it the authority to compel encrypted messaging services to build a backdoor to give An Garda Síochána access to the plain text of encrypted messages, platforms offering end-to-end encryption will face an impossible choice: either comply and weaken the security of their services, or exit the Irish market.

In both cases, the result would be weaker security and reduced privacy for Irish citizens, businesses, and institutions that depend on encryption to maintain trust in the digital world, including Irish Government ministers and the gardaí themselves.

Legal precedent

Irish efforts to force access to encrypted services is unlikely to stand up in court due to the disproportional impact on human rights, including freedom of expression. In *Podchasov v Russia*, the European Court of Human Rights last year held:

> …[the] statutory obligation to decrypt end-to-end encrypted communications [...] is accordingly not proportionate to the legitimate aims pursued […]Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general, and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications."[5]

The UN High Commissioner for Human Rights has similarly been clear: mandating so-called backdoor access to encrypted communications creates liabilities that go far beyond their usefulness with regard to specific users identified as crime suspects. Such access jeopardises the privacy and security of all users, exposing them to unlawful interference.[6]

Ireland and EU 'Chat Control'

This domestic proposal must also be seen in the context of Ireland's continued support for the hugely controversial and widely criticised[7] EU Child Sexual Abuse Regulation, also known as 'Chat Control', which would mandate the mass scanning of private communications, including encrypted conversations, for child sexual abuse material (CSAM).

It must also be seen in the context that Ireland maintains the position that this type of scanning is comparable to companies scanning for spam or malware,[8] even though they are not comparable.[9]

---

[5] *Podchasov v Russia*, Application no. 33696/19, 77, European Court of Human Rights, 13 February 2024 https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-230854%22]}

[6] The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, August 2022, https://docs.un.org/A/HRC/51/17

[7] Is this the most criticised draft EU law of all time?, EDRi, 29 August, 2023, https://edri.org/our-work/most-criticised-eu-law-of-all-time/

[8] Speech by Minister for Justice, Home Affairs and Migration, Jim O'Callaghan: A Contested Arena: Balancing competing human rights in the area of Justice, Home Affairs and Migration, 16 July 2025, https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/publications/speech-by-minister-for-justice-home-affairs-and-migration-jim-ocallaghan-a-contested-arena-balancing-competing-human-rights-in-the-area-of-justice-home-affairs-and-migration/

[9] EDRi, Briefing on the fundamental differences between spam/malware filters and CSA detection in private communications, September 2025, https://edri.org/wp-content/uploads/2025/09/Briefing-on-the-fundamental-differences-between-spam-malware-filters-and-CSA-detection-in-private-communications.pdf

As emphasized in previous Global Encryption Coalition statements, including the most recent Steering Committee statement,[10] mandated scanning in encrypted environments creates a dangerous false sense of security for children and parents. Mandated scanning of encrypted communications undermines security and privacy for everyone, but could easily be circumvented by criminals who would continue to share illegal material.

These concerns were recently shared by Ireland's former special adviser on cybersecurity to Europol Brian Honan who has warned Chat Control would not just threaten individual privacy and undermine public trust in digital life, it would also open an enormous attack surface intentionally built into every European device that hostile states, authoritarian governments and cybercriminals could exploit for their own nefarious means.[11]

Ireland is among 15 countries who support 'Chat Control' while Austria, Finland, the Netherlands, Poland, the Czech Republic and Belgium have opposed it, citing privacy and security concerns. Belgium has reportedly called the bill "a monster that invades your privacy and cannot be tamed."[12]

If the impasse[13] remains unresolved by the latter half of 2026, when Ireland assumes the EU Council Presidency, and Irish authorities steer Chat Control while continuing to underestimate the grave consequences of weakening encryption - as evidenced by the current domestic proposal - the privacy and security of all European citizens, and beyond, will be at risk.

Errors and misidentification

It is important to recall that Irish institutions and civil society have already highlighted the flaws and real-life dangers inherent in the proposal.

In March 2023, Ireland's parliamentary justice committee issued a communication opposing the EU proposal over concerns about mass surveillance and the undermining of the security of everyone's communications[14] but this position has not been reflected in Brussels.[15]

---

[10] GEC Steering Committee Statement on 1 July Text of the European CSA Regulation, 2 September 2025, https://www.globalencryption.org/2025/09/gec-steering-committee-statement-on-1-july-text-of-the-european-csa-regulation/

[11] Brian Honan, Proposed EU Chat Control regulation could create surveillance state, Irish Examiner, 8 September 2025, https://www.irishexaminer.com/opinion/commentanalysis/arid-41700062.html

[12] Belgium, https://fightchatcontrol.eu/

[13] 16 countries burned Poland's bridges on the CSA Regulation: What now?, EDRi, 21 August 2025, https://edri.org/our-work/16-countries-burned-polands-bridges-on-the-csa-regulation-what-now/

