

Briefing for the Incoming Minister of Justice

Office of the Privacy Commissioner

6 November 2020

Executive summary

- A new Privacy Act comes into force on 1 December 2020. It creates some new obligations and gives the Privacy Commissioner new compliance powers.
- The Office of the Privacy Commissioner (OPC) has launched a major campaign, 'Privacy is Precious', to raise awareness of the new Act and of good privacy practice.
- Developments affecting privacy are taking place so rapidly that ongoing review and reform of the Privacy Act is needed. The Privacy Commissioner has identified further desirable privacy law reforms, including the introduction of a consumer data right.
- Some current and emerging privacy issues that OPC is focusing on are:
 - providing advice on contact tracing and other sharing of personal information as part of the response to the Covid-19 pandemic
 - developing guidance on disclosure of personal information from government departments to Ministers
 - ensuring agencies comply with the Privacy Act's requirement to give individuals access to their own personal information
 - promoting consideration of privacy impacts and mitigations in projects that use emerging technologies such as facial recognition
 - engaging with Māori and other communities to better understand diverse cultural perspectives on privacy
 - contributing to the European Union's review of its recognition of New Zealand as a country that adequately protects privacy.
- The Privacy Commissioner would welcome the opportunity to meet with you in the near future.

Who we are

OPC is New Zealand's privacy regulator. The Privacy Commissioner is established by the Privacy Act. Working through his Office, the Privacy Commissioner takes action to support, encourage and incentivise compliance with the Privacy Act for the protection of personal information by government, business and civil society. The Privacy Commissioner is an independent Crown entity and a corporation sole. Further information about OPC is provided in **Appendix 1** (headline information) and **Appendix 3** (an excerpt from our 2020 Annual report which is in the final stages of being readied for publication).

The Privacy Act applies to agencies in the private and public sectors. It includes exceptions and mechanisms to reflect the wide variety of contexts in which it operates. On 1 December 2020, the Privacy Act 2020 will replace the Privacy Act 1993. Like the previous Privacy Act, the Privacy Act 2020 was passed unanimously. Privacy legislation has received cross-party support over successive governments. Unless the context indicates otherwise, references to the Privacy Act and the Commissioner's powers under the Act in this Briefing relate to the Privacy Act 2020.

OPC's role includes:

- building understanding of privacy through education and advocacy
- monitoring and enforcing compliance with the Privacy Act
- investigating complaints about breaches of privacy
- examining proposed legislation and policy proposals for impacts on privacy
- overseeing authorised government data matching programmes and monitoring authorised information sharing agreements
- advising on the risks and benefits of new technologies or initiatives
- developing codes of practice for particular sectors or activities
- receiving reports of notifiable privacy breaches.

The Privacy Commissioner can, among other functions and powers:

- make public statements about matters affecting privacy
- inquire into any matter if it appears to the Commissioner that privacy is being or may be infringed
- report to the Minister of Justice and the Prime Minister
- publish reports on the Commissioner's investigations
- issue codes of privacy practice
- direct an agency to provide a person with access to that individual's information
- issue compliance notices requiring agencies to take steps to remedy a breach of the Privacy Act.

An important part of OPC's role is investigating and seeking to resolve complaints of interference with individuals' rights under the Privacy Act. Complaints that OPC is unable to resolve can be taken to the Human Rights Review Tribunal either by the aggrieved individual or by the Director of Human Rights Proceedings. The Tribunal can grant remedies if there has been an interference with the privacy of an individual.

Other agencies with roles in privacy protection are listed in **Appendix 2**. OPC works with these and other agencies on issues of common interest, and the Privacy Commissioner consults with other regulators as appropriate. The Commissioner can

transfer a complaint to another body (including an overseas privacy regulator) if the complaint relates more closely to that body's jurisdiction.

Media, in relation to their news activities, are not covered by the Privacy Act but have their own regulatory frameworks requiring them to comply with privacy standards.

