Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner

Compliance and Regulatory Action Framework

Privacy Act 2020

NOV 2020

Privacy Commissioner
Te Mana Mātāpono Matatapu

Table of Contents

Commissioner's foreword

The Privacy Act 2020 gives the Privacy Commissioner new powers to improve and protect privacy for New Zealanders. Budget 2020 gave the Commissioner increased funding to do the same.

How and where we deploy these new powers and resources requires a careful consideration of competing criteria and priorities, and inevitably, tradeoffs. We want to make decisions that achieve the greatest benefit for the greatest number of New Zealanders. To help us make those decisions we've come up with this Framework.

It is my responsibility as Commissioner to ensure that we get maximum influence from our regulatory powers, and that those who are harmed by egregious privacy breaches are properly compensated and assured that others will not suffer the same fate.

Good privacy outcomes are best achieved when everyone understands their rights and responsibilities and is motivated to act on them. Decisions about how we intervene to promote and protect privacy must be predictable, rational, and defensible. We will use the right tool for the right situation. Our aim in publishing this Framework is to make our regulatory approach as transparent as possible. Our goal is high levels of voluntary compliance.

The 2020 Act imposes some new obligations on agencies, including in relation to breach reporting. A failure to report a notifiable breach will be punishable on prosecution with a fine of up to $10,000. It will take a bit of time for industry to fully understand those obligations, which is why, for the first 3–6 months we'll be primarily focussing on the education and awareness end of our "regulatory pyramid".

But for those obligations that agencies have had 27 years to get used to, we won't hesitate to use the new powers Parliament has given us to uphold people's rights. For example, everyone has a right to get access to their personal information, and it shouldn't have to take years, lengthy Privacy Commissioner investigations and Human Rights Review Tribunal proceedings to get it. Expect to see access determinations requiring disclosure.

Where we see non-compliance that might not be actionable by individuals but aggregated across the economy constitutes a significant intrusion on New Zealanders legitimate expectations, expect to see compliance notices that will seek to raise standards across an industry or sector. At the same time, we will find ways to celebrate and share good privacy practice.

This Framework will be a living document, updated as we learn what works and what doesn't. As a modern privacy regulator, we will be analysing data and insights to hone our approach, set our priorities and target our interventions. Your feedback will be an important input. Help us raise the standards of privacy protection to meet the expectations of all New Zealanders.

We can't be everywhere, and can't take action on everything, but this Framework will guide us to ensure we are where we most need to be and are taking the action that will have the greatest impact.

John Edwards
Privacy Commissioner

Our approach to compliance

The Privacy Commissioner is New Zealand's privacy regulator. The Office of the Privacy Commissioner (OPC) is an independent Crown entity that operates in an ever-evolving privacy landscape. Massive technological change continues to generate new issues and challenges in the privacy and data landscape.

Personal information is more valuable than ever before. Exchanges of personal information are central to everyday transactions and vulnerable to misuse if appropriate care is not taken. Trust in the agencies that handle our personal information is critical to individual, whanau, community, social, and economic well-being and underpins our democratic institutions. Effective privacy regulation is a critical enabler of this trust.

The modernised Privacy Act 2020 enhances the Privacy Commissioner's role as a regulator and gives the OPC an additional range of compliance and enforcement tools. As an effective modern regulator our aim is to use the full breadth of these tools – from communication and education through complaint investigation and dispute resolution to compliance notices and prosecutions. We will focus on selecting the tools that are most appropriate to the particular situation.

OPC is both a promoter of individual rights to privacy and an enabler of agencies seeking to use personal information in a safe, responsible and privacy enhancing way. Our goal is to achieve high levels of voluntary compliance. We aim to:

- empower individuals with knowledge and understanding of their privacy rights
- support and share examples of good privacy practice
- make compliance as easy as possible for those agencies that are capable and want to comply
- assist those agencies who are trying to comply but not succeeding
- use intelligence and insights to identify and deter those agencies who are reluctant to comply, and to identify systematic issues within the agencies we regulate; and
- use the compliance and enforcement tools available for those agencies who do not want to comply or are wilfully negligent.

OPC is also focused on delivering the best privacy outcomes for the highest public benefit. To achieve this, we are extending our compliance lens from a single focus on individual complaints to a greater focus on systemic issues. We will also work to identify emerging risks which, if resolved, will result in benefit for a larger number of people. This will require us to draw on internal and external intelligence and insights.

OPC will also work with other regulators and interested parties both domestically and internationally to secure good privacy outcomes. This policy also supports our goal of being a good regulatory steward. Where possible we will take a systems approach to issues, we will look across a sector and also across other regulatory bodies to ensure that our response is effective and efficient.

