Briefing to the Incoming Minister of Justice
Office of the Privacy Commissioner

4 December 2023

Change is needed to address privacy harms and secure benefits

The Privacy Act 2020 protects the personal information of all New Zealanders, whether they are dealing with the public or private sector, filling in a paper form or chatting with an artificial intelligence (AI). The use of personal information is critical to Government policy initiatives, such as initiatives to strengthen policing or improving healthcare. Privacy also supports the digital economy, with the Privacy Act being the only statute that requires security safeguards to be in place.

Significant privacy breaches are occurring. Many agencies are not taking the steps necessary to safeguard personal information, contributing to the 79 percent increase in privacy complaints and 59 percent increase in serious privacy breaches that occurred between 2021/22 and 2022/23. These breaches are directly harming individuals (whether financially and/or emotionally), are costly to agencies, and are undermining trust in government and institutions. Our investigations into privacy breaches have shown that some agencies do not care about privacy as they know there are no significant financial penalties – contributing to serious cybersecurity risks.

The privacy harms we are observing can only be addressed through further modernising the Privacy Act and better resourcing the privacy regulator. The Privacy Act is based on policies agreed in 2013, and this past decade has witnessed the development and widespread adoption of significant new technologies such as biometrics and AI, and does not account for new risks to children's privacy. The Privacy Act is increasingly out of alignment with like-minded countries, who have been prioritising privacy reform.

Falling behind global privacy regulatory approaches could impact on New Zealand's technology sector and place in the global data economy. We currently benefit from European Union 'adequacy status', a formal recognition of our privacy protections that supports the low cost transfer of personal information and reduces regulatory barriers. Privacy experts have commented that if we do not keep up with global privacy standards there are risks to this formal recognition and potential perceptions that we may no longer be one of the safest places to process personal information.

We recommend a set of specific amendments to make the Privacy Act fit-for-purpose in the digital age. A civil penalty regime for major non-compliance should be introduced alongside new privacy rights for New Zealanders to better protect themselves. Stronger requirements for automated decision making and agencies demonstrating how they meet privacy requirements should also be established. Ensuring the Privacy Commissioner is resourced to effectively carry out all his statutory functions and proceeding with the above amendments is important, especially if the Government proceeds with the proposed Consumer Data Right.

As the Minister of Justice, you are responsible for the Privacy Act. You will see the Privacy Commissioner's comment on policy proposals being provided to Ministers and you will be the voice for privacy concerns arising at the Cabinet table. To assist you in your role, the Privacy Commissioner will take a 'no surprises' approach to briefing you, such as when a significant Privacy Commissioner comment has been inserted into a Cabinet paper.

The Privacy Act enables a flourishing economy and society

The Privacy Act enables New Zealanders to have trust in the companies and government services they use every day. It is a broad and flexible piece of legislation that safeguards the collection, use and disclosure of New Zealanders' personal information. The Privacy Act covers the public, private and not-for-profit sectors, and is technology neutral.

The Privacy Act supports three outcomes:

1. Agencies better achieve their own objectives through respecting privacy rights
   When personal information is protected, it builds trust and allows for innovation and effective and efficient delivery of services. Privacy breaches reduce the trust New Zealanders have in agencies and create significant direct costs, such as through loss of customers or clients, redress and stopping further breaches. Identity theft and cyber support agency, IDCare, estimates the average cyber security incident costs a small business about $40,000. Latitude Financial, whose March 2023 privacy breach affected millions of Australians and New Zealanders, has said that their privacy breach has so far cost them AU$76 million[1].
2. Individuals are more confident that their privacy is protected
   Good privacy practices reduce the harms caused by privacy breaches, whether emotional, reputational, financial, or physical. Specific harms that we have seen arise from privacy breaches include identity theft, having to move home, family violence, arson and suicide. Privacy complaints involving financial harm, such as through scams, are also increasing. About 5-10 percent of the nearly 800 privacy complaints we investigate a year result in a cash settlement averaging $10,000. Human Rights Review Tribunal findings that awarded damages for privacy cases have averaged $21,000[2] with the highest over $168,000.
3. The right to privacy and the protection of personal information is valued in New Zealand
   Privacy is a fundamental human right, aspects of which attract constitutional protection. Privacy enables people to have greater trust in government and institutions as they know that the information precious to them will be treated well. In this way, the Privacy Act contributes to the 82 percent of New Zealanders who, based on their personal experience, trust public services[3]. This trust is especially important for whānau, hapū and iwi in achieving their aspirations for equitable outcomes.

Privacy supports New Zealand's international trade agenda

Countries are increasingly expecting that the personal information of their citizens will only be sent to countries with the legislation in place to provide an equivalent level of privacy protection. Modern free trade agreements and other country level agreements have privacy specific chapters in place to support the digital economy.

As a specific example of how privacy supports New Zealand's international trade agenda, in 2012 New Zealand's privacy regime was granted 'adequacy status' from the European Commission (this is currently under review). This status means that our agencies do not need to put in place additional privacy safeguards (such as contractual clauses) when undertaking trade with the European Union – lowering compliance costs. Our adequacy status has also helped to facilitate cross border agreements to support policing, for example with Europol, the European Union Agency for Law Enforcement Cooperation.

