

3 May 2023

Hon Kiritapu Allan
Minister of Justice
Parliament Buildings
WELLINGTON

Dear Minister

QUARTERLY REPORT OF THE PRIVACY COMMISSIONER FOR THE PERIOD 1 JANUARY 2023 TO 31 MARCH 2023

Highlights

During this quarter we developed a new Statement of Intent and the Statement of Performance Expectations that reflects the 3-5 Year Strategic Plan that we began implementing late last year. Draft versions of the new documents will be consulted with you in April, in accordance with the Crown Entities Act 2004.

Recruitment has been a priority of our strategy this quarter. We have expanded our Pou Ārahi role to full time, a position that was previously shared with the Commerce Commission. We are also significantly expanding our Compliance and Enforcement team in light of the higher than expected rates of non-compliance with the Privacy Act 2020.

Internationally, the Australian Attorney-General's Department released its Privacy Act Review Report, which contained 116 proposals to strengthen the Australian privacy regime. While the Australian Government is yet to respond to this review, if the proposals are implemented they will significantly extend beyond the New Zealand Privacy Act (for example, establishing a right to erasure) and increase the pressure for future privacy law reform in New Zealand.

We have continued to support the Ministry of Justice on the development of a Privacy Amendment Bill to broaden the Privacy Act's notification requirements. We have also initiated our own internal workstreams to review specific areas where the Privacy Act may no longer be fit-for-purpose. We have provided you and your officials with our advice on possible future amendments to the Privacy Act that could be developed and will update you progressively as we explore these issues and the case for reform.

Planning is well underway for Privacy Week, which will be held on 8 to 14 May. The theme of Privacy Week this year is 'privacy rights in the digital age.'

Responding to developments in artificial intelligence

The past year has seen considerable public and media attention on generative artificial intelligence (AI), following the launch of OpenAI's ChatGPT app. ChatGPT has demonstrated the enormous potential of generative-AI, and stimulated a response from competitors to launch or accelerate development of their own AI systems (such as Google's Bard AI; Microsoft's AI-generated Bing search). These systems appear to be a dramatic improvement over the prior generation of AI systems, a trend that we expect will continue.

While the Privacy Act is technology-neutral, the types of AI systems that are emerging can supercharge some of the threats to privacy that we see today. AI can collect and analyse personal information to a much greater degree, and more swiftly, than current human-led processes. AI also increases problems relating to a lack of transparency about how public and private sector agencies are using personal information. AI can also be used to empower malicious actors to breach cybersecurity protections, rapidly and convincingly generate fake information (including images), and do not necessarily demonstrate how they comply with the laws and cultural expectations of New Zealand. In March the Privacy Commissioner publicly expressed his concerns about AI in an opinion piece for Stuff¹.

Our international counterparts are working to respond to AI, with the UK Government issuing a white paper² outlining key principles that should underpin AI regulation, including safety and security, transparency, fairness and accountability. The European Union is similarly pushing forward to develop a legal framework for AI³.

The Privacy Commissioner is writing to key public sector Chief Executives asking that they come together as a group of digital regulators to drive a collective response to these issues and avoid duplication of individual effort. There is precedent for this type of approach in Australia, where they have Digital Platform Regulators Forum. The Commissioner is seeking to supplement existing entities (such as the Digital Executive Board) so that digital regulators can directly address the potential harms of AI.

Privacy is not incompatible with the development of AI technologies, provided it is done in a manner that respects the important protections for individuals provided by the Privacy Act. A coordinated effort across public agencies will lead to AI being regulated in a safe and privacy-protective way, while also addressing the other interests and opportunities provided by AI technology.

¹ *AI and privacy concerns go hand-in-hand*, Privacy Commissioner at Stuff.co.nz

² *A pro-innovation approach to AI regulation*, Department for Science, Innovation and Technology, United Kingdom

³ *Regulatory framework proposal on artificial intelligence*, European Commission

Other activities of our Office

Policy and international related activities

In December 2022 the Privacy Commissioner announced that he intended to explore the option of issuing a Code of Practice under the Privacy Act for biometrics, including facial recognition technology. We have continued this work and are intending to undertake targeted consultation on proposals for a Code during the next quarter.

