Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner
PO Box 10094, The Terrace, Wellington 6143
Level 11, 215 Lambton Quay
Wellington, New Zealand
P +64 4 474 7590 F +64 4 474 7595
E enquiries@privacy.org.nz
0800 803 909 Enquiries
privacy.org.nz

31 January 2025

Hon Paul Goldsmith
Minister of Justice
Parliament Buildings
WELLINGTON

Dear Minister

QUARTERLY REPORT OF THE PRIVACY COMMISSIONER FOR THE PERIOD 1 OCTOBER 2024 TO 31 DECEMBER 2024

Highlights

In October, the Justice Committee undertook its 2022/23 annual review of the Office of the Privacy Commissioner. This hearing went well, with the Privacy Commissioner outlining the importance of New Zealanders being able to trust agencies to protect their personal information. The Commissioner noted that as regulator we face a range of challenges, including the lack of accountability mechanisms and fines in the Privacy Act 2020 and funding constraints. These challenges are driving a need to increasingly prioritise our activities as key operational volumes increase. Committee members were interested in a range of topics including artificial intelligence, facial recognition, the Police photographing of youth and access to the Motor Vehicle Register.

We established a Māori Reference Panel in December, with the objective of advising the Privacy Commissioner about how we can work in partnership to further develop Māori perspectives about privacy. The Privacy Commissioner appointed members to ensure that the panel has a strong mix of expertise in Māori privacy matters and community leadership. The members of the Panel are Kura Moehau, Tahu Kukutai/Vanessa Clark, Māhera Maihi, Chris Cormack and Mercia Yates.

Foodstuffs North Island announced that their six-month facial recognition system trial across 25 New World and PAK'nSAVE supermarkets was successful in avoiding approximately 100 serious harm incidents. We are currently assessing the results of the independent evaluation that Foodstuffs commissioned and have requested some further information to inform our Inquiry into the trial. We expect to complete our Inquiry in the next few months.

A major achievement during this quarter was the release of the Biometrics Process Privacy Code for public consultation, as detailed in the next section.

Consulting on the Biometrics Process Privacy Code

On 18 December the Privacy Commissioner announced his intention to issue the Biometrics Processing Privacy Code. Public consultation on the Biometrics Code is being held in accordance with the statutory requirements of the Privacy Act and submissions are due from agencies and the public by 14 March 2025.

The Biometrics Code will modify some of the principles in the Privacy Act and create more specific privacy rules for agencies using biometric technologies to collect and process biometric information. The major additional rules in the Code are:

- adding a requirement to do a proportionality test and put in place privacy safeguards
- stronger notification and transparency obligations
- limits on some uses of biometric information (e.g. emotion analysis and types of biometric categorisation).

This is the second round of consultation on the development of a Code for biometrics, following consultation on an exposure draft in April 2024 and engagement with key technology agencies.

The feedback we received on the exposure draft led to us simplify some aspects of the Biometrics Code. This simplification will improve the understanding of what biometrics processes are in covered by the code and what is exempt or remains subject to the Privacy Act or the Health Information Privacy Code.

The restrictions on using biometrics (fair use limits) are now targeted to the most intrusive and highest risk uses. We have also added a new requirement for agencies to tell people where they can find a rundown of their assessment that agencies will be required to undertake of the relative benefits and impacts of using biometrics, if this is made public.

Other changes to the Biometrics Code include increasing the commencement period from six months to nine months for agencies already using biometrics and allowing agencies to undertake trials to assess the effectiveness of their proposed use of biometrics.

Draft guidance material has been developed to help organisations know what the rules will be and explain how to comply with the Code. The Code is expected to be issued and come in force in 2025.

Activities of our Office

Policy

Our Policy team progressed a review of schedule 4 of the Telecommunications Information Privacy Code, which provides for the cell phone location information of individuals to be provided to emergency services. This schedule was last revised in 2020 and requires review as the host agency of key information systems is shifting from MBIE to the Next Generations Critical Communications group hosted by New Zealand Police. Other minor amendments are also necessary to ensure the schedule remains fit for purpose. Any potential amendments will be publicly consulted in upcoming months.

The issues in the Government's policy programme we were consulted on in the last quarter included:

- the contribution of boarders to in the calculation of subsidies for private and social housing
- penalties related to anti-social road use
- the Time of Use Charging Bill, relating to road charges
- the potential for the greater use of data under the social investment approach
- engaging with StatsNZ on the future of the Integrated Data Infrastructure.