Why we wrote this policy

Our aim in producing this Compliance Policy is to be open and transparent about the way in which OPC intends to approach its regulatory and compliance activities. This includes setting out the principles that underpin our approach and the factors we use when making decisions about regulatory and compliance interventions.

We will select the best tools for the job by considering the extent or risk of harm to individuals, the public interest/benefit, the attitude to compliance and the conduct of the individual or agency. We aim to use our compliance tools predictably, proportionately, consistently and judiciously.

At the same time, we will promote compliance with the law by identifying and celebrating best practice and sharing lessons learnt to support agencies and individuals to build their privacy maturity.

Ultimately, our Office's role is to promote and protect individuals' privacy and we can only do that through taking a holistic approach to compliance, including:

- assisting and supporting agencies to understand their obligations;
- taking proportionate and appropriate action in response to breaches of the Act.

There are three key drivers that inform our approach to regulatory and compliance action. These are:

Public Trust - we are a critical part of New Zealand's trust infrastructure

Independent oversight bodies like us are essential to maintaining public trust. Our independence is also central to our ability to celebrate best practice and call out poor compliance behaviour when we see it. Without public trust, it is much more difficult for public and private sector agencies to engage with individuals, and this has flow-on effects to wider society and the economy. Respect for privacy is part of the essential social licence between an individual and the agencies they deal with.

Education - we promote good practice and seek to facilitate compliance

We provide agencies with tools, resources, guidance and advice about how they can best protect individual privacy. We also provide individuals with their own resources to help them exercise their rights and entitlements under the Privacy Act. We want agencies to understand their obligations and for individuals to know their rights, as together this facilitates compliance.

We also celebrate agencies who go above and beyond what is required of them by making privacy an embedded value in their products or services.

Accountability – we hold agencies to account for their actions

Our approach is designed to take account of the need to protect individual privacy while ensuring agencies have the ability to operate efficiently and effectively. We support agencies to uphold individuals' rights to privacy but take a robust, fair and considered approach to non-compliance. In these cases, we seek to hold agencies to account for their actions. We will act proactively and take prompt action where we see poor compliance with the Privacy Act.

WHO WE ARE

Our role is to be:

An effective modern privacy regulator both in New Zealand and abroad.

WHAT WE'RE HERE FOR

To achieve this we:

Work to promote a culture in which personal information is protected and respected.

And our objectives are to:

- make privacy protection effective and easy to achieve
- keep the costs of privacy compliance at a minimum
- be a responsive, fair and trusted regulator
- be influential and promote good privacy practice.

HOW WE'LL DO IT

We'll deliver this by being:

- Fair
- Proportionate
- Consistent
- Accountable
- Transparent
- Partnering with Māori

The Privacy Commissioner has a range of tools at his discretion when responding to privacy concerns and issues. These allow the office to take the most appropriate response in the circumstances. The factors we consider when deciding what approach to take are:

- How serious, widespread or systemic the issue is
- Whether there is a broader public interest in the matter because of its educational, deterrent or precedential nature
- The conduct the agency has displayed, eg staff education, proactive engagement with OPC etc
- Whether the agency's attitude suggests the issue is wilful, negligent or intentional
- Whether OPC can effectively partner with another regulator to achieve compliance
- How effective any action is likely to be

Privacy Commissioner
Te Mana Mātāpono Matatapu

Privacy Commissioner
Te Mana Mātāpono Matatapu

What we do

The purpose of the Privacy Act is to promote and protect individual privacy. Our mission is to give effect to our functions and powers under the Privacy Act in a way that is meaningful and responsive and upholds the purpose of the Act.

The Privacy Act provides a framework for protecting an individual's right to privacy of personal information. The Act also creates obligations for agencies regarding how they handle personal information. Where these standards are not met, the Privacy Act gives individuals the ability to challenge those actions through OPC, the independent regulator.

The Privacy Commissioner is empowered by the Privacy Act 2020 to protect personal privacy and oversee agencies compliance with their obligations under the Act.

This compliance and enforcement policy explains the use of the compliance tools and the exercise of regulatory powers related to those functions. These include the functions to engage and work with other agencies, as well as powers to investigate Privacy Act complaints, facilitate the settlement of complaints, and issue access directions and compliance notices. These functions and powers can be delegated by the Commissioner to OPC staff.

The Privacy Act applies to any public or private sector agency that collects or holds personal information.[1] An agency is any business, group, or organisation (and can include an individual) that collects personal information. For example, 'agency' includes clubs, landlords, charities, sole traders, banks and government departments[2] The Act applies to the actions of agencies, both within New Zealand and outside of it.[3] Agencies covered by the Privacy Act are required to comply with the relevant provisions in the Act and legislative instruments made under the Act (such as Codes of Practice).