---

[1] ACS Information Age, *Data breach cost Latitude $76 million*, 22 August 2023.
[2] Human Rights Review Tribunal Decisions, Ministry of Justice.
[3] Public Services Commission Kiwis Count Survey results, July 2023.

But the Privacy Act is in need of significant modernisation

The Act is losing alignment with like-minded countries

The policy approvals for the Privacy Act were agreed by Government in 2013, following a Law Commission review that made recommendations in 2011. The resulting Privacy Act reflected those recommendations without being updated. The past decade has seen international privacy legislation strengthen as like-minded countries respond to a rapidly changing environment.

Developments that have gone beyond our privacy legislation include:

- the European Union General Data Protection Regulation (GDPR) came into effect in 2018, pioneering a significant penalty regime, new privacy rights (such as a right to erasure) and new requirements (such as standards for automated decision-making)
- the United Kingdom passed the Data Protection Act 2018 to implement the GDPR
- the California Consumer Privacy Act came into effect in 2020
- Australia introduced a penalty regime for their privacy legislation in 2022
- the Australian Government has recently accepted and announced widespread reforms of their privacy legislation, which will align it much closer to the GDPR
- the Canadian Parliament is currently advancing significant privacy law reform.

The Act has not been amended in response to new technologies

Technologies such as biometrics, social media and the 'Internet of Things' are increasingly part of everyday life. Countries have been modernising their privacy regimes to capture the benefits and avoids the harms presented by new technologies. Ensuring that both individuals and agencies benefit from new technologies requires that they are implemented in a privacy protective manner.

AI is the newest challenge that needs to be met – and the Privacy Act is a core part of New Zealand's legislative framework for regulating it. We have already issued guidance to assist agencies with implementing AI under the Privacy Act, however more is required.

Many governments are actively addressing the opportunities and risks of AI through developing AI-specific strategies and legislative proposals. New approaches are developing, based on regulating AI at different levels, depending on what it is being used for.

It is increasingly clear our country needs to directly address the opportunities and risks of technologies, such as AI, through strengthening the Privacy Act. While the Privacy Act is technology neutral, it is missing key obligations, rights and powers that have been considered internationally to address new technologies.

New Zealand needs a coordinated and comprehensive response to AI

Seizing the potential and minimising the harms of AI will require a coordinated response from government. To support such a response to AI, the Privacy Commissioner is establishing a Digital Regulators Forum with key government agencies.

We recommend that the Government response to AI includes reviewing the existing regulatory framework (including the Privacy Act) that safeguards New Zealanders. This should be centrally coordinated to ensure that the wide range of interests in AI (including human rights) are considered.

The Act has limited protections for sensitive personal information, such as biometrics

Unlike many other countries, our Privacy Act does not establish a separate category of 'sensitive personal information' where privacy risks are particularly acute. One type of sensitive personal information is biometric information - information about an individual's biological or behavioural characteristics, such as their face or fingerprints.

Biometric technologies, such as facial recognition, are increasingly widespread and being adopted by the public and private sectors alike. There are a range of privacy risks with biometric technologies, including that individuals cannot change their biometrics easily and may be unaware that they are being collected.

We are using the tools we have under the Privacy Act to better protect the biometrics of New Zealanders. We have recently announced that we will developing an exposure draft of a biometrics Code of Practice under the Privacy Act. If such a Code is put in place, it would place tighter controls on how the Privacy Act applies to agencies using biometric technology to collect, analyse and use biometric information. However, the cross-cutting issues raised by biometrics are such that legislative amendments may also be necessary to safeguard this sensitive personal information.

The Act offers limited protection for risks to children's privacy

Privacy and fairness concerns about the collection of personal information are magnified when it comes to collecting information from children. These concerns arise from the greater cognitive, emotional, and physical vulnerabilities of children, and them being less able to understand the long-term implications of consenting to data collection or sharing.

Technological changes are seeing children and young people increasingly online and using social media. This has created new privacy risks, such as children and young people being exposed to online harms and their personal information being monetised. The education system has also been shifting to online platforms, spurred on by the COVID-19 pandemic.

The Privacy Act requires that agencies consider the fairness and intrusiveness of how they will collect personal information, particularly when it will be collected from children or young persons. This limited protection is being exceeded internationally, with countries beginning to create specific children and young people requirements:

- in 2020 the United Kingdom issued an Age Appropriate Design Code under their Data Protection Act
- in July 2024 California will be enacting an Age-Appropriate Design Code Act.

We have initiated a project to determine whether the current regulatory framework adequately supports children and young people's privacy rights in the current environment. We are currently seeking information from professionals who work with children (such as teachers and doctors), and non-governmental organisations who advocate for children and young people.

We will be working through any further engagement and policy recommendations in the new year, to support consideration of whether current privacy protection regulatory frameworks for children and young people remain fit-for-purpose, or whether new or expanded regulatory responses are required.

And we have insufficient funding to address regulatory failures

The frequency and impact of privacy breaches is increasing

We are notified of two types of privacy breaches:

1. Privacy complaints from individuals
   Where their privacy may have been interfered with. Complaints typically relate to an individual but can be caused by a systemic issue.
2. Privacy breach notifications from agencies
   When a breach occurs that could cause serious harm to an individual. These can affect many thousands of New Zealanders.

