DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

9 Ref: OIA-2025/26-0406

9 February 2026

[redacted]

Tēnā koe [redacted]

Official Information Act request relating to European Union's Chat Control

Thank you for your Official Information Act 1982 (the Act) request, which was received by the Department of the Prime Minister and Cabinet (DPMC) on 18 December 2025. You requested:

> *I'm requesting any records the DPMC may have regarding the European Union's Chat Control.*

Information being released

One document has been identified as relevant to your request titled *'Working Group Recommendations Preliminary Papers Annexes June'.* Please find attached two pages from that document which are being provided as an extract, as allowed per section 16(1)(e) of the Act. A small amount of information has been withheld as it is not in scope of your request and is marked accordingly.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on DPMC's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Nāku noa, nā

Jeremy Clarke-Watson
Deputy Chief Executive
National Security and Resilience

Executive Wing, Parliament Buildings, Wellington, New Zealand 6011
☎ 64 4 817 9698 www.dpmc.govt.nz

Not in Scope

European Union

31. In the European Union (EU) the German Presidency of the Council of the EU called for a 'balance between security through encryption and despite encryption.' The declaration called on EU Member States to work with industry to create this balance and establish a regulatory framework and innovative approaches.

32. On 11 May the European Commission proposed a new legislation to create a uniform EU approach to preventing and combatting child sexual abuse material (CSAM) online, as well as to support the work of law enforcement and assistance to victims.

33. Progressing the legislation is a priority for President von der Leyen's Commission, as CSAM online has overwhelmingly increased in recent years, particularly during the pandemic (up to 25% in some Member States), and Europe is a global hub for this material (with 60% estimated to be hosted on EU servers).

34. Another key driver for a binding EU legal framework is to replace the current temporary system in place until August 2024, which is based on voluntary detection and reporting by companies – under the ePrivacy Directive temporary derogation Not in Scope . While voluntary action is important, it has been judged insufficient, especially noting that in 2019 and 2020, 95% of all reports globally came from one single service provider despite evidence that the problem does not exist only on one platform.

35. The legislation follows the July 2020 EU Strategy for a More Effective Fight Against Child Sexual Abuse, which set out a comprehensive response to the growing threat of child sexual abuse both offline and online, by improving prevention, investigation, and assistance to victims. It also comes after the Commission presented its March EU Strategy on the Rights of the Child, which proposed reinforced measures to protect children against all forms of violence, including abuse online.

36. The CSAM proposal obliges online service providers offering services in the EU, including hosting services, messaging services, app stores and internet access providers - which together have been identified as the services most misused for CSAM - to prevent child sexual abuse online. Providers will have to assess whether their services can be misused for online child sexual abuse (CSA), including for grooming or the dissemination of illegal material, and put in place mitigation measures.

37. The obligation to detect, which has proved the most controversial proposal due to privacy and mass surveillance concerns, would only come into place if the risk of online CSA after putting in place mitigation measures remains high and a court or an independent national authority considers it necessary.

Not in Scope

38. The legislation is technology neutral and encrypted services are not exempted from the requirements. If a service provider is not established in an EU member state but offers services in the EU, they will be required to designate a legal representative in the EU to facilitate enforcement of the legislation. If a service provider does not comply, they risk court orders to take action and fines of up to six percent of their global revenue. To enforce the above obligations, the proposal creates national authorities in each EU Member State, similar to the model in the Digital Services Act, the Coordinating Authorities on Child Sexual Abuse issues. They are empowered to impose penalties in case on infringements of the legislation.

39. Before the legislation can be adopted, the Commission proposal will need to be agreed by the European Parliament and the Council. Whether this is straightforward remains to be seen. While it is widely recognised the EU needs to do better at tackling CSAM online, the proposal has received criticism from members of the European Parliament (as well as privacy advocates). They have expressed concern that the legislation risks undermining privacy online, including for end-to-end encrypted messages and enabling mass surveillance. German MEP Patrick Breyer said, "This plan is nothing other than terrorism against our digital fundamental rights, which I will not relent to fight" while German MEP Moritz Körner said the proposals risked dealing a knockout blow to "the privacy of digital correspondence."

40. The proposal is also already proving controversial with EU member states, primarily Germany. In a press release, the country's digital minister Volker Wissing said the European Commission was going "too far" and that the proposal could interfere with a German legal right to confidentiality of communications. "We must protect digital civil rights, which includes a right to encryption. We need a protected space for private communication," he said. "The general control of chat histories and bypassing encryption go too far."

41. European Commission Vice-President Margaritis Schinas pushed back on these assertions - characterising the new rules as "clear, targeted and proportionate obligations," with what service providers are able to do as "very tightly ring-fenced." He compared the rules as allowing services to undertake "programme scanning for markers of illegal contenting the same way cyber security programmes run constant checks for security breaches." Through its design, the Commission considers the new rules require service providers to use the least intrusive measures. Any necessary reviews would take place on an anonymous basis, and only to identify users in case potential online child sexual abuse is detected. The technology used would not be able to extract any other information than what strictly necessary to detect the abuse.

42. With the ratification of the EU – New Zealand Agreement that will allow the exchange of personal data to fight serious crime and terrorism (the Europol Agreement) on the near horizon, this legislation will also potentially increase opportunities for law enforcement cooperation on CSAM between New Zealand and the EU. This includes the potential to bring more perpetrators to justice and help victims.