OPC has a broad range of functions including[4] the ability to:

- make public statements on matters affecting individual privacy
- investigate complaints about breaches of privacy
- build and promote an understanding of the privacy principles
- monitor and examine the impact that technology has on privacy
- develop codes of practice for specific industries or sectors
- examine draft legislation for its possible impact on individual privacy

[1] Section 7 of the Privacy Act 2020 says Personal information (a)means information about an identifiable individual; and (b)includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995)
[2] Privacy Act 2020, ss 4, and 7.
[3] Privacy Act 2020 ss 4, and 8-9.
[4] A full list of the Commissioner's functions is set out at section 17 of the Privacy Act 2020.

- monitor data matching programmes between government departments
- inquire into any matter where it appears that individual privacy may be affected
- receive reports of notifiable privacy breaches
- monitor and enforce compliance with the Privacy Act; and
- report to government on matters affecting privacy, both domestic and international

OPC also has oversight functions relating to privacy matters under other enactments.

Guiding principles

OPC will be guided by the following principles in our approach to compliance and regulatory action. These principles inform our approach to all of our regulatory behaviours and sit alongside the factors we consider when deciding which regulatory action to take (these are set out in the next section of this policy).

1. **Fairness** –As a modern regulator we take a considered approach to compliance and regulatory efforts in order to get the best outcomes for New Zealanders. OPC acts independently in accordance with the principles of natural justice.
2. **Consistency and transparency -** OPC will act consistently and transparently. OPC will be open about how it uses its powers, including through publishing guidance (including this policy). OPC will also act in accordance with the principles of good decision making, including as set out in the Office of the Ombudsman's guidance on good decision making by state sector agencies.[5]
3. **Proportionality** – Any regulatory or compliance action OPC choose to take will be proportionate to the conduct which has occurred and the benefits which are expected to result.
4. **Accountability** – OPC is accountable for any regulatory action we take, including through review and appeal rights. We will ensure stakeholders are advised of these rights.
5. **Kōtuitui**[6] - OPC seeks opportunities to partner with Māori whenever possible. OPC strives to interweave mātauranga[7] Māori for positive intercultural outcomes.

[5] ombudsman.parliament.nz/sites/default/files/2019-08/Good%20decision%20making.pdf.
[6] 'to lace, fasten, interlace, connect'
[7] Mātauranga Māori provides insight into different perspectives about knowledge and knowing. Mātauranga Māori in our mahi is not just creating a space for Māori ways of being and knowing but valuing the richness that these whakaaro (ideas) bring to our kaupapa (agenda). It is understanding that there is no 'one' way to 'know' something. It is also understanding that the strength in our mahi

We recognise the importance and relevance of the principles of Te Tiriti o Waitangi (Treaty of Waitangi) and the concepts of participation, protection, and partnership. We are at the early stages of our journey of learning and engaging with mātauranga Māori. We will continue to work with and in consultation with Māori to gain a deeper and more productive understanding of how our work can honour and give practice to Te Tiriti. We believe that this work will be of benefit to all New Zealanders.

When investigating or inquiring into an alleged interference[8] or infringement with individual privacy, and broader non-compliance with the Privacy Act we will consider each matter on a case by case basis and have regard to all the relevant circumstances of the individuals and agencies involved.

Decision factors

OPC takes a considered approach to the regulatory action we take. We prioritise certain matters for compliance or regulatory action and select the most appropriate response in the circumstances. We seek to use our limited resources to best effect. Factors we will consider when deciding whether to take action in response to an issue, and what action to take, along with the purpose and objectives of the Privacy Act, include the following[9]:

Seriousness

- the nature and seriousness of a privacy issue, or the potential impact, including:
  - the adverse consequences caused or likely to be caused to the affected individual/s
  - whether the matter involves sensitive information
  - the number of individuals potentially affected
  - whether disadvantaged, vulnerable, or a particular group of individuals have been or may be adversely affected
  - whether the conduct indicates a potential systemic issue (either within the agency concerned or within a sector or industry) or an increasing issue which may pose ongoing compliance or enforcement issues

Public interest

- the level of public interest in the issue, or in compliance or regulatory action being taken including:

(work) comes from multiple world views and the acknowledgement that Mātauranga Māori can deepen and enhance other theories (e.g. critical theories). – Kia Eke Panuku - https://kep.org.nz/

[8] An interference with the privacy of an individual occurs when an agency breaches a privacy principle, a code of practice, an approved information sharing agreement, an information matching agreement, or the requirement to give an affected individual notice of an identifiable privacy breach, and that action result in harm to an individual

[9] Note these criteria are not intended to be exhaustive. There are additional and specific criteria which are relevant to our various compliance response tools.