The volume of privacy harms being experienced is increasing, and therefore so is the pressure on our front-line services. In the 2022/23 financial year, the number of privacy complaints increased by 79 percent compared to the prior year. The volume of serious privacy breaches increased by 59 percent over the same period. Annex 2 contains data on key operational volumes, such as the number of privacy complaints and privacy breaches that are notified to us.

It is difficult to compare privacy breaches, as each breach is different in its cause and impact. For example, while the majority of privacy breaches affect a small number of individuals, a small number of breaches affect many thousands or millions of people. In addition, not all privacy breaches are being reported or complained about.

Recent high-profile privacy breaches provide a sense of the significant regulatory failure occurring:

- the 2021 ransomware attack on Waikato DHB severely disrupted service delivery and led to sensitive health information of thousands of people being sold on the dark web
- the 2023 Latitude Financial data breach has seen the records of over a million New Zealanders exposed, including driver licenses, passports and sensitive financial data. Our investigation into this breach is ongoing and we are working with our Australian counterpart, the Office of the Australian Information Commissioner.

We have also seen a growing number of small- to-medium sized organisations who do not understand or meet even the basic requirements of the Privacy Act, including a failure to appoint a privacy officer or establish policies and practices to effectively manage privacy impacts of their activities. While we respond effectively to address the privacy concerns these organisations create our current resourcing limits our ability to uplift privacy capability and understanding across the economy.

Agencies need to make privacy a core focus, similar to finance or health and safety

Our experience is that many agencies have low privacy capability and compliance, leading to privacy related harms. Very few agencies are meeting all of their privacy requirements under the Privacy Act, although some have robust processes for certain requirements (such as providing individuals with access to their own information).

A primary driver behind low privacy capability and compliance is the lack of accountability and consequences for managing personal information poorly. Many agencies that we investigate are aware of the lack of meaningful financial penalties and our relatively limited compliance powers in the Privacy Act and so are not incentivised to consider privacy in the same way they consider other requirements, such as complying with financial reporting standards or health and safety.

We have been committing our limited resources to best effect

To shift the focus of our Office to ensuring that privacy is a core focus for agencies, we have been:

1. Strengthening the Compliance and Enforcement function
   We aim to promptly use all of our compliance powers and have allocated additional resources to Compliance and Enforcement and are enhancing our policies and procedures.
2. Shifting the Policy and Advocacy function towards proactive work
   We are placing a greater emphasis on setting clear expectations for agencies, such as through our work on children's privacy, biometric technologies and AI.
3. Preparing for the re-development of our digital services platform
   We aim to empower New Zealanders to understand and use their privacy rights, and so are preparing to re-develop our digital services platform. Our current website is outdated and does not meet governmental digital accessibility standards.

However, our Office is small and is limited in what it can achieve

Our Office has 51 staff and is funded by an operating grant of $8.171 million from Vote Justice. When the Privacy Act commenced in 2020 we were provided with some additional funding in acknowledgement of the Office's new responsibilities under the Privacy Act, and then was provided with an additional amount in Budget 2023. These funding increases have been consistently below what is required to implement the significant new responsibilities and powers that the Privacy Act provided us, given the high level of privacy risk outlined in this briefing. This funding shortfall has led to us deferring work and will see us committing our cash reserves to critical areas that need addressing, such as replacing our website.

We have insufficient funding to effectively address the significant regulatory failure occurring across the public and private sectors under the Privacy Act. We do not believe we can fully deliver on our statutory responsibilities and meet the expectations of citizens and organisations with our current funding and powers. Additional funding will also be required if the Privacy Commissioner assumes additional responsibilities such as being a regulator of the proposed Consumer Data Right.

We would support a review of our funding model to ensure that we are placed on a sustainable footing into the future.

We are not resourced to investigate complex cyber attacks

While privacy breaches involving complex cyber attacks are increasingly common and concerning, we have not been provided with the resourcing necessary to forensically investigate them. Redacted under s206 Privacy Act 2020 [redacted]

We have been fortunate to leverage the resources of the Office of the Australian Information Commissioner in our joint investigation into the Latitude Financial breach, which affects millions of Australians and New Zealanders. Redacted under s206 Privacy Act 2020 [redacted]

An overview of the Privacy Act

The Privacy Act is enabling and broad

The Privacy Act is enabling legislation – through it, individuals can trust that agencies will collect, use and share their personal information in a responsible way.

The Privacy Act places obligations to protect personal information on almost all agencies operating in New Zealand – across the public, private and not-for-profit sectors. These protections extend to people of all ages, whether they are citizens or not, and regardless of their location.

For the private sector, the Privacy Act applies regardless of the size or sophistication of the business, whether it is a corner dairy or large listed company. For the public sector, the Privacy Act covers personal information about individuals in the hands of Ministers, government agencies, law enforcement, and the intelligence agencies. There are exceptions to the Privacy Act, including the courts in their judicial capacity, Parliament, and regulated news media (for news activities).

The Privacy Act only has limited sanctions in the form of criminal offence provisions with very low fines. For example, these provisions can be used following enforcement proceedings in the Human Rights Review Tribunal if an agency does not comply with a direction to improve its systems and processes.

The Information Privacy Principles – the heart of the Privacy Act

The 13 Information Privacy Principles (IPPs) establish the obligations and safeguards for collecting, using, and sharing personal information.

