



New Zealand House of Representatives
Te Whare Māngai o Aotearoa

Petitions Committee

Komiti Whiriwhiri Take Petihana

54th Parliament
August 2026

Petition of Katja Feldtmann: Strengthen enforcement powers and penalties under the Privacy Act 2020

Presented to the House of Representatives
by Greg O'Connor, Chairperson

Contents

Recommendation.....	3
Request regarding the Privacy Act.....	3
Comments from the petitioner.....	3
Comments from the Office of the Privacy Commissioner	4
Comments from the Ministry of Justice.....	5
Our response to the petition	5
Appendix.....	7

Petition of Katja Feldtmann

Recommendation

The Petitions Committee has considered the petition of Katja Feldtmann—Strengthen enforcement powers and penalties under the Privacy Act 2020—and recommends to the Government that it commence a review of the Privacy Act, with particular regard to the potential harms arising from artificial intelligence and other emerging technologies.

Request regarding the Privacy Act

This petition was signed by 1,533 people. It was presented to the House by Hon Dr Ayesha Verrall on 10 March 2026, and requests:

That the House of Representatives increase penalties for serious or repeated privacy breaches, strengthen the Office of the Privacy Commissioner's enforcement powers, and improve accountability where organisations fail to protect personal or health information.

Comments from the petitioner

The petitioner noted the 2025 annual report of the Office of the Privacy Commissioner, which stated that “serious” privacy breaches had increased by 43 percent since the previous year. Ms Feldtmann is concerned that, given the number of privacy breaches occurring in New Zealand, both the Office of the Privacy Commissioner's enforcement powers and the penalties available under the Privacy Act 2020 are insufficient. She said that the Privacy Commissioner lacks an adequate legal framework to enforce compliance or to issue penalties that act as a real deterrent.

The petitioner argues that major data breaches in 2026, such as the Manage My Health and MediMap breaches, are evidence of systemic issues in which organisations are not incentivised to establish effective controls over cybersecurity and privacy. Ms Feldtmann warned that, without credible enforcement mechanisms, New Zealand risks attracting or enabling organisations that fail to invest in adequate data protection practices.

International practice

Ms Feldtmann referred to Australia's Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022, which expanded the enforcement powers of the Office of the Australian Information Commissioner and introduced a severe penalty regime. The regime includes a maximum fine for serious or repeated breaches of \$50 million or 3 times the benefit obtained, or 30 percent of adjusted turnover during the period of the breach, whichever is higher. The EU's General Data Protection Regulation sets the maximum fine for

serious data breaches at EUR 20 million, or 4 percent of global annual turnover, whichever is higher.¹

In Ms Feldtmann's view, New Zealand risks positioning itself as a regulatory outlier among OECD jurisdictions because of its limited enforcement tools and small penalties. She stated that the maximum penalty under the Privacy Act is \$10,000, and that enforcement relies on investigation, mediation, or referral to the Human Rights Review Tribunal. She said it is evident, given increasing data breaches and global regulations, that the enforcement mechanisms in the Privacy Act do not match the complexity, scale, or consequences of modern data breaches.

The petitioner's request

The petitioner would like the House to consider:

- establishing a new, much stronger penalties regime
- strengthening the Privacy Commissioner's enforcement abilities by, for example, allowing the office to conduct regulatory audits and to require organisations to demonstrate how they meet their privacy requirements
- modernising the Privacy Act to address potential harms arising from artificial intelligence, such as by introducing a "right to erasure" that allows individuals to ask organisations to delete their personal information.

Ms Feldtmann said this would strengthen trust, raise standards, better protect people's information, improve outcomes for people affected by breaches, and enable more secure innovation through digital services.

Comments from the Office of the Privacy Commissioner

The Privacy Commissioner said the Privacy Act does not provide sufficient incentives for many organisations to understand or meet "the most basic privacy requirements". He referred to articles and submissions he has written since 2018 that call for stronger penalties and greater enforcement powers to be included in the Act. He told us that compared to Australia's multimillion dollar penalty regime, New Zealand lacks a civil penalty regime.

The commissioner said that strengthening the office's enforcement powers would enable it to monitor and respond to non-compliance with a broader range of options. He said that allowing the office to conduct regulatory audits would support intervention prior to harm.