- the educational, deterrent or precedential value of taking action
- whether the issue would clarify or test a matter of law
- the way the issue came to OPCs attention, and if relevant, failure or delay by the relevant individual or agency to notify OPC of the breach or issue
- whether the agency responsible for the incident or conduct has been the subject of prior compliance or regulatory enforcement action by OPC, and the outcome of that action
- the need to inform individuals to provide a full picture, or correct inaccurate, incomplete or misleading information

Attitude and Conduct

- the attitude to compliance, and conduct of the agency concerned, including:
  - the state and nature of any protective or preventative policies, technology or other measures being utilised by the agency at the time since the actual or alleged issue occurred
  - the agencies general approach to compliance and engagement with OPC
  - action taken by the agency to remedy and address the consequences of the conduct, including whether they attempted to remedy their conduct, and whether the agency cooperated with OPC and with affected individuals
  - whether the conduct is or appears to be wilful, negligent or intentional
  - whether the conduct is an isolated instance, and the likelihood of the agency repeating the behaviour at issue in the future
  - the position, seniority and level of experience of the person or persons responsible for the conduct

Statutory factors

The Commissioner must also consider certain matters when exercising any functions under the Privacy Act. [10] These include:

- Other human rights and interests such as the desirability of facilitating the free flow of information, and government and business efficiency in achieving their objectives
- Cultural perspectives on privacy
- New Zealand's international obligations, including international technology of communications

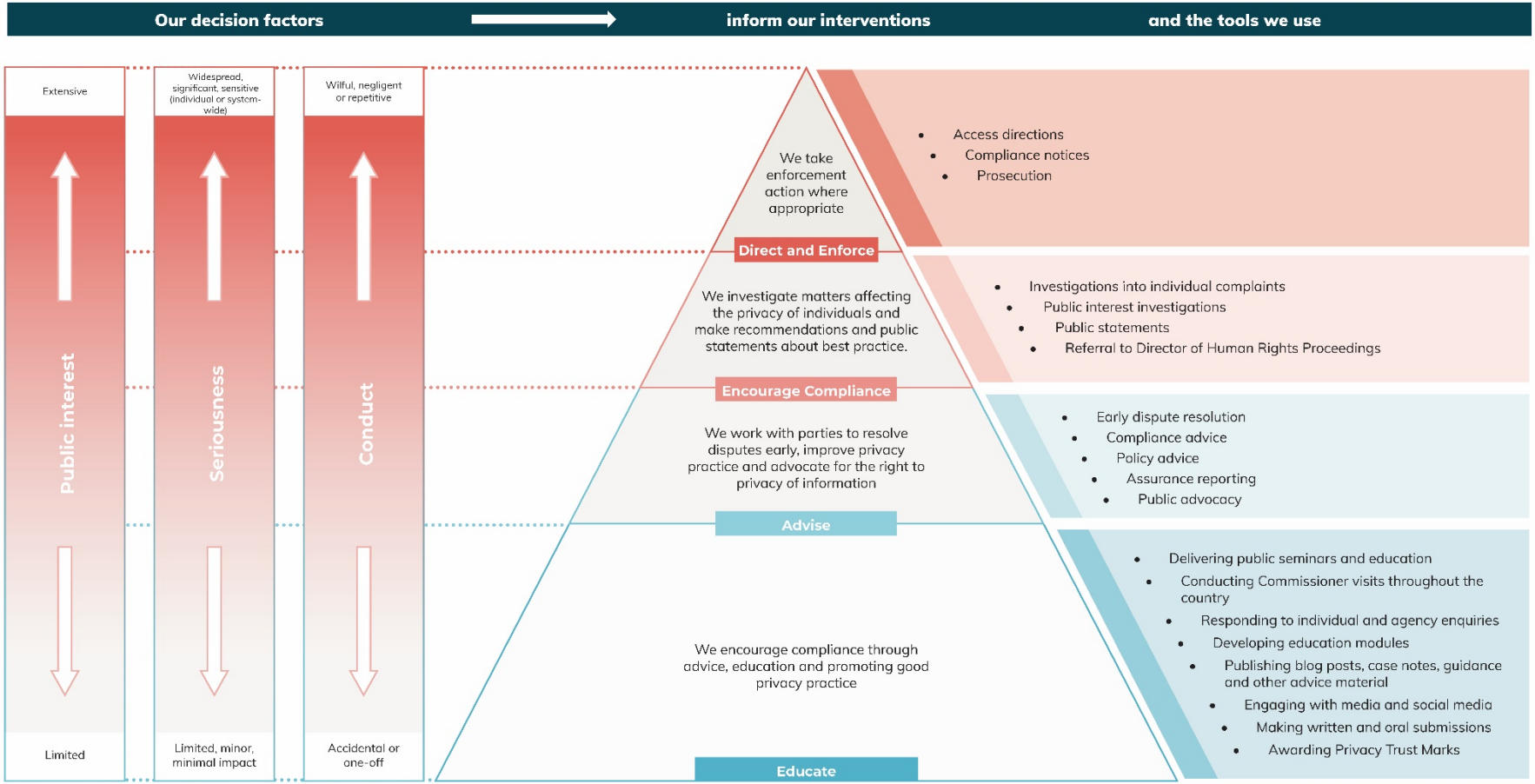
[10] Privacy Act, s 21.