We also submitted on the following Bills being considered by Select Committees:

- Responding to Abuse in Care Amendment Bill
- Mental Health Bill
- Crown Minerals Amendment Bill.

The Privacy Commissioner attended the Australia New Zealand Summit of the International Association of Privacy Professionals (IAPP), which was held in Sydney in December. The Commissioner was a keynote speaker at the Summit and spoke about artificial intelligence, the guidance work our Office has been doing and the attitudes and concerns that New Zealanders have about privacy. The Deputy Privacy Commissioner attended the Asia Pacific Privacy Authorities Forum held in Japan that provided an opportunity to discuss privacy developments and build networks with other privacy regulators in our region.

Capability and guidance

Our Capability and Guidance team issued guidance throughout this quarter to help agencies and individuals navigate and understand their privacy obligations. This guidance related to:

- the use of third-party providers, which is a topic we regularly receive questions about from both public and private sector agencies
- step-by-step guidance on how agencies can manage privacy complaints, including maintain relationships with their customers and clients so the complaints are less likely escalated to our Office.

The Capability and Guidance team continues to engage groups from around the country to build an understanding of how to meet privacy requirements while maintaining efficient processes. Examples of this engagement include presentations to the MBIE Project Management Community of Practice, the South Island Privacy Network and recording a podcast with Retail New Zealand to help support retailers.

The team also completed the information gathering stage of the review of the Gang Intelligence Centre Approved Information Sharing Agreement and are drafting our provisional findings. This draft report will be circulated to the government agencies involved in this information sharing agreement before completing the report. We have also reviewed and provided feedback on operational protocols for a number of other AISAs.

There were a range of statutory consultations on international and domestic information sharing agreements, including under the Policing Act, Land Transport Act, Integrity Sport and Recreation Act, and Public and Community Housing Management Act.

Communication and engagement

Improving communication for diverse audiences was a theme for our Communications team. For example, after we were approached by a mining business who wanted to educate their staff about privacy but did not have easy internet access, we developed our Privacy ABCs e-learning module into a presentation with voiceover to allow them and others in similar remote locations to keep learning. We have made this resource available online for other agencies.

Another improvement we made was to develop versions of our privacy rights brochure into Simplified Chinese, Traditional Chinese, and Vietnamese, which can be printed out by anyone wanting them.

This was a busy media quarter as privacy issues continue to be relevant and interesting to wider society. We issued six proactive media releases:

1. Nobody should be happy we've received over 1000 privacy complaints
2. Statement in response to Inland Revenue's updated hashing information relating to social media companies
3. Global privacy authorities issue follow-up joint statement on data scraping after industry engagement
4. Camera creep/s causing concern
5. Police well on the way to compliance; one critical step remains
6. Privacy Commissioner announces intent to issue Biometrics Code.

We answered media enquiries from New Zealand and Australia about privacy breaches at Bloom Hearing (ransomware attack)[1], Palmerston North City Council (breach of submitters personal details)[2] and Saint Kentigern (cyber attack).[3] The issues we spoke to media about included intimate recordings, our Inquiry into the Foodstuffs facial recognition trial, Bunnings Australia's use of facial recognition, banking scams, Chat GPT, 23 and Me and artificial intelligence.

As an Office we give at least 80 presentations and speeches a year. The highlight this quarter was the Commissioner's speech to NZX top 50 chairs (speaking on AI and privacy), at the request of the Institute of Directors, at their Millbrook retreat.

Compliance and enforcement

The Compliance and Enforcement team has observed a change in the volume and causes of privacy breach notifications from public sector agencies that may cause serious harm. The number of serious privacy breaches this financial year is significantly lower, with a 51% decrease for the July to December 2024 period when compared to July to December 2023. Our working hypothesis is that the reduction in reporting serious privacy breaches may be due to a reduction in privacy and information management staff in public sector agencies.

---

[1] https://www.nzherald.co.nz/nz/new-zealand-hearing-clinic-bloom-warns-of-massive-data-theft-in-ransomware-attack/PQX7ZE3GGRAQDDP7ABPLP37CAU/

[2] https://www.thepost.co.nz/nz-news/350432603/liquor-licence-objectors-details-accidentally-shared

[3] https://www.nzherald.co.nz/nz/saint-kentigern-college-cyber-attack-auckland-private-school-warns-of-phishing-emails-data-breach/SNYF2DVMARHPJMHLG3BN7WNLLY/

We are also observing an increase in the proportion of public sector serious privacy breaches caused by employee browsing or unauthorised sharing. In the year to date these types of breaches are 45% of serious public sector breaches, while in 2023/24 they were only 32%. We will continue to monitor these developments, especially as we have not seen such significant changes in private sector reporting.

