Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner

Decision Guide: Investigations and Dispute Resolution

Updated March 2024

Our investigative function

In general, the Privacy Act doesn't provide detailed procedural requirements for our investigations and dispute resolution function. Instead, there are a relatively small number of key mandatory requirements or legal checkpoints – such as the requirement to notify the parties if the Privacy Commissioner ("the Commissioner") intends to investigate the matter. The Act gives the Commissioner and his staff (under delegation) a significant amount of autonomy and discretion in carrying out investigations, choosing to facilitate settlement either with or without investigation as well as a discretionary power to decline to investigate if certain grounds exist.

The impact of our decisions: Legal and practical consequences

The Office of the Privacy Commissioner ("OPC")'s decision to investigate, attempt to settle or decline to take action affects the legal rights of complainants and respondent agencies. If we decline to investigate a complaint for lack of jurisdiction, or using our section 74 discretion, the complainant will not have access to the Human Rights Review Tribunal ("the Tribunal"). While our decision to decline to investigate can't be taken to the Tribunal it is subject to review by the Office of the Ombudsman ("Ombudsman") or to judicial review in the High Court. In this way we have something of a gatekeeper role, directly limiting access to judicial decision-makers who can provide remedies.

OPC has created a Compliance and Regulatory Action Framework ("CARAF"), which should be used to inform the decisions we make to investigate, decline to investigate or take some alternative action.[1]

Our complaints role in context: One of a range of tools for addressing non-compliance

Investigators need to bear in mind that investigations of individual complaints is only **one** of the means established by the Privacy Act for addressing breaches of the privacy principles.

If, for example, our assessment of a complaint finds there's been a breach but no harm, but we consider there are issues that warrant some action, there may be other options available to address the matter under our other statutory functions. There are a range of options that are available in these situations, including providing advice to the agency, or issuing a case note or guidance document where wider dissemination of the learnings could help promote an understanding of the Act's requirements more generally. If an investigation into a complaint by an aggrieved individual is not appropriate, the investigator can also consider referring the matter to the Compliance & Enforcement Team or the Compliance Advisory Board ("CAB"), particularly if the breach is serious.

We have a number of other options for addressing systemic or significant privacy problems within a particular agency or type of agency. We might utilise these options before, instead of after, or during the investigation of a complaint, depending on the circumstances.

[1] https://privacy.org.nz/about-us/what-we-do/caraf/

Examples of further action

- A warning or compliance advice letter
- Ongoing monitoring of the agency
- Approaching the Chief Executive or the Minister about an underlying systemic issue
- Educating for the agency or industry
- Guidance for the agency or industry (e.g. our Tenancy Guidance, CCTV guidelines)
- Transferring the matter to another investigating agency
- Public comment (media release, *Privacy News*, social media comment)
- Naming the respondent in accordance with our naming policy[2]
- Issuing a compliance notice.

Legal checkpoints: Key statutory and common-law rules

Below are some key legal rules and principles that provide a framework for all actions and decisions in our complaints and investigations role.

Act within the law

- Don't exceed the power given by the Privacy Act or interpret its provisions unreasonably. Interpretation should be consistent with the purpose of the Act (section 3).
- Maintain independence and impartiality. We do not act as an advocate for either party.

Accessibility focused approach

- Don't assume either the complainant or the respondent will have knowledge of our process.
- Don't try and interpret facts in order to fit a Privacy Act complaint.
- Do try and work out what the complainant and respondent are trying to achieve and help direct them to the most appropriate place for that.
- Do try and manage expectations about what we can and cannot do.

Natural justice

- Give people a reasonable chance to have a say and listen to them.
- Give clear reasons for our decisions and actions.

[2] https://privacy.org.nz/assets/New-order/About-us/Transparency-and-accountability-/3.-Naming-policy.pdf

- Give people an opportunity to be heard on any proposed adverse comment.
- Significant discussions with a party over the telephone may need to be followed up in writing.

Using our discretion

- The processes we follow shouldn't be so rigid that we fetter our discretion under the Act.
- But at the same time be as consistent as possible. Our decisions should be consistent with the Commissioner's earlier interpretations of the law and of established judicial authority – and if we do change our mind, we need to acknowledge the change and carefully justify it with clear reasons.

Secrecy and privileged information

- Maintain the secrecy of all information and matters that come to your attention during your work, unless we need to disclose the information to fulfil the purposes of the Act (section 206).
- Protect privileged information (section 90). Make sure that privileged information we receive as part of an investigation remains privileged. We can see it, but no-one else should.
- Protect whistleblower information under the Protected Disclosures (Protection of Whistleblowers) Act 2022 ("the Protected Disclosures Act").

Don't copy correspondence from one party to the other

Sometimes we are asked by one party for a copy of correspondence that we've received from the other party. We deny these requests, relying on sections 29 and 206.