- International guidelines relevant to the better protection of individual privacy
- Information Privacy Principles.

Other factors

- the time since an actual or alleged breach or issue occurred
- the appropriateness and proportionality of taking particular compliance or regulatory action, including:
  - whether the burden on the agency likely to arise from the regulatory action is proportionate to the risk posed to the protection of personal information
  - whether another regulator, law enforcement body, or authority is already taking (or has already taken) action in respect of the same matter
  - the cost and time to OPC in order to achieve an appropriate remedy or improved compliance
  - whether there is adequate evidence available to prove a breach, alleged breach, interference, or infringement; and
- any other factors which OPC considers relevant in the circumstances, including factors which are relevant to the specific compliance function or regulatory power being exercised.

REGULATORY ACTION AND COMPLIANCE



Compliance intervention options

The compliance pyramid is designed to create downward pressure – that is, to encourage non-compliant individuals or organisations to move down the pyramid to full compliance and to where lower-level and less costly interventions are effective.

While we seek to encourage and support agencies to comply with their privacy obligations, we will act to hold agencies to account where this is necessary to address serious non-compliance. This means we will not necessarily take an escalating approach to regulatory action – some issues may require an immediate enforcement approach.

We take a constructive and educative approach to our compliance actions. We believe the most efficient and effective means of protecting individual privacy is through enabling agencies to educate themselves about their obligations and for our Office to provide guidance and advice to support agencies to do so. We also have a number of other regulatory tools available to us to facilitate compliance, which are set out alongside the pyramid above, and are discussed in more detail below.

Educate – We encourage compliance through advice, education and promoting good privacy practice

OPC provides agencies with guidance and tools to promote best practice and to identify and address privacy concerns as they arise. Our preferred approach is to facilitate voluntary compliance with the Privacy Act, and we provide a range of education tools and resources to encourage this.

OPC encourages agencies to seek out the tools and resources available on the OPC website to improve their understanding and compliance with the Privacy Act.

OPC also supports agencies and individual's understanding of the Privacy Act through:

- delivering education and outreach seminars
- attending privacy conferences and events
- conducting Commissioner visits throughout the country
- developing free educational modules
- the ongoing development of our AskUs knowledge base tool
- writing timely and relevant blog posts and case notes
- publishing guidance
- engaging with media and social media
- making written and oral submissions on important privacy issues

Advise - We work with parties to resolve disputes early, improve privacy practice and advocate for the right to privacy of information

Privacy issues and concerns come to our attention from a range of sources, including:

- individual complaints and enquiries
- agency enquiries and engagement
- privacy breach notifications
- media and social media enquiries

We encourage agencies and individuals to seek guidance, advice or comment from our Office after utilising our publicly available resources. We can also assist agencies to identify risks and competing interests (e.g. privacy interest which compete with business interests) and provide pragmatic advice.

We work to advise agencies about best practice and inform individuals of their rights through our enquiries function. We get thousands of enquiries per year from members of the public and agencies alike about the operation of the Privacy Act and associated issues. In response we do everything from provide information and generic advice about how the Privacy Act works, to advising on whether we could investigate a complaint under the Act (more on this below). Where appropriate we will attempt to resolve disputes about alleged interferences with privacy prior to launching a formal investigation.

We also proactively engage with agencies to provide advice where an issue has been drawn to our attention. We seek to understand the issue and provide advice or guidance necessary in order to resolve or address any non-compliance.

We advocate for the protection of privacy rights through our public statements, research activities and submissions on matters of public importance such as draft legislation and government policy.

We undertake assurance reporting activities, where we ask agencies to report on their compliance with certain obligations. These activities help provide transparency about particular sectors activities and information sharing arrangements. For example, the Credit Reporting Privacy Code requires credit reporters to submit annual reports to provide assurance about their compliance with aspects of the Code. The reports cover staff training and processing of individual requests for information.

Encourage Compliance – We investigate matters affecting the privacy of individuals and make recommendations and public statements about best practice.