Key concepts within the IPPs include agencies being required to have a lawful purpose to collect personal information, to store the information with security safeguards and only as long as necessary, and use and disclose the information for the purpose it was collected (with exceptions, outlined below).

Individuals are provided with protections relating to fairness and transparency, and rights to access and correct personal information held by agencies.

The IPPs are technology neutral and flexible enough to apply to a range of different contexts and to new technologies. In this way, the IPPs and the Privacy Act supports the lives of New Zealanders and every part of our society. Likewise, they support the economy, including the digital economy.

The Privacy Commissioner issues Codes of Practice to modify the IPPs, primarily setting sector specific requirements such as for health information and credit reporting. Codes can also apply in specific situations, for example the Civil Defence National Emergencies (Information Sharing) Code allowed greater information collection, use and disclosure in areas affected by Cyclone Gabrielle.

Law enforcement, public health and research are woven through the Privacy Act

Public interest is integrated in the Privacy Act through exceptions to the IPPs, including through enabling the use and disclosure of information for public health and safety, the safety of an individual, research purposes, law enforcement and the security intelligence services.

To illustrate, the public health and safety exception was important during the COVID-19 response where the risks to public health sometimes justified the collection and sharing of health information (such as vaccination status) that would not have been appropriate outside of pandemic conditions.

The Privacy Act enables a wide range of public sector information sharing

The Privacy Act has several mechanisms that allow for information sharing across government. New mechanisms have been added in the 30 years since the original Privacy Act 1993 and now enable a large range of public sector information sharing. These mechanisms include:

- **Approved Information Sharing Agreements (AISAs):** introduced in 2011, these enable personal information to be shared between (or within) agencies for the purpose of delivering public services. These agreements are created by regulations through Order in Council and in consultation with the Privacy Commissioner.
- **Information Matching Agreements:** are a legacy information sharing tool that has been replaced by AISAs and required legislation to be passed by Parliament.
- **Identity information:** enables the sharing and verification of identity information between core public services such as policing, health, immigration, corrections, and at the border.
- **Law enforcement information:** enables sharing between the Courts, Police, Corrections and Ministry of Justice and also motor vehicle register information.

In addition to these information sharing mechanisms, dozens of statutes override specific aspects of the Privacy Act to explicitly provide for information collection, use and sharing in specific contexts.

The Treaty of Waitangi / Te Tiriti o Waitangi is directly relevant to privacy

The Privacy Act requires the Privacy Commissioner to take into account 'cultural perspectives on privacy' in the exercise of their functions. Recognising the Treaty of Waitangi / Te Tiriti o Waitangi as a founding constitutional document and its place in New Zealand statute and case law, one of our key objectives is to work in partnership with Māori to take a Te Ao Māori perspective on privacy. For example, we have engaged with tikanga and Māori data experts for our work related to the regulation of biometric technology.

Improving public sector information sharing is now about capability building

Our experience is that enabling legislation is no longer the primary difficulty stopping public sector agencies from sharing information. For example, the November 2022 inquiry into the death of five year old Malachi Subecz from physical abuse found that enabling provisions existed, but recommended an "enhancement of understanding of the information sharing regime in the Oranga Tamariki Act 1989".

Another example is that of AISAs – the Privacy Act tool for enabling sharing for public services. To date, 14 AISAs have been established and our observation is that the largest difficulty with their effective use is with the internal capabilities of the public sector agencies. For example, the Gang Intelligence Centre AISA provides for very wide-ranging information sharing about persons related to gangs, but after six years it is still not being fully utilised.

Greater emphasis should be placed upon the ability of operational staff to understand and use the wide-ranging information sharing mechanisms available, rather than establishing new enabling legislation that could jeopardise public trust and social license. To this end, we have begun working with the Government Chief Privacy Officer to on ways to build the public sector's information sharing capability.

How we work to improve privacy outcomes

Our purpose and functions are clear

Our purpose is to ensure that privacy is a core focus for agencies, similar to health and safety or good financial reporting. Achieving success will see us protecting the privacy of individuals, enabling agencies to achieve their own objectives and safeguarding a free and democratic society.

Our five functions undertake a range of activities to achieve this purpose:

1. Communication and Education
   Informing people about their privacy rights and promoting agency privacy understanding. This is achieved through the media and by producing material and resources.
2. Investigations and Dispute Resolution
   Investigating privacy complaints for settlement where possible. Referring serious cases to the Director of Human Rights Proceedings to bring to the Human Rights Review Tribunal.
3. Compliance and Enforcement
   Undertaking proactive or reactive compliance work, ranging from providing guidance to issuing compliance notices. Reviewing breach notifications and other information sources.
4. Policy and Advocacy
   Providing advice on the privacy implications of policy proposals and draft legislation, including briefing Ministers if necessary. Setting clear regulatory expectations through guidance and Codes of Practice.
5. Strategy and Insights
   Analysing the enquiries, complaints and privacy breach information we receive. Understanding the impact of technological developments on privacy.

How we will work with you as the Minister of Justice

As Minister of Justice you are responsible for the Privacy Act and are the voice for privacy concerns that may arise at the Cabinet table. The Cabinet Manual requires that the Privacy Commissioner be consulted on draft legislation that will have a privacy impact, and he can also inquire into privacy matters generally and proactively advise Ministers or the Prime Minister.