The commissioner commented on Ms Feldtmann's suggestion of a "right to erasure". He noted that since his predecessor recommended adding this to the Privacy Act, the EU's General Data Protection Regulation has provided precedents for when a right to erasure is useful. This includes when an individual has withdrawn consent or where information has been unlawfully obtained. He pointed out that the right to erasure shifts decision-making from the agency to the individual, giving the latter more control over their personal information.

¹ The European Union General Data Protection Regulation (GDPR) came into force in 2018, pioneering a significant penalty regime and new privacy rights (such as the "right to erasure"). The United Kingdom passed the Data Protection Act 2018 to implement the GDPR.

Comments from the Ministry of Justice

The ministry described the existing investigative functions of the Privacy Commissioner, and the commissioner's abilities to issue compliance notices and refer matters to the Director of Human Rights Proceedings.² The Director may decide to bring a case before the Human Rights Review Tribunal, which can order damages up to a maximum of \$350,000 if satisfied that an individual's privacy has been interfered with. The ministry noted that some breaches of the Privacy Act may result in criminal prosecution, but said that these mostly relate to procedural matters rather than infringements of an individual's privacy.

The Privacy Commissioner's submission on the Privacy Amendment Act

The ministry referred to the Privacy Commissioner's submission to the Justice Committee on the Privacy Amendment Act 2025.³ In his submission, the commissioner noted that the Privacy Act 2020 is missing obligations, rights, and powers that have been deployed internationally to address new technologies. These include AI, biometrics, and everyday items that, due to sensors and software, can collect information and act autonomously.

He noted that offences in the Privacy Act are insufficient for enforcing serious breaches of privacy. He said that "many agencies are aware of the lack of meaningful financial penalties and limited compliance powers and so are not incentivised to consider privacy in the same way they consider other standards, such as financial reporting requirements and health and safety".

The commissioner referred to the EU's and UK's General Data Protection Regulation, and noted that Australia passed a first tranche of legislative privacy reforms in 2024, in addition to its severe penalty regime.⁴ He said the Privacy Act is beginning to lose alignment with international best practice, which may lead to consequences for international cooperation and trade.

Advice being developed by the Ministry of Justice

The Government's recent Cyber Security Strategy 2026–2030 is accompanied by the Cyber Security Action Plan 2026–2027. Among other actions, the plan states that the ministry will advise on options that could incentivise the protection of personal information from cyber threats, such as introducing a civil penalty regime under the Privacy Act. The ministry said it would seek decisions from Ministers "in due course".

Our response to the petition

We note the Office of the Privacy Commissioner's report, *Research on Privacy Concerns and Use of Personal Information*, published in May 2026.⁵ The report states that only 18

² The Director heads the Office of Human Rights Proceedings, which is an independent part of the Human Rights Commission.

³ Office of the Privacy Commissioner, Submission on the Privacy Amendment Bill, 10 December 2024; paragraphs 24 and 27.

⁴ In Australia, the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 introduced a severe penalty regime. The Privacy and Other Legislation Amendment Act 2024 introduced a statutory tort for serious privacy intrusions, criminalised doxing, established a Children's Online Privacy Code, and expanded the enforcement powers of the Office of the Australian Information Commissioner.

⁵ Privacy Commissioner, Research on Privacy Concerns and Use of Personal Information, 11 May 2026.

percent of those surveyed are confident or very confident that New Zealand law adequately protects personal information, while 33 percent have little or no confidence.

We agree with Ms Feldtmann that, in the interests of this country's international trade and the rights of New Zealanders, the Privacy Act must be modernised. We recognise the work being done by the Ministry of Justice to advise on options that could incentivise the protection of personal information from cyber threats. We recommend that the Government commence a review of the Privacy Act, with particular regard to the potential harms arising from artificial intelligence and other emerging technologies.

Appendix

Committee procedure

The petition was signed by 1,533 people on the Parliament website. It was presented to the House by Hon Dr Ayesha Verrall on 10 March 2026 and referred to us on the same day. We met between 26 March 2026 and 27 August 2026 to consider it. We received written submissions from the petitioner, the Ministry of Justice, and the Office of the Privacy Commissioner.

Committee members

Greg O'Connor (Chairperson)
Hon Andrew Bayly (from 1 July 2026)
Greg Fleming
Paulo Garcia (until 1 July 2026)
Celia Wade-Brown

Related resources

The documents we received as evidence in relation to this petition are available on the [Parliament website](#).