OPC has two main regulatory tools which encourage compliance– Investigations of individual complaints, Public interest investigations (Inquiries) and public statements. An investigation or Inquiry can result in further compliance or regulatory action being taken by our Office.

When addressing issues brought to our attention, OPC will take into account the steps taken by an agency to comply with its privacy obligations, in addition to the factors outlined above in this policy.

Investigations into individual complaints

The Privacy Act provides the Privacy Commissioner with the role of receiving, investigating, and conciliating complaints about privacy. An individual, or their authorised representative, can make a complaint to OPC if there has been an actual or apparent interference with their privacy.[11]

As discussed above where appropriate we will attempt to resolve disputes early, however if we cannot do so, we can launch a formal investigation to determine if there has been an interference with the privacy of an individual or individuals.

In respect of the right of access to and correction of personal information, an interference will occur if the agency refuses a request without proper basis or makes a decision under Part 4 of the Privacy Act without proper basis (such as the decision to charge for access to information).

During an investigation, the Commissioner has powers to require any person to provide any relevant information to OPC. The Commissioner also has powers to summons individuals and question them under oath.

We have a strong dispute resolution mandate and work with parties to achieve fair outcomes. During, an investigation OPC will use best endeavours to secure a settlement of the complaint or seek assurances from the agency concerned that there will not be a repetition of the action that gave rise to the complaint.[12] We frequently use the opportunity we have to talk to agencies during the investigation process about their ongoing obligations and overall attitudes to privacy.

Where our dispute resolution and investigatory attempts to settle or resolve a complaint are unsuccessful, we have the option of either moving to enforcement interventions (more on this below) or closing our file, which will allow the individual the option of pursuing their case in the Human Rights Review Tribunal. The Tribunal hears matters 'de novo' – this means they can make a fresh determination on the case. Individuals can take their own cases before the Tribunal.

Referral to the Director of Human Rights Proceedings

In exceptional cases, where we have found an interference with privacy but have not been able to achieve settlement, the Commissioner can choose to refer matters to the Director of Human Rights Proceedings. The Director can decide

[11] An interference with the privacy of an individual occurs when an agency breaches a privacy principle, a code of practice, an approved information sharing agreement, an information matching agreement, or the requirement to give an affected individual notice of an identifiable privacy breach, and that action result in harm to an individual (see section 69(2)(b) of the Privacy Act). There are also actions under statutes other than the Privacy Act which are treated as a breach of an information privacy principle, or an interference with the privacy for the purposes of section 123(1)(b) of the Privacy Act. These are set out in full in Appendix 1 of OPCs Compliance Notice Policy. That appendix also sets out the codes of conduct in other legislation which, if breached, provide an avenue for complaints to the Privacy Commissioner.

12 Sections 77 and 83(1).

whether to take action in the Tribunal on behalf of the individual or individuals concerned. The Director is independent of our Office and once a matter is referred, we have no further engagement or involvement.

Generally, we only refer cases to the Director where there is a significant interference with privacy, issue of law, or wider systemic problem.[13] If a matter is referred to the Director, the Director can either attempt to settle the complaint themselves through negotiation with the parties or can take the matter to the Human Rights Review Tribunal for a ruling.

Public interest investigations

The Privacy Commissioner also has the discretion to undertake investigations into matters where the privacy of individuals is being or may be infringed (these are sometimes called inquiries). The Commissioner may initiate such an investigation where there are systemic issues occurring within an agency or sector, general issues of non-compliance, the matter has failed to be resolved through other means, affected a large number or a vulnerable group of individuals and/or where there are matters of public importance.

These investigations also engage the Commissioner's powers to require information to be provided and to summons individuals and question them under oath.

The Commissioner can choose to initiate a public interest investigation following a complaint, enquiry, data breach notification or of their own volition. The factors in decisions making described above will be considered before launching any inquiry.

Many of these public interest investigations also result in the publication of a report, which is widely disseminated. These reports are designed to provide lessons learned across sectors and agencies, not just to the agency or agencies involved in the investigation. Reports can also be sent to any relevant Ministers or the Prime Minister if the agency involved is a public one.

At any time during an investigation being conducted on the Commissioner's own initiative, the Commissioner may use best endeavours to secure an assurance from the respondent that there will not be a repetition of the action that gave rise to the investigation, or of a similar kind of action.[14]

Public statements

Section 206 provides discretion for the Commissioner to make disclosures where they consider that information should be disclosed to give effect to the Privacy Act.

[13] None of these factors, or any others which may arise in a particular case will necessarily be determinative in themselves. All relevant factors must be weighed individually and all balanced in the overall circumstances of the complaint.
[14] Section 83(2).