We have continued our investigation into the Latitude Finance breach of 2023 where identity and financial information of over 1 million New Zealanders was stolen in a cyber-attack. Our investigation has focused on possible breaches of the information retention and security elements of the Privacy Act. We are now aligning our findings with the Australian Privacy Commissioner on its investigation so that we can leverage the cyber security analysis of the breach that it is commissioning.

At the time of writing, we are awaiting the final outcome of the Public Service Commission Inquiry into data misuse allegations at Manurewa Marae and the Stats NZ independent investigation into the potential misuse of 2023 census data. We expect the Inquiry to make a referral to us on some matters.

Investigations and dispute resolution

As outlined in Appendix A, we continue to receive privacy complaints and public enquiries at high levels. During this quarter the total number of privacy complaints increased to a record high level, driven by a 66% increase in complaints that we took a fast resolve approach to. Complaints for investigation decreased in this quarter (from 107 to 87) while public enquiries also decreased by 8%.

As reported in our last quarter, given our constrained resources we have focused on the efficiency of our processes while allocating some of our diminishing cash reserves to temporarily bolster this function.

The management of organisational risk

During this quarter we reviewed and updated our organisation wide risks and the associated risk management architecture. This review showed that the key risks facing our Office remain the same, with long-term financial sustainability and health, safety and wellbeing of our people continuing to be priorities.

With respect to long-term financial sustainability, we continue to proactively work at identifying areas of savings, whilst remaining mindful of our ability to deliver a large proactive work programme and reactive core services. Note that we have had some early discussions with MBIE officials on how we could be resourced to undertake our responsibilities as a regulator of the Customer and Product Data Bill. We will keep you informed as to how these discussions progress.

For health, safety and wellbeing we continue to see elevated levels of unreasonable conduct from some members of the public. We address this through situational safety training and revisiting our policies covering physical security threats. This is being monitored closely within the Office.

Financial report

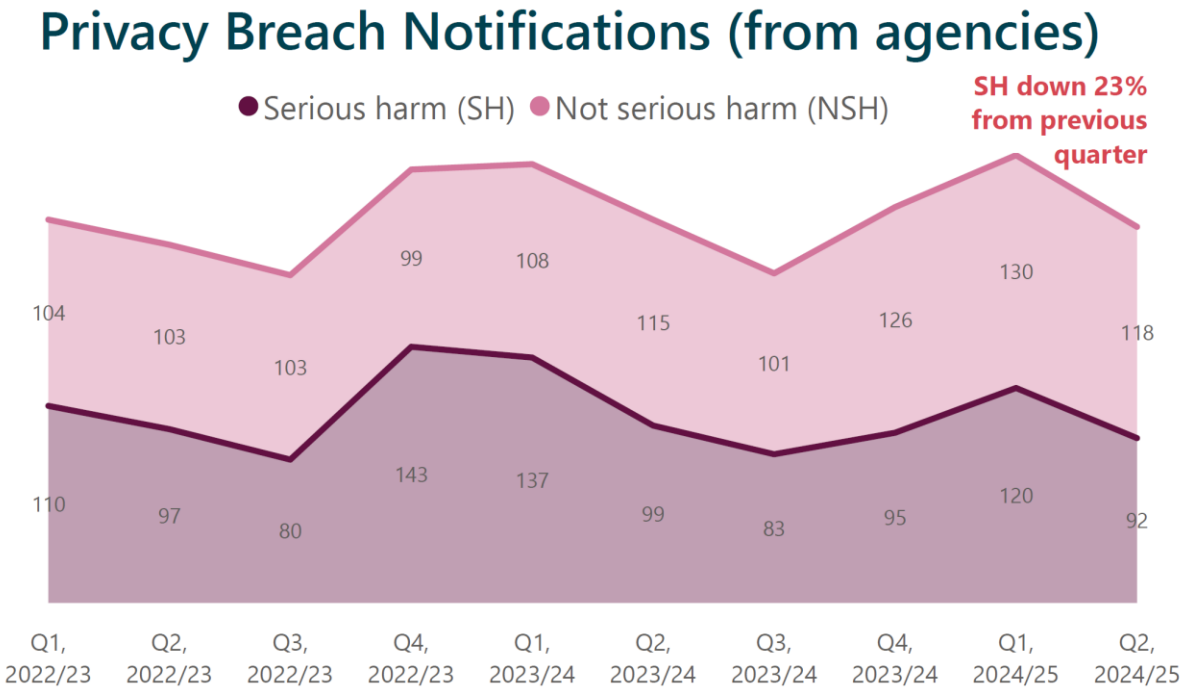
We are reporting a deficit of $121,655 for the three months ending 31 December 2024. This is favourable against a budgeted deficit of $373,638. The variance against budget is mainly due to decreased staff costs as a result of vacancies as a result of staff resignations, plus decreases in computer maintenance and network costs. These decreases have been offset by increases in specialist services for an independent security review, and policy and legal services. We are currently forecasting a deficit of $533,000 for the year to June 2025. The Office will be utilising cash reserves to fund this deficit for the current financial year. Further details of financial information and performance against the Statement of Performance Expectations are included as appendices to this report.