You should instead simply summarise the substance of the relevant allegations and arguments from the first party. Here you should be careful about exactly what you relay to the other party. Ensure that you are communicating the information necessary to progress the matter. If the information is particularly sensitive (for example, a complainant's description of their harm) check with the party who provided it first to confirm they are comfortable with your summary.

Ensure that where information is covered by the Protected Disclosures Act, information is protected in accordance with that Act. If you have any questions about this, discuss with your manager.

Other legal rights and interests

We must also take into account other rights and interests, including:

- other human rights and social interests that compete with privacy, such as the general desirability of the free flow of information and the right of government and business to achieve their objectives in an efficient way
- New Zealand's international obligations, and general international guidelines relevant to privacy
- cultural perspectives on privacy, including the concepts and principles underpinning Te Ao Māori
- rights under Te Tiriti o Waitangi, including a focus on Treaty of Waitangi obligations:
    - interpretation and the application of the principles of the Treaty,
    - racial equity,
    - personal bias and the existence and impact of institutional racism, and
    - tikanga Māori.

Protected Disclosures

- We are an appropriate authority under the Protected Disclosures Act to receive complaints about serious wrongdoing in respect of the privacy of individuals or security of personal information.
- This means that where a complaint is from a current or former 'employee' of the reported agency (including a contractor, secondee, volunteer, someone involved in the management of the agency, a homeworker, or Member of the Armed Forces) and the conduct may reach the threshold of 'serious wrongdoing', we need to clarify whether that Act applies and, if so, comply with its requirements (which includes protecting the confidentiality of the discloser and others involved in any investigation, consulting before any referral to another agency, and timeframes for responding).
- If you receive correspondence that you think might be a protected disclosure, discuss with your manager.

Complaints

Complaints can be oral

Complaints do not have to be in writing. We can't therefore insist a complainant must put their complaint in writing before we can accept it.

However, the Act also says an oral complaint must be put into writing as soon as practicable, and that we have to give the complainant "such reasonable assistance as is necessary in the circumstances" to enable them to put it in writing (section 72). This means it is generally more efficient for a complainant (or their advocate) to put the complaint in writing themselves if this is possible. If you do take a verbal complaint, send the written version to the complainant to confirm you have accurately recorded their concerns before you progress the matter further.

Initial screening:
Is this a complaint we can and should investigate?

When we first receive a communication, we need to:

- establish whether the person intends it to be a complaint under the Privacy Act
- decide whether it's a complaint we have jurisdiction to investigate.

If we do have jurisdiction, we then need to decide what action to take. This includes whether we should decline to investigate it using our discretion under section 74, if one of the grounds in that provision applies.

If it is a complaint, is it one we have jurisdiction to investigate?

People and bodies outside our jurisdiction

We don't have jurisdiction to investigate the complaint if it concerns a person or body that is not an "agency" within the terms of section 8 of the Privacy Act.

Overseas agencies

If an overseas agency is carrying out business in New Zealand, the Privacy Act will apply to the information it collects or holds in the course of carrying out that business. However, the definition of overseas agency excludes foreign governments, entities carrying out public functions on behalf of any foreign government and news entities (to the extent that it is carrying on news activities).

The Act also applies to an agency that is a foreign individual, but only in respect to information collected by that individual in New Zealand or that is being held by them while that individual is present in New Zealand.[3]

Is it an agency?

The news media is excluded when carrying on news activities – as long as they are regulated (e.g., BSA, Media Council or overseas equivalent).

There are organisations that don't fall within the definition of "agency" for the purposes of their interactions with the public, but are "agencies" in relation to the personal information they hold on their employees. For example, we can't investigate complaints about courts or tribunals in relation to judicial functions. That exclusion covers judges and court/tribunal officials – but it **doesn't** cover other people in a court or judicial context, such as lawyers or witnesses. For the application of this exclusion to registrars and other courts officials, see *Ministry of Justice v S* (High Court, Wellington, CIV-2005-485-1138, 7 Apr 2006).

You may need to determine whether the respondent body or individual is a "tribunal" under the Act. The term "tribunal" essentially refers to statutory bodies with a judicial function (*Director of Human Rights Proceedings v Catholic Church for New Zealand* [2008] 3 NZLR 216). To determine, however, whether a body is acting judicially as a "tribunal" rather than administratively is not always easy. The key distinction is whether the activity is more judicial than administrative and takes into account a number of factors set out in the leading case, *Trapp v Mackie* [1997] 1 All ER 489.

There are also a number of other exceptions set out in section 8(b). For example, the Sovereign, Governor-General, House of Representatives, Members of Parliament in their official capacity, and the Parliamentary Service Commission are excluded. So too is an Ombudsman, and 'inquiries' (under the Inquiries Act 2013 or appointed under any other Act to inquire into a specified matter).

Our jurisdiction over intelligence organisations

What the Act says: Section 28, "Intelligence organisations"

"Information privacy principles 2, 3, and 4(b) do not apply to information collected by an intelligence and security agency."