The disclosures the Commissioner may choose to make can take several forms including press statements, blog posts, case studies and speeches (there is more information on Adverse Comment and public disclosures below).

In order to influence agency or sector behaviour and encourage compliance with the Privacy Act the Commissioner may also choose to name an agency publicly. Naming will predominantly occur where the Office becomes aware of agency non-compliance but could also occur in relation to the notification of a privacy breach or through other monitoring practices.

Any public statement made will be guided by the Regulatory Action Principles described above. If a disclosure would amount to an adverse comment about an agency or its practices the Commissioner will consult with that agency prior to making any disclosure -discussed further below.

We are committed to acting fairly with any entity that may be the subject of any of our regulatory powers, including public statements. We are mindful of the reputational impacts that statements from our Office can have when exercising this discretion.

Direct and Enforce – We take enforcement action where appropriate

OPC has three direction/enforcement tools. Our main ones are Compliance Notices, and Access Directions. In addition, in particular instances of non-compliance the Commissioner may also decide to bring a Prosecution.

Compliance notices

OPC monitors compliance with the Privacy Act through a range of channels - public enquiries, media reports, privacy complaints, Commissioner initiated inquiries and investigations, the exercise of the Commissioner's oversight and monitoring functions, privacy breach reporting, and referrals from other regulators, both within New Zealand and internationally. Compliance issues can arise from a specific incident or from repeated or systemic issues.

On becoming aware of a compliance issue, the Privacy Commissioner may consider issuing a compliance notice. A compliance notice is a written notice from the Privacy Commissioner to an agency advising them they are in breach of their statutory obligations. A compliance notice will specify the nature of the breach and require the agency to remedy the breach, by taking certain action or discontinuing certain actions, so that they comply with their statutory obligations. Sometimes they will be required to do this with a specified timeframe.

Compliance notices are enforceable in the Human Rights Review Tribunal if the agency does not comply with the notice or fails to appeal the notice. The Tribunal may make an order that the agency comply with the notice by a specified date. Failure to comply with a Tribunal order is an offence, and if prosecuted, an agency could be fined for non-compliance.

Access directions

Access directions relate to the right of access which individuals have under principle 6 of the Privacy Act. If OPC has investigated a complaint about access to personal information, and it is not resolved despite using our best endeavours, we will consider making an access direction to the relevant agencies.

An Access Direction is a written notice requesting an agency to confirm whether it holds any specified personal information, permit the individual concerned access to any specified personal information and make specified information available to the individual.

If the agency does not comply with an access direction, the complainant may apply to the Tribunal for enforcement of an access direction. Agencies can also appeal an access decision to the Human Rights Review Tribunal.

Prosecution

OPC can bring prosecutions under the Privacy Act in limited circumstances. Our ability to prosecute primarily relates to matters to do with our process, rather than infringements or interferences with the privacy of an individual.

There are only two offences which relate to personal privacy – one where a person impersonates an individual, or falsely pretends to be acting under their authority, in order to access that individuals personal information, or to have it used altered or destroyed, and one where anyone destroys personal information knowing that a request has been made for that information.

The other offences are procedural and relate primarily to:

- obstructing the Commissioner,
- failing to comply with a lawful requirement of the Commissioner,
- represents directly or indirectly that they hold any authority under this Act when they do not hold that authority,
- making false representations to the Commissioner, or
- failing to report a notifiable privacy breach to the Commissioner.

The offences under the Privacy Act carry with them a maximum fine of $10,000 on conviction.

Prosecutions under the Privacy Act are rare, and not an enforcement tool we use lightly. There are strict evidential and public interest considerations we must take into account when deciding whether to prosecute, as well as a number of other factors. More detail about prosecution decisions are set out in OPCs Prosecution Policy.

Confidential process

Section 206 of the Privacy Act requires that the Commissioner and any person who is or has been employed or engaged by the Commissioner must maintain

strict secrecy in respect of all matters which come to our knowledge while working in the Office.[15]

Our secrecy obligations mean that in general we do not release information we have received from an individual or agency to the agency or individual concerned, other agencies or individuals, or the media. This allows both agencies and individuals to provide information to us confident that it will not be passed on. For example, during an investigation of a complaint we will not share information between parties.

Adverse comments

Any public statement OPC makes must comply with the Privacy Act. From time to time the Commissioner may choose to make statements about compliance actions that OPC have taken. Such statements are designed to promote and protect individual privacy through providing teachable moments.

As a matter of course, we will provide an opportunity to comment from those we regulate about the use of our compliance or regulatory tools, or a determination we have made during an investigation. This is because the Commissioner must not make any comment that is adverse to any person or agency unless that person has been given an opportunity to be heard.[16] As well as being a statutory obligation, this is also a matter of natural justice and fairness.