Minister of Justice's role under the Privacy Act

You have portfolio responsibility for the Privacy Act and the Ministry of Justice administers the Act. The Minister of Justice is defined as the responsible Minister in the Act and has a number of roles and functions under the Act.

As the responsible Minister, you may need to:

- consider and respond to advice, reports or submissions from the Privacy Commissioner
- recommend that regulations be made prescribing countries whose laws provide comparable safeguards to those in the Privacy Act, or binding schemes that provide comparable safeguards, for the purpose of restrictions in the Privacy Act on cross-border disclosures of personal information
- recommend the making of other regulations necessary for the administration of the Privacy Act
- recommend amendments by Order in Council to Schedules 3 and 4 of the Privacy Act, which deal with access to identity and law enforcement information.

You can, and in some cases must, consult the Privacy Commissioner before exercising these functions.

In addition, you may recommend the approval by Order in Council of authorised information sharing agreements for which the Ministry of Justice is the lead agency. Other Ministers will be responsible for recommending approval of information sharing agreements in their portfolio areas.

Why privacy matters

Legislative protection of informational privacy:

- supports individual autonomy and self-determination by guarding against unreasonable intrusions into personal affairs and facilitating people's access to and control of their own data
- enables trust in institutions by ensuring that, as much as possible, people know who has their information and what it will be used for
- promotes fairness by requiring that people's access to services is assessed on the basis of information that is accurate and relevant.

Personal information is more valuable than ever before. Exchanges of personal information are central to everyday transactions and such information is vulnerable to misuse if appropriate care is not taken. Trust in the agencies that handle personal

information is critical to individual, whānau, community and societal wellbeing, and underpins our democratic institutions.

Privacy is a dynamic and multi-faceted issue. It is affected by wider social, cultural, technological, environmental and economic trends, both within New Zealand and internationally. These trends include the following:

- Technology continues to develop rapidly. Technological tools with major implications for privacy – such as biometrics, artificial intelligence, facial recognition and the Internet of Things – are increasingly part of everyday life. Personal information is being collected, distributed, stored and used on an unprecedented scale.
- As technology makes ever-growing volumes of personal information available, government and business are increasingly data-driven. The public and private sectors can analyse, combine and reuse personal information in ways that can have significant impacts on people's rights and interests.
- Privacy issues are increasingly international, due to globalisation and the ease with which personal information can be transferred across national borders.
- Māori are calling for greater control over data relating to them. The concept of Māori data sovereignty provides a useful focus for thinking about how Māori worldviews and aspirations can become part of privacy protection.

Privacy 2.0

A new Privacy Act and additional funding for OPC in Budget 2020 have made possible organisational changes and new areas of focus that OPC refers to as Privacy 2.0. OPC's work has previously been largely demand-driven, but the office now has the capacity to take a more strategic approach to privacy regulation, including through identification of systemic issues and priority areas for action (such as particular sectors or technologies).

As part of Privacy 2.0, OPC will also have an increased focus on:

- strengthening OPC's compliance and enforcement capability and becoming more proactive about compliance activities (while still responding to individual enquiries and complaints)
- increasing OPC's effectiveness through improved data analytics and performance monitoring
- building OPC's capability to engage with Māori and in Te Ao Māori, and working in partnership with Māori to apply a Māori cultural lens to privacy issues.

Privacy Act 2020

Key changes in the Privacy Act 2020 include:

- notification of significant privacy breaches to affected individuals and OPC will be mandatory

- the Privacy Commissioner will be able to issue notices to businesses or organisations, requiring them to do something, or stop doing something, in order to comply with the Privacy Act
- the Commissioner will be able to direct agencies to give individuals access to their personal information, allowing faster resolution of access complaints
- a new privacy principle places controls on sending personal information overseas, so that in most cases information sent overseas will be subject to comparable safeguards to those under the Privacy Act
- the application of the Act to overseas agencies that carry on business in New Zealand is expressly addressed.