We have been providing significant support for Approved Information Sharing Agreements (AISA) made under the Privacy Act over the past several months. The Department of Internal Affairs-led AISA on sharing death information received its Order in Council on 20 March, and we have set the reporting requirements for this. We have also supported the Gang Harm Intelligence Centre on the Development of their Operational Procedures for information sharing under the Gang Intelligence Centre Agencies AISA, which came into force in early 2019.

During this reporting period we made the submissions to Parliamentary select committees on the:

- Therapeutic Products Bill, and the
- Inspector General of Defence Bill.

We also submitted to the Statistics New Zealand on their Long Term Insights Briefing.

No international meetings were held in this period, however preparations have begun for the upcoming Asia Pacific Privacy Authorities Forum that will be held in Mexico in June.

Compliance and enforcement

We continue to engage regularly with Police as it works towards implementing the recommendations from the compliance notice issued under the Privacy Act in December 2022. That notice required Police to cease the practice of collecting voluntary photographs and prints from youth, develop appropriate procedures and implement training relating to such photographing. Police are providing quarterly reports on progress in fulfilling the compliance notice.

In this quarter, we have seen the occurrence of New Zealand's largest privacy breach when Latitude Financial (operating in New Zealand as Gem Finance) was subject to a cyber hack that compromised the accounts of 7.9 million customers. As at 28 March 2023, Latitude had identified approximately 1.037 million New Zealanders (13% of the total) related to New Zealand driver licenses and approximately 36,000 passports had been compromised. Our Office has been in regular contact with Latitude Financial as the full impacts of the breach unfold. As Latitude Financial is based in Melbourne, we are also working with the Office of the Australian Information Commissioner.

The Latitude Financial breach reflects the trend of breaches caused by malicious activity. Cyber hacks such as that inflicted on Latitude Financial can generate a significant level of harm across several million people through a single breach event. Charts on the volume of privacy breach notifications and cause of serious privacy breaches are available in Appendix A of this report.

Investigations and dispute resolution

Following the Latitude Financial privacy breach, we have been contacted by many New Zealanders concerned about the lack of contact they received from Latitude and how long Latitude has been retaining their personal information. We are providing what guidance and assistance that we can.

We have received a privacy complaint from a lawyer on behalf of 148 individuals where there have been significant delays from a large government agency in providing the individuals with their personal information, in the context of the Abuse in Care Royal Commission of Inquiry.

During this quarter we have seen increased levels of unreasonable behaviour from individuals involved in privacy complaints. We are ensuring we have the right policies and procedures in place to keep our staff safe.

We will soon be shifting our 0800 number contact line to a new call centre provided by the Ministry of Business, Innovation and Employment's Service Centre. This shift is intended to improve the quality of the advice being provided to callers.

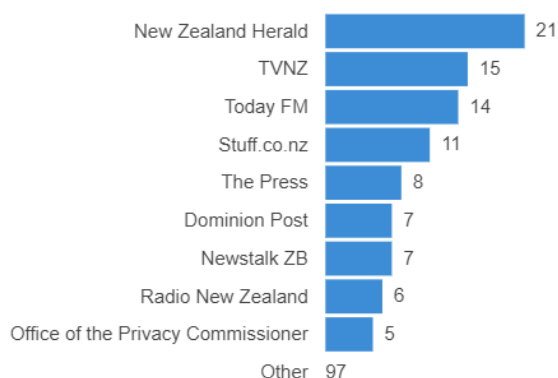
Communication and education

During this quarter we have made a concerted effort to increase our proactive media engagement on issues of privacy, to ensure we are consistently speaking on this topic. The nine media releases we made related to notable increases in data breaches, what a state of emergency means for privacy rules, comment on Twitter's end of free SMS two factor authentication, and tips for being privacy-savvy at Easter. In addition to our proactive work, we have been available to media for comment, information, and clarification about privacy topics and have spoken widely about privacy breaches, safety, and new technology.