This applies to:

a. Notification and results of an investigation
b. Publishing general reports and case notes
c. Reports to the Prime Minister
d. Public statements about privacy issues
e. Reports of a breach of duty or misconduct

A comment made by OPC will not necessarily be ‘adverse’ just because it goes against the interests of an agency or rejects an allegation or legal argument they have put forward. Generally however, a finding that a respondent agency has breached a privacy principle or rule, interfered with the privacy of an individual or individuals, or infringed on individual privacy, will be an ‘adverse’ comment and we will give you an opportunity to comment before finalising our view. We will give you a reasonable time frame to respond, which will be determined on a case by case basis, at the discretion of the Commissioner.

[15] Privacy Act, s 206.
[16] Privacy Act, s 210.

Working with agencies

Working with other regulators

We look to cooperate and coordinate with other regulatory bodies both domestically and internationally in order to make the best use of our resources. For example, we have worked closely with the Independent Police Conduct Authority regarding the Police Vetting Service including conducting a joint review. We look to take joint regulatory action where appropriate.

On other matters, we may consult agencies across the public and private sector for their input or for the perspectives of those who will be impacted by a proposed approach to compliance and the exercise of the Commissioner's functions.

OPC participate in international networks and forums and is closely connected with privacy enforcement authorities overseas. We draw on the relationships we have with our international colleagues to get expert input from around the world on matters we are dealing with domestically, to get inspiration for the development of our own guidance and policies, and to discuss privacy and data protections issues which are occurring on a global scale. Participation also allows us to coordinate our efforts to ensure to best effect.

OPC is a member of the Global Privacy Enforcement Network (GPEN) whose mission is to improve cooperation in enforcement of cross-border laws affecting privacy. We also have Memoranda of Understanding with some authorities which promote exchange of information in order to assist each other in the enforcement of laws protecting personal information.

Referring matters to other regulators

In some cases, OPC will not be the best agency to deal with an issue which has been brought to our attention. We co-operate with both other regulators and overseas privacy enforcement authorities on a range of matters.

In terms of complaints, the Commissioner may transfer a complaint in whole or in part if it relates to a matter more properly within the jurisdiction of:

a. an Ombudsman
b. the Health and Disability Commissioner
c. the Inspector-General of Intelligence and Security
d. the Independent Police Conduct Authority
e. an overseas privacy authority

Before we transfer a complaint, we will consult with the relevant agency and decide the appropriate means of dealing with the complaint. We also have the ability to transfer a complaint in whole or in part to an overseas privacy enforcement authority if the Commissioner considers the matter is more properly within their jurisdiction. As with transfers within our own jurisdiction, the Commissioner must consult with the other privacy authority first and decide the appropriate means of dealing with the complaint.

Working with agencies we regulate

OPC's approach to regulation is to facilitate voluntary compliance with privacy obligations and to work with agencies to ensure best practice and prevent privacy harm to individuals.

Whether undertaking proactive work or resolving matters brought to our attention by member of the public, we will take into account the steps taken by an organisation to comply with their privacy obligations, the seriousness of the issue and whether the matter is systemic, ongoing or isolated in addition to considering the other factors outlined in this policy.

This will often be an efficient and effective means of pursuing the objects of the Privacy Act. We can use a range of tools as part of this approach, only some of which involve the use of regulatory powers. In line with our commitment to transparency and accountability, we will be as open as possible about our compliance and regulatory work when we are dealing with an agency faced with a compliance issue.

Effectiveness

Our Statement of Intent sets out the measures we apply to the effectiveness of our work. We are also committed to reviewing and amending where necessary the measures we use to assess the effectiveness of our regulatory actions.

We will report annual to Parliament about our work, including our compliance and enforcement activity. We will also publish an annual report which will include information on:

- Number of complaints received
- Average length of complaint investigation
- Inquiries undertaken
- Data breach notifications received
- Speaking engagements attended
- Enforcement action undertaken

Throughout the year we will also report on specific issues where we believe there is a significant public interest.

In line with our commitment to transparency and accountability, we will as open as we can be about our regulatory, and, where relevant, enforcement work. We will normally publish details about the volume and types of cases we pursue and the outcomes we achieve. In particular, we will report on those relating to access directions, compliance measures and prosecutions.

We may publish case study examples to illustrate good practice or learning. We will take care to ensure that redaction of confidential, personally sensitive or commercially sensitive information is properly considered when publishing details of specific cases.

We welcome and actively seek feedback from the regulated sector, individuals and other regulators on the impact of our actions.

Review of policy

This policy will be kept under review and updated as necessary.