These and other changes will strengthen OPC's ability to work with agencies to ensure they protect New Zealanders' personal information.

Additional baseline funding for the Office of the Privacy Commissioner

The Privacy Commissioner's baseline funding has been increased in recent years to recognise OPC's heavier workload and the need for an increased input by the Privacy Commissioner into a range of government initiatives. Additional funding has also been provided for the transition to the new Privacy Act. Total additional annual funding of \$2.306m has been provided from 2020/21 onwards, taking the new annual baseline to \$7.276m.

Progress on implementing the new Privacy Act

OPC's work on implementation of the Privacy Act 2020 has been guided by a focus on ease of compliance for regulated agencies. OPC has invested in the development of tools that will assist agencies to comply with new requirements in the Act, and thereby reduce costs for agencies. Two key products are:

- NotifyUs, an online tool which agencies can use to work out if they are required to notify OPC of a privacy breach, and to report such breaches
- model contractual clauses that agencies can use to comply with new restrictions on the transfer of personal information overseas.

Other implementation work has included:

- working with the Ministry of Justice on Privacy Regulations under the new Act specifying details of various matters, such as the procedure for giving public notice of a privacy breach
- updating and reissuing six codes of practice made under the Act to make the codes consistent with changes to the Act (these have been provided to your office for tabling in the House)
- issuing guidance about matters introduced by the new Act (such as controls on cross-border transfers of personal information) and updating existing guidance

- developing resources to inform the public about changes to the Act, including free e-learning modules, podcasts and videos.

OPC launched a national awareness-raising campaign, 'Privacy is Precious', during Privacy Week (2-6 November 2020). The campaign, including a 30-second commercial, is intended to reach audiences and communities that may be less aware of the Privacy Act, and may have unmet privacy needs. It is aimed at educating people about good privacy practice and about the new Privacy Act. Our 2020 UMR privacy awareness research showed that declared awareness of the Privacy Act has remained high at around 85% of the general population. However, it also showed that awareness levels differ across demographics with 57% of 18-29 year olds, 69% of Māori and 63% of Pasifika indicating an awareness of the Privacy Act. These groups will be a focus for OPC effort as they also tend to be lower users of our complaints and dispute resolution services and may therefore have unmet privacy needs.

Current and emerging issues

Covid-19 information sharing

OPC has been heavily engaged in work on Covid-19 information sharing. OPC has provided advice and guidance to agencies in the public and private sectors on issues such as contact tracing apps, testing, employment and the application of Privacy Act exceptions relating to serious threats to public safety. OPC has:

- provided guidance for hospitality businesses and event organisers, employers and employees, landlords and tenants and healthcare professionals
- commented on the operation of the Civil Defence National Emergency (Information Sharing) Code after a state of national emergency was declared
- completed a Privacy Commissioner's Inquiry into the Ministry of Health's use and disclosure of Covid-19 patient information
- been highly engaged with the Ministry of Health's work on the Covid Tracer App and with ongoing work on the use of digital technologies as contact tracing tools
- been involved in work with data protection authorities globally through the Global Privacy Assembly's Covid-19 Taskforce
- submitted to the Finance and Expenditure Subcommittee's Inquiry into the operation of the Public Health Response Act 2020.

OPC understands that work is ongoing in Government to consider whether there are legislative gaps that require additional information sharing authorities. The Privacy Commissioner considers that there is already flexibility in the Privacy Act to allow for information sharing where it is demonstrably necessary for the pandemic response. The Act provides for disclosure of personal information to deal with serious threats to public health or safety. Any legislative amendment to enable large-scale sharing of personal information between government departments should be carefully considered prior to implementation to avoid the potential of Government overreach, which may hinder the public's trust in the Government's response to Covid-19.