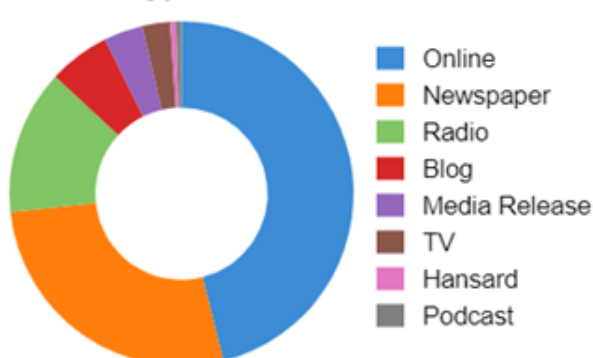
In March we began an agreement to supply regular content to Management Magazine, adding to our regular contributions to the New Zealand Doctor magazine.

In early February we switched media reporting tools, and the graphs below show the coverage we received from 1 February – 31 March 2023.

Sources



Content Types



Financial report

Financial information and performance against our Statements of Performance Expectations are appended to this report. The Office has continued to report a surplus in excess of its quarter 3 budget mainly as a result of various staff vacancies (like many agencies, we are facing high staff turnover, but are also actively working to fill vacancies), lower contract services' costs and reduced travel.

The Privacy Commissioner tabled his Annual Report for 2021/22 at the end of the quarter 3. The delay in tabling was due to a shortage of auditors to complete our audit within agreed timelines.

Yours sincerely

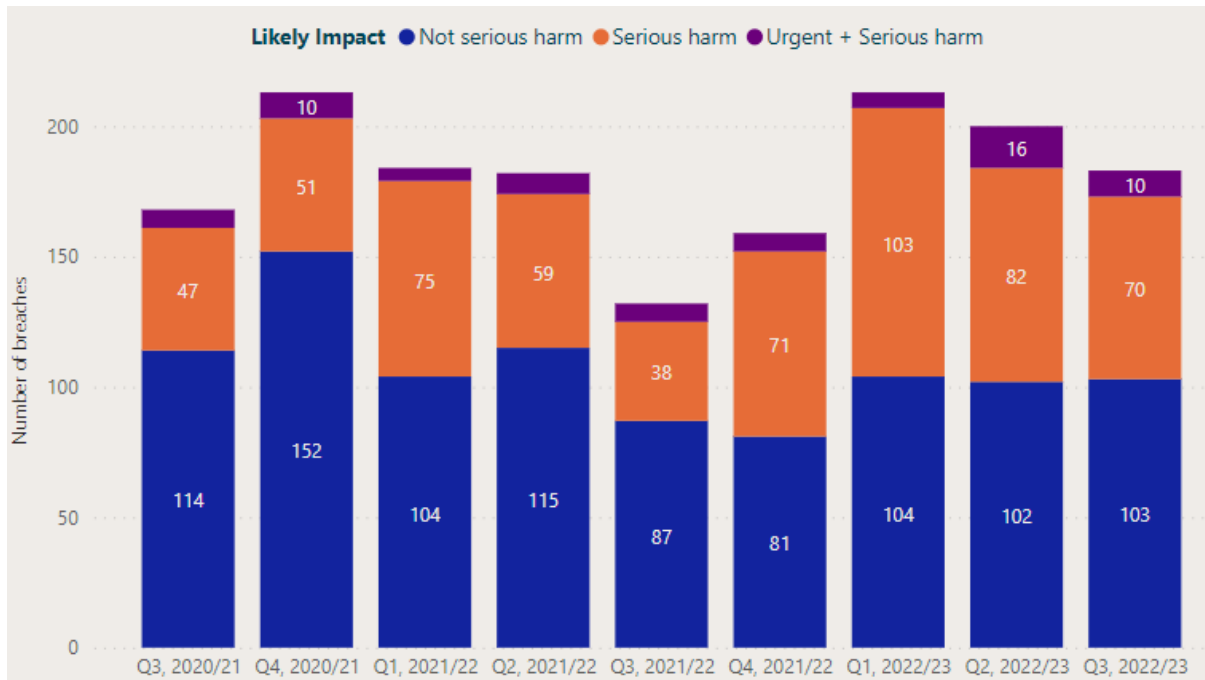


Michael Webster
Privacy Commissioner

Encl: Appendix A: Breach notification charts
 Appendix B: Q3 KPI Trend Report – March 2023
 Appendix C: Financials for period ending 31 March 2023
 Appendix D: Performance against Statement of Performance Expectations - Year to Date

Appendix A:

Volumes of privacy breach notifications



Primary cause of serious privacy breach notifications