As an independent Crown entity, the Privacy Commissioner can disagree with policy proposals being provided to Ministers, and comment on Cabinet papers. The Privacy Commissioner will also make written and oral submissions to Select Committees on Bills being considered.

Our approach to assessing policy proposals is practical, focusing on necessity and proportionality. For example, we provided extensive support to health agencies to mitigate the privacy impacts of COVID-19 responses, leading to better designed legislation and initiatives.

We can also assist with managing the consequential impacts of policy changes, such as repealing existing legislation. For example, if the Fair Pay Agreements Act 2022 is repealed we can provide advice on how what should happen with personal information that unions have collected under that Act.

Generally, we consider that carve-outs from the Privacy Act should be limited. Often information can already be shared between agencies without the need for bespoke and inflexible legislation that can weaken the protections afforded by the Privacy Act.

The Privacy Commissioner will be commenting on a range of proposals and at times meet with your ministerial colleagues. We will take a 'no surprises' approach to briefing you, including when making a significant or adverse Privacy Commissioner comment in a Cabinet paper.

The specific reforms the Privacy Act needs

Empowering New Zealanders to better protect themselves

The Privacy Act provides individual New Zealanders with important rights – such as rights to request and correct the personal information an agency holds about them. It also requires that agencies only hold personal information for as long as they require it for their lawful purposes.

With the increasing digitisation of modern economies, many of our international partners have established new rights for their citizens, such as a 'right to erasure'. Rights to erasure provide individuals with the power to ask agencies to delete their personal information and sets out when agencies must do so. The European Union first introduced this important right in 2018, California in 2020 and the Australian Government has just agreed in-principle to establish a right to erasure.

The benefits from implementing a right to erasure are significant. For example, this year the Latitude Financial privacy breach affected over one million New Zealanders, even though many had reportedly not interacted with Latitude for years. A right to erasure could have reduced the harm of this breach as individuals could have been ensuring that Latitude was only holding the personal information as long as it actually needed. Under the current settings, it is up to agencies such as Latitude to proactively review their data retention practices and delete data they no longer need.

Providing individuals with a right to erasure will empower them to resolve issues with agencies directly. We can then provide guidance and act on complaints and compliance issues that arise.

Agencies need strong incentives to take privacy seriously

The maximum penalty under the Privacy Act is a fine not exceeding $10,000, and this can only occur in limited circumstances. For example, it is an offence for failing to notify the Privacy Commissioner of a privacy breach that may have caused serious harm – but it is not an offence to have caused that privacy breach itself, whether through negligence or deliberate means.

Our investigations into privacy breaches have revealed that some agencies do not care about privacy as they know there are no significant financial penalties. For example, the Office is currently engaging with one multi-national agency that is not complying with a statutory information request to inform our investigation. A criminal fine not exceeding $10,000 is not always providing sufficient incentives for the agency to comply with our statutory demand or the requirements of the Privacy Act. The incentives for compliance with privacy regulations are further reduced as this agency has been fined several hundred thousand dollars under a different regulatory regime.

In contrast, other countries are steadily introducing very high financial penalty regimes, reflecting the digital age we live in. For example, in 2022 Australia strengthened their civil penalty regime so that a serious or repeated interference with privacy has a maximum penalty of a $50,000,000 (AUD) or three times the value of the benefit obtained directly or indirectly.

Strengthening privacy supports the proposed Consumer Data Right

We have worked closely with the Ministry of Business, Innovation and Employment on designing a Consumer Data Right that will provide individuals and businesses with greater choice and control over their data (similar to Australia).

While we support the Privacy Commissioner regulating privacy matters under this new right, the Privacy Act provides us with few powers and penalties to implement our responsibilities and we have not yet been resourced to undertake this new remit.

Agencies should be able to demonstrate how they meet their privacy requirements

Our experience has shown that many agencies have not considered how they will safely manage personal information. While the Privacy Act has requirements that the agency must meet (such as maintaining appropriate security safeguards), there is no requirement for anything to be documented. This creates difficult situations for us where non-compliant agencies have no policies, procedures or privacy documentation at all.

Many countries and international privacy frameworks have an 'accountability principle' that requires agencies to be able to demonstrate the purposes for which they are collecting personal information and how they will safely manage the information. For example, the OECD guidelines (that the Privacy Act gives effect to) governing the protection of privacy[4] state that agencies should have in place privacy management programmes tailored to their size.

To help address difficulties in this area, we will be providing comprehensive guidance to agencies on how to build a privacy-protective culture. Redacted under s206 Privacy Act 2020

New Zealanders need stronger protections for automated decision-making

Automated decision-making tools rely on algorithms or AI to assess information and help improve services and productivity by automating manual decision-making processes. The Privacy Act does not expressly address the privacy risks created by automated decision-making tools.

Significant privacy risks arise from automated decision-making, with problems such as inaccurate predictions, discrimination, unexplainable decisions, and a lack of accountability. Failures in such tools are usually not evenly distributed, perpetuating or exacerbating poor outcomes for disadvantaged communities. An example of how automated decision-making can go wrong is the Australian 'Robodebt' scheme, an automated debt assessment and recovery system that incorrectly issued over 440,000 debts to those receiving government support payments, resulting in a Royal Commission of Inquiry.