Disclosure of personal information to and by Ministers

Ministers are agencies subject to the Privacy Act in their own right, separate from their portfolio departments. OPC is working with the Crown Law Office and other key agencies on guidance about the sharing of personal information from departments to Ministers and the onward disclosure of such information by Ministers. This guidance will be published on OPC's website and provided to departmental chief executives and Ministers' offices. It is designed to assist in decision-making about when personal information can lawfully be disclosed in the context of the relationship between departments and their responsible Ministers. The Privacy Commissioner will be involved in the induction briefing for new Ministers and will cover the content of the guidance at that briefing.

Access requests

The bulk of complaints investigated by OPC concern alleged breaches of individuals' rights to access personal information about themselves. There are significant problems in the handling of access requests by some agencies, including government departments. These problems include poor response times and misuse of grounds for withholding relevant personal information. Failure to provide people with their own information in a timely manner reduces trust in agencies. Such failure can also adversely affect individuals, who may wish to use the information held about them to assert their rights and to be assessed on the basis of accurate information. Access requests will be an area of focus for OPC's compliance work, making use of new powers to issue access directions and compliance notices.

Technological challenges

Some of the most significant privacy challenges relate to technological developments such as artificial intelligence and machine learning, facial recognition, camera-equipped drones, deepfakes and synthetic media. OPC works with agencies in the public and private sectors to ensure that privacy impacts and mitigations are considered in projects that use emerging technologies. OPC promotes privacy by design: building privacy into systems and projects from the design stage onwards. For example, OPC is engaging with the Police about its use of emerging technologies.

Cultural perspectives on privacy

How people understand privacy is influenced by their culture and lived experience. The Privacy Act 2020 includes a new requirement for the Privacy Commissioner to consider cultural perspectives on privacy in exercising the Commissioner's functions. OPC will engage with others to better understand what privacy means to New Zealand's diverse cultural communities and the implications for OPC's work. In particular, OPC has a responsibility to engage with Māori as Treaty partners to understand privacy from the perspective of Te Ao Māori. OPC has been contributing to work on Māori data governance, led from the Crown side by Statistics New Zealand.

Review of European Union adequacy status for New Zealand privacy law

To facilitate the flow of information that is integral to international communications and trade, New Zealand privacy law needs to remain broadly in line with that of our trading partners. A key advantage that New Zealand currently enjoys is that our privacy law was recognised as ‘adequate’ by the European Commission in 2012. This recognition allows for the free flow of personal data from EU countries to New Zealand without the need for additional compliance measures. Only twelve jurisdictions currently have adequacy status, which is difficult to obtain.

New Zealand’s adequacy status is currently under review, following the replacement of previous EU data protection law by the General Data Protection Regulation (GDPR) in 2018. New Zealand’s response to the review is being led by the Ministry of Justice, with assistance from OPC and the Ministry of Foreign Affairs and Trade. An update on progress towards renewal is expected by the end of 2020.

[redacted under [section 9\(2\)\(g\)](#) of the Official Information Act 1982]

Further privacy law reform proposals

The replacement of the previous Privacy Act was largely a response to a major review of privacy law by the Law Commission, completed in 2011. The Privacy Act 2020 modernises New Zealand privacy law and addresses some significant gaps in the previous legislation. The Commissioner will use the new powers in the Act to actively address non-compliance and promote good privacy practice.

However, technological, social and other developments affecting privacy have continued apace since the policy work for the Privacy Act 2020 was undertaken. Further changes are desirable to respond to these developments. In some respects, New Zealand’s privacy law has also not kept pace with comparable legislation in our major trading partners and other countries with which we commonly compare ourselves. The Privacy Commissioner therefore considers there is a need for further privacy law reform. Due to the rapid pace of change, further reforms are best considered and implemented as issues come to light, rather than following another wholesale review of the Privacy Act.