Yours sincerely

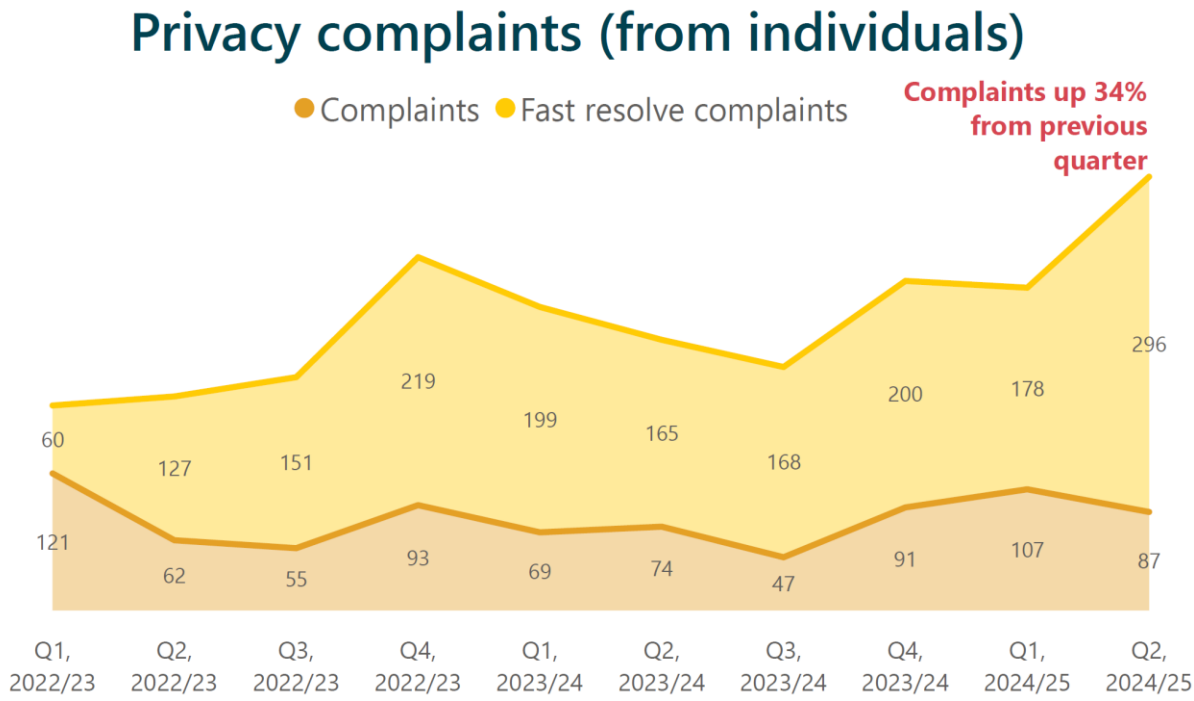
Michael Webster
Privacy Commissioner

Encl: Appendix A: Key operational volumes
Appendix B: Financials for period ending 30 September 2024
Appendix C: Performance against Statement of Performance Expectations - Year to Date

Appendix A: Key operational volumes



Agencies are required to notify OPC of serious/extreme harm data breaches. A single breach can impact a number of individuals for example the Latitude Finance data breach impacted 1 million New Zealanders.



Enquiries to our Office