[14] Political Contribution on Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse {SEC(2022) 209 final} - {SWD(2022) 209 final} - {SWD(2022) 210 final} March 2023, https://opac.oireachtas.ie/Data/Library3/Documents%20Laid/2023/pdf/MTQzZG9jc2xhaWQzMDAzMjAyM18gMzAwMzIzXzEyMjEzMA%3D%3D.pdf

[15] Chat Control: The list of countries opposing the law grows, but support remains strong, Tech Radar, 30 August 2025, https://www.techradar.com/computing/cyber-security/chat-control-the-list-of-countries-opposing-the-law-grows-but-support-remains-strong

Six months earlier, civil society in Ireland published rare figures[16] demonstrating that the error-prone scanning techniques at the heart of this EU proposal are already resulting in innocent people being wrongly flagged as sharers of child sexual abuse material.

The US National Center for Missing and Exploited Children (NCMEC) has been forwarding information about suspected CSAM, and people suspected of sharing it, to An Garda Síochána since 2010. In 2022, the Irish Council for Civil Liberties (ICCL) and Digital Rights Ireland (DRI) obtained data about NCMEC's 2020 referrals to Ireland. They showed that An Garda Síochána received 4,192 referrals in 2020, of which 409 were "actionable". A higher number - 471 or 11% - were deemed *not* CSAM by An Garda Síochána themselves. The people concerned were innocent, and the materials were innocuous images or videos, such as children playing on a beach.[17]

Yet even after *clearing* those wrongly flagged, An Garda Síochána did not delete their data. Instead it retains personal data about people wrongly flagged as "reference and intelligence material in respect of future investigations".[18] It is unknown how many people cleared of suspicion of sharing CSAM remain in An Garda Síochána's files.[19] But should Chat Control be enacted, as currently drafted, there would be many more innocent people in those files.

Recommendations

Any country that undermines encryption risks threatening the privacy and security of people far beyond its borders. But Ireland, as host to the EU headquarters of major tech companies including Apple and Meta, bears particular responsibility. We make the following recommendations:

- We call on Minister O'Callaghan to reconsider his stated intention to grant An Garda Síochána access the plain text of encrypted messages
- We call on Ireland's Ministers in the Council of the EU to change their position on Chat Control, withdrawing their support for mandated scanning within encrypted environments.

We remain committed to providing our collective expertise and invite Minister O'Callaghan to meet with us so we can engage in constructive dialogue and ensure any legislation - domestic or EU - protects, rather than undermines, the privacy, security, and fundamental rights of people in Ireland and beyond.

---

[16] Susan Landau, The EU's dangerous proposal for stopping online child sexual abuse material, The Progressive Post, 5 July 2023, https://feps-europe.eu/the-eus-dangerous-proposal-for-stopping-online-child-sexual-abuse-material/

[17] An Garda Síochána unlawfully retains files on innocent people who it has already cleared of producing or sharing of child sex abuse material, Irish Council for Civil Liberties, 9 October 2022, 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/

[18] Gardaí defend policy of keeping data of cleared people, RTE, 19 October 2022, https://www.rte.ie/news/ireland/2022/1019/1330023-garda-data/

[19] An Garda Síochána unlawfully retains files on innocent people who it has already cleared of producing or sharing of child sex abuse material, Irish Council for Civil Liberties, 9 October 2022, 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/

Signatories:

Organizations

Blacknight Internet Solutions Ltd
Castlebridge
Center for Democracy & Technology
Girlhype Coders - Women In Tech
Global Partners Digital
Internet Society
Internet Society Catalan Chapter
Internet Society Colombia Chapter
Internet Society India Hyderabad Chapter
Internet Society Lesotho Chapter
Internet Society - Paraguay chapter
Internet Society South Sudan Chapter
Irish Council for Civil Liberties
Koneta Hub
LGBT Tech
Mozilla
Paperclip Inc.
The Tor Project
Tolerant Networks LTD
Tuta Mail

Individual Experts*

Prof. Jordi Domingo-Pascual, Universitat Politècnica de Catalunya (UPC BarcelonaTECH)
Dr. Stephen Farrell, Trinity College Dublin
Dr Elizabeth Farries, UCD Centre for Digital Policy
James Gannon, PharmaLedger Association
prof. dr. Jaap-Henk Hoepman (Radboud University, The Netherlands and Karlstad University, Sweden)
Nick Hilliard, Island Bridge Networks Ltd
Mallory Knodel, NYU
Barry Leiba, ICANN Security and Stability Advisory Committee
Daragh O Brien, Founder and Managing Director, Castlebridge
Barry O'Donovan, Internet Infrastructure Specialist, Open Source Solutions Ltd
Conor Murphy, Dublin Linux Community
Michele Neylon, CEO of Blacknight, Irish internet entrepreneur
Niall O'Reilly, RIPE
Paul Wouters, Internet Engineering Task Force (IETF) Security Area Director

***Affiliations listed for identification purposes only**