The Commissioner made the case for further changes to the Privacy Act in his 2017 report on the Act to the Minister of Justice and in his 2018 submission on the Privacy Bill. Some key reforms recommended by the Commissioner that have not yet been implemented are:

- **Data portability.** The right of individuals to access their personal information should be strengthened by introducing a right of personal information portability. OPC is contributing to the current consideration of a consumer data right by the Ministry of Business, Innovation and Employment.
- **Right to be forgotten.** A ‘right to be forgotten’ (for example, to have personal information delinked from search engine results) should be introduced. This

right would protect individuals from the public availability of personal information that is offensive or otherwise harmful. It would support the existing privacy right of individuals to correct their personal information and the requirement that agencies only use information if they have checked its accuracy.

- **Re-identification.** Safeguards should be introduced to protect individuals against the risk of being identified from information that has purportedly been de-identified.
- **Algorithms.** New provisions in the Act should limit harm from automated decision-making and provide greater transparency about the use of algorithms in making decisions about individuals.
- **Civil penalties.** There should be a power for a court to impose a civil penalty of up to \$100,000 for serious or ongoing breaches of the Privacy Act.
- **Compliance reporting.** The Privacy Commissioner should have a power to require agencies to report on the steps they are taking to comply with the Act.

The Commissioner would be happy to brief you on these proposed reforms.

[redacted under [section 9\(2\)\(g\)](#) of the *Official Information Act 1982*]

Authorised Information Sharing Agreements

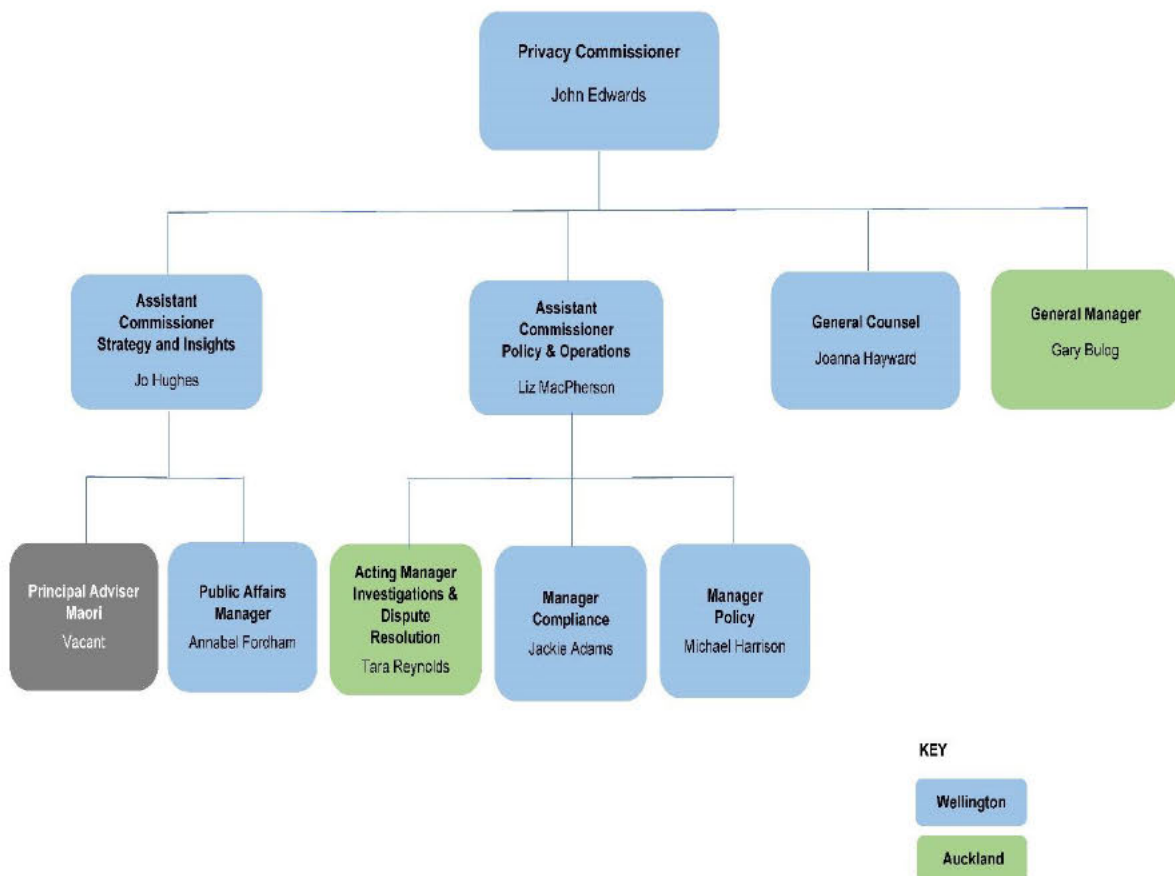
An amendment to the Privacy Act in 2013 provided for Authorised Information Sharing Agreements (AISAs), as recommended by the Law Commission in 2011. AISAs allow government departments to share personal information in order to deliver public services. They authorise agreed departures from the privacy principles, with appropriate safeguards for the individuals whose personal information is being shared.