Our trading partners have been introducing greater protections for automated decision-making. The European Union regulates automated decision-making and profiling by imposing certain restrictions and creating rights to challenge certain processes or require them to be justified to the individuals concerned. The Australian Government has just accepted that individuals should have a right to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made.

New measures need to be included in the Privacy Act to manage the risks of automated decision-making to ensure that New Zealanders are treated fairly and equitably.

[4] Organization for Economic Cooperation and Development, 2013. *The OECD Privacy Framework*.

The Privacy Amendment Bill (Ministry of Justice lead)

We have been working closely with the Ministry of Justice on a specific Privacy Amendment Bill to broaden the notification requirements in the Privacy Act. The Bill will mean that individuals would be notified when an agency collects their personal information indirectly through a third party (with exceptions). This change will help individuals understand how their personal information is being collected and used and enable them to exercise their rights to access and correct their personal information.

This Bill will address an issue relating to the equivalence of New Zealand's privacy framework with that of the European Union. New Zealand is one of a small number of countries that have European equivalency status and maintaining this is important to the seamless flow of information between our jurisdictions. The Ministry of Justice and Ministry of Foreign Affairs and Trade have been working to ensure the continuation of New Zealand's adequacy status. This has been the subject of review over five years and is now close to completion. Successful confirmation of New Zealand's adequacy status is contingent on the timely progress of the Privacy Amendment Bill.

The Amendment Bill was introduced in the House on 6 September 2023. We support the re-introduction of this Bill into Parliament and will be making a submission to select committee in support of it. This Bill is a necessary improvement to the Privacy Act framework, although further modernisation of the Privacy Act is required. There may be an opportunity for the Government to consider some of these wider reforms as part of the current Amendment Bill process.

We look forward to discussing our work with you

We would welcome the opportunity to meet with you to discuss our work and how privacy intersects with your other portfolios.

Please note that the contents of this briefing will need to be reviewed by the Office of the Privacy Commissioner before any proactive or reactive release.

Annex 1: Michael Webster, Privacy Commissioner

Michael Webster took up the role of Privacy Commissioner on 5 July 2022.

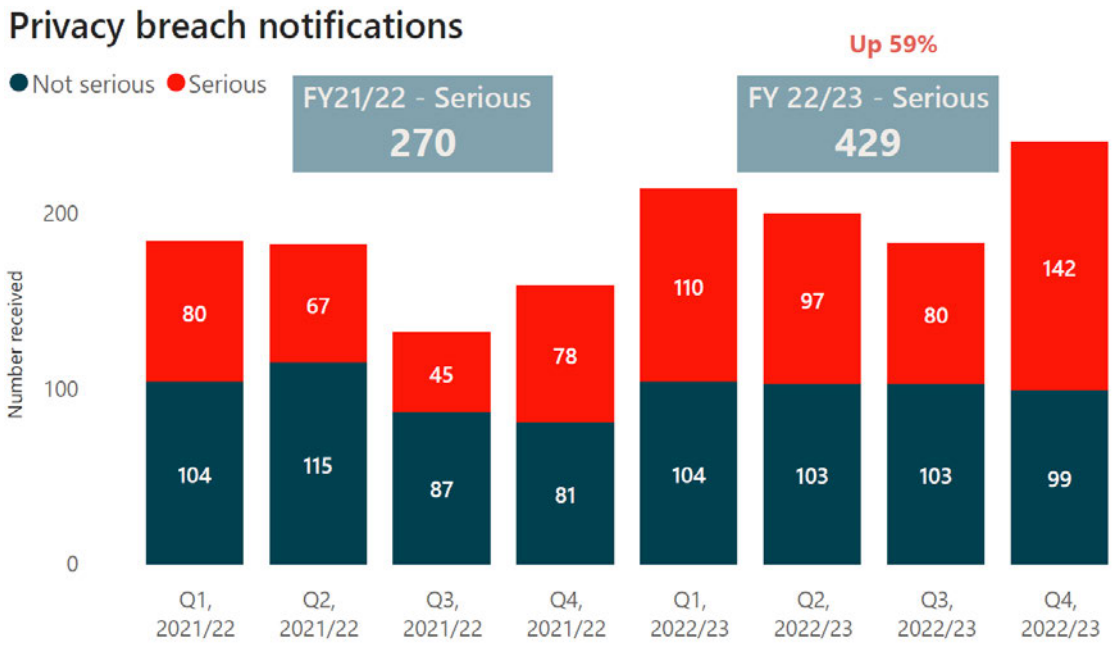
Prior to Michael's appointment he worked in the Cabinet Office, Department of the Prime Minister and Cabinet for 14 years from July 2008 and held the position of Secretary of the Cabinet and Clerk of the Executive Council from March 2014.