Our jurisdiction over intelligence and security agencies – that is, the New Zealand Security Intelligence Service ("NZSIS") and the Government Communications Security Bureau ("GCSB") – excludes complaints under principles 2, 3, and 4(b). We also cannot issue an access direction or refer the complaint to the Director.

See also the specific exception in principle 10(2) that allows an intelligence and security agency to use personal information for a secondary purpose and the exception in principle 11(g) that permits the disclosure of personal information by any agency that believes on

[3] Section 4.

reasonable grounds that the disclosure is necessary for an intelligence and security agency to perform any of its functions.

If we do investigate an intelligence agency, the process ends with our Office. The complainant is not able to pursue the matter in the Tribunal (section 95).

Parallel jurisdiction with IGIS?

When we do have jurisdiction to investigate a complaint, check if the complaint "more properly" belongs with the Inspector-General of Intelligence and Security ("IGIS"). Usually complaints about access and correction "more properly" belong to the Office of the Privacy Commissioner, but other complaints may require consultation with IGIS before deciding where they "properly belong".

For more information see: Intelligence and Security Act amendments to Privacy Act: FAQs[4]

Other limits on our jurisdiction

The principles do not apply to personal information collected or held by individuals for their personal or domestic affairs (section 27) unless:

- the collection is unlawful (principle 4(a) continues to apply); or
- the collection, use, or disclosure of the personal information would be highly offensive to a reasonable person.

There are also a number of exceptions to the application of principles 6 and 7 set out in section 29. For example, an individual does not have a right to access personal information contained in an agency's correspondence with us where that relates to our investigation and was not in existence before the investigation commenced.

Other laws are also relevant and can operate as 'overrides' to the Privacy Act. Other laws may, for example, authorise or require information to be made available, or impose a prohibition or restriction on the availability of personal information. Also, if the action complained of is authorised or required by or under a New Zealand law, this will often operate as a limit on our jurisdiction (see section 24).

[4] https://privacy.org.nz/publications/guidance-resources/intelligence-and-security-act-amendments-to-privacy-act-faqs/

If we have jurisdiction, should we investigate?

Section under which the Commissioner has discretion to decline to investigate	Factors we would consider
S74(1)(a) The complainant has not made reasonable efforts to resolve the complaint directly with the agency concerned	What is reasonable – • Has it been brought to the attention of the privacy officer and/or complaints team at the agency? • Has the agency acknowledged receipt of the complaint and/or confirmed it is working on it? • How much time has the individual given the agency to respond? • What is the relationship between the complainant and respondent? • What are the complainant's circumstances? Are they vulnerable and/or is there a significant power imbalance? • Is the complainant represented by a lawyer or advocate? • If it is an allegation of a failure to respond to an access request, has the complainant followed up with the respondent? • Is it a sole trader/small agency and has the relationship broken down? • Have the parties reached a settlement? • Has the party suffered harm to meet the threshold in section 69 (apart from principles 6 and 7).
S74(1)(b) – alternative dispute resolution process because of membership of a particular agency/profession	Examples • Lawyer – Law society • Private Investigator – PSPLA • Health Practitioner – relevant registration board • Finance company – can search the Financial Service Providers Register to find out relevant resolution body (note - credit complaints about correction of credit reports, usually can't be addressed by these other bodies) • Bank – Banking Ombudsman • Telecommunications company – TDR • Utility company – Utilities Disputes • Social Workers Registration Board • Real Estate professionals - Real Estate Authority

Section under which the Commissioner has discretion to decline to investigate	Factors we would consider
S74(1)(c) There is an adequate alternate remedy (other than a right to petition the House of Representatives/Ombudsman), which it would be reasonable for the complainant to pursue	It can be difficult to try to facilitate a resolution to a complaint if the respondent is being asked to respond to similar facts in another forum at the same time. Rather than running a parallel process it may be preferable for the complainant to pursue both the privacy and other issues in one forum. While the other forum can't make a ruling on whether the Privacy Act was breached, it may be able to deal with the underlying facts in respect of the legal obligations it does have jurisdiction to determine. Access • If proceedings have been filed in the Employment Relations Authority ("ERA") or the Courts and the individual says they need the information for their proceedings, usually discovery or the ERA's powers to compel information would be an adequate alternate remedy. • Is the information predominantly company information? Is the respondent a lawyer/accountant – would a better remedy be access to a client file through their professional association e.g. NZLS/NZICA? (Could also be s74(1)(b)). Other complaints • The facts alleged to be a privacy breach are intertwined with a larger issue that is being or would be better addressed in another forum. • The complainant has a mediation scheduled in another forum (this may resolve the wider issue and even if the privacy concerns are not directly addressed, both parties may be able to move forward). This may be a temporary decline on the basis the complainant can come back if it is not resolved.
S74(1)(d) There is a complaints procedure in a code