OPC has developed guidance about AISAs and assists agencies with the development of AISAs. However, unlike codes of practice, work on AISAs is led by departments and Ministers, not by OPC. To be successful, AISAs require strong leadership and mandates for the projects in question.

OPC has identified that the barriers to information sharing are primarily operational rather than legislative. The solutions for information sharing are therefore likely to lie primarily with agencies using the flexible and enabling nature of the Privacy Act to achieve their aims. The Privacy Commissioner does not see a need for law reform in relation to information sharing but would be happy to brief you further about opportunities to improve practice in this area.

Appendix 1: key information about the Office of the Privacy Commissioner

Privacy Commissioner	John Edwards
Term Commenced	February 2014
Legal Entity	Corporation sole (Privacy Act 2020) Independent Crown Entity (Crown Entities Act 2004)
No. of Staff	37.6 FTEs
Office Locations	Wellington (27.4 FTEs) Auckland (10.2 FTEs)
Budget	\$7.276m (2020/21)
No. of Enquiries and Complaints received	Public enquiries 7,734 in 2019/20 Complaints 691 in 2019/20 Media enquiries 291 in 2019/20



Appendix 2: Other agencies involved in privacy protection

Other public agencies that play roles in the protection of privacy include the following:

- The Ministry of Justice administers the Privacy Act and is responsible for amendments to the Act and regulations made under the Act.
- The Government Chief Privacy Officer, located within the Department of Internal Affairs, supports government agencies to meet their privacy responsibilities and improve their privacy practices.
- The Director of Human Rights Proceedings can bring proceedings in the Human Rights Review Tribunal in relation to Privacy Act complaints referred to the Director after the Privacy Commissioner has been unable to resolve a complaint.
- The Human Rights Review Tribunal can hear Privacy Act complaints the Privacy Commissioner has been unable to resolve and grant remedies if there has been a breach of the Act and the complainant has suffered harm. Compliance notices issued by the Privacy Commissioner are also enforceable in the Tribunal.
- The Ombudsman assesses privacy issues when dealing with complaints about responses to official information requests.
- The Health and Disability Commissioner considers complaints about breaches of patients' physical privacy in health and disability services.
- The Inspector-General of Intelligence and Security can consider complaints about whether intelligence and security agencies have complied with the Privacy Act (the Privacy Commissioner can also consider such complaints).
- The Broadcasting Standards Authority considers complaints about breaches of privacy by broadcasters.
- The Human Rights Commission has an interest in privacy as a human right.
- CERT NZ works to support businesses, organisations and individuals who are affected or may be affected by cyber security incidents.

Some non-government organisations also play a role in privacy protection:

- The New Zealand Media Council considers complaints about privacy breaches by print and online media.
- Netsafe helps to resolve reports of harmful digital communications (including communications that disclose sensitive personal facts about an individual) under the Harmful Digital Communications Act 2015.

OPC also participates actively in international privacy networks, including the Global Privacy Assembly, which brings together privacy authorities from around the world to share thinking and resources.