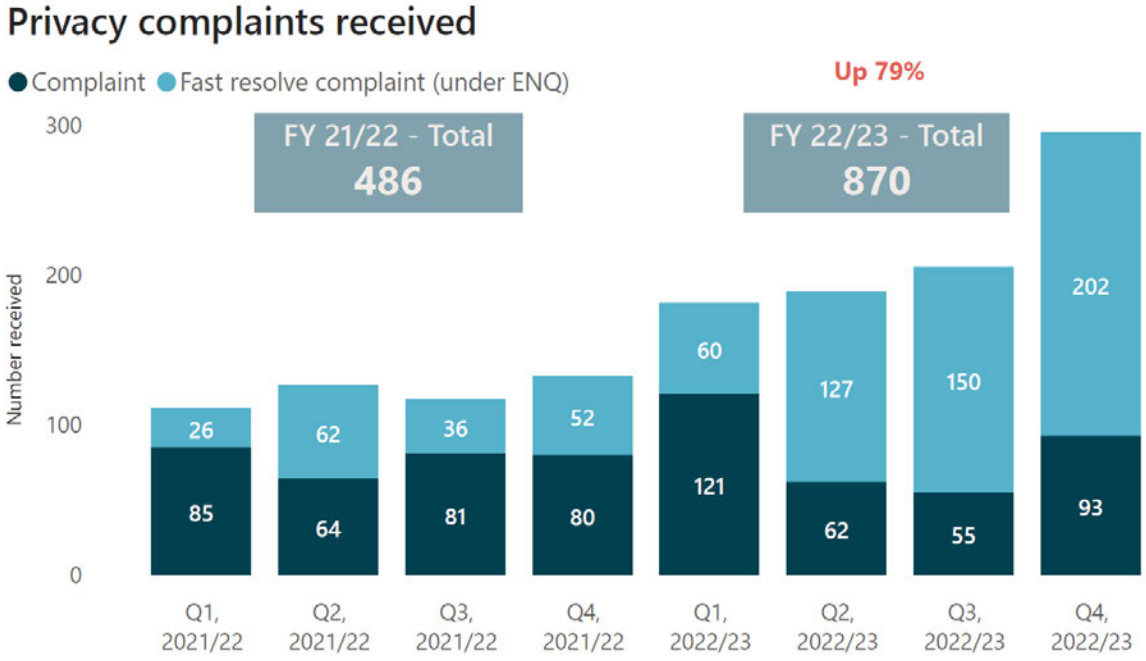
He has a long history of public service, with expertise in policy development, corporate strategy and planning and risk management. His career has to date focused on enabling and driving good governance, the promotion of democratic rights and values, the development and application of codes of conduct and behaviour and working to ensure compliance with both statutory provisions and constitutional conventions.

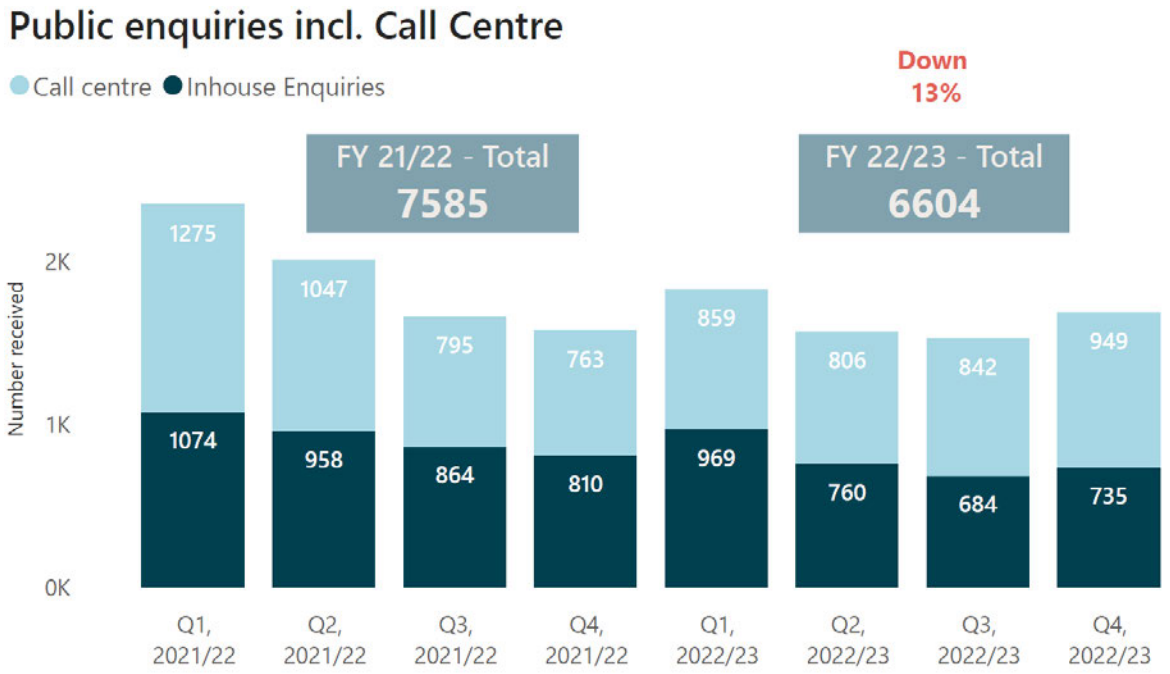
Michael holds a Master of Public Management and BA (Hons) from Victoria University of Wellington and is a graduate of the EY/Darden School of Business Programme, and the Executive Fellows Programme of the Australia and New Zealand School of Government.

Annex 2: Key privacy system information

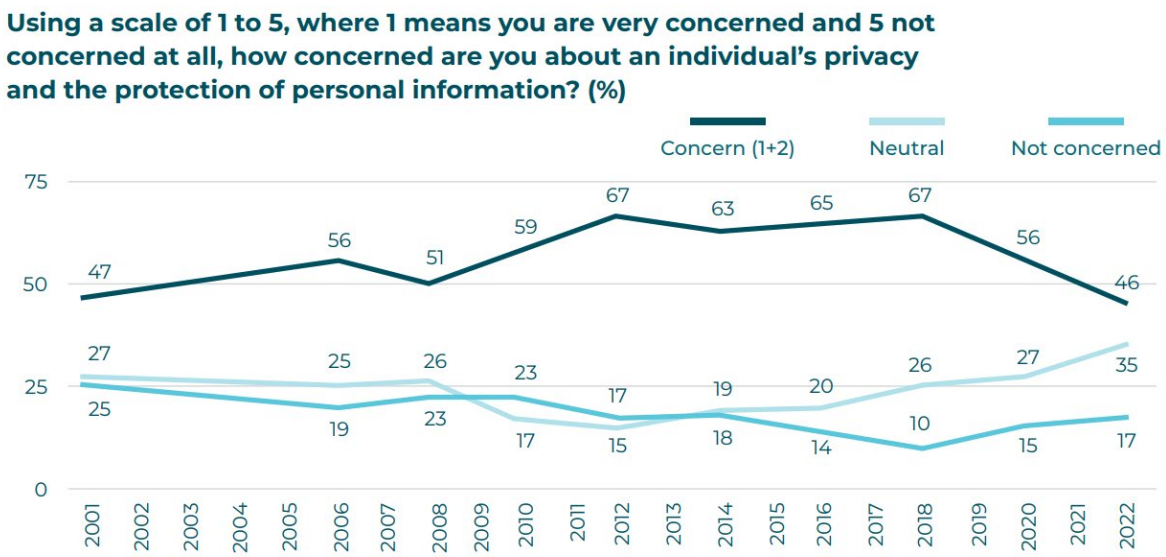
Operational volumes





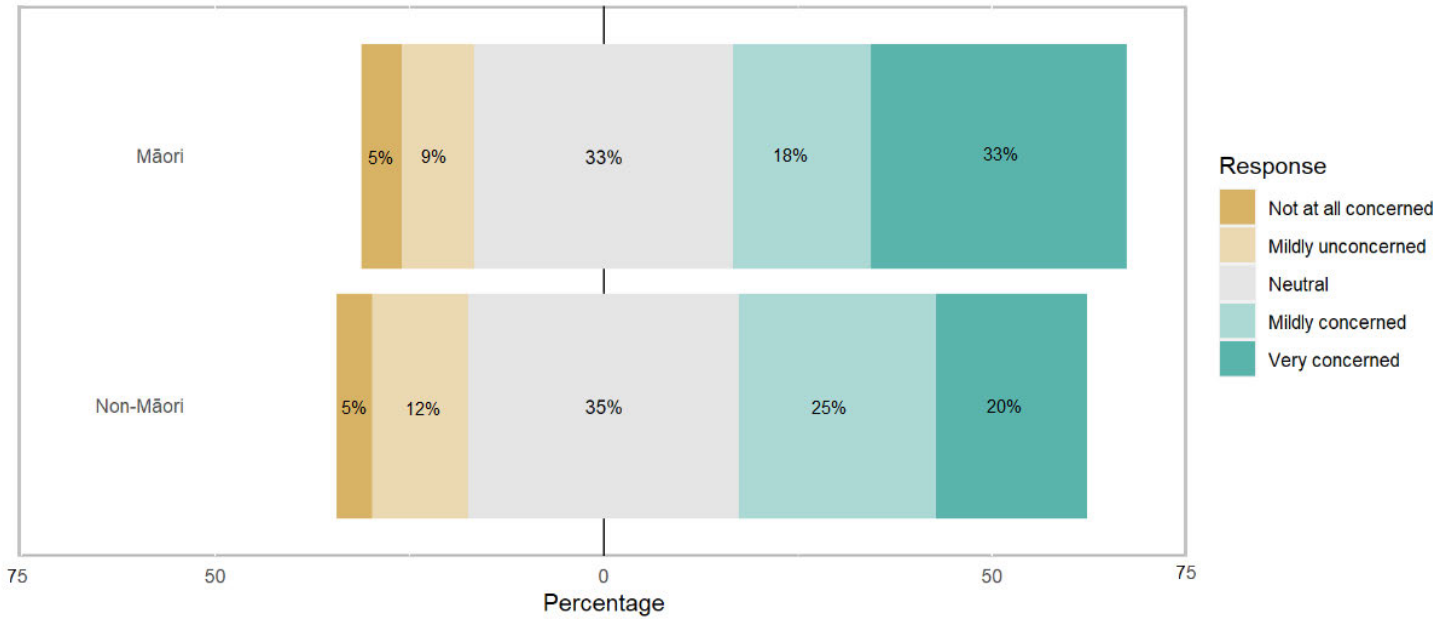


Surveyed public concern about privacy[5]



[5] *Privacy concerns and sharing data*, Omnibus research commissioned by the Privacy Commissioner. AK Research & Consulting, March 2022.

Concern about an individual's privacy and protection of personal information by ethnicity



Awareness that the Privacy Act provides individuals with a right to access their personal information that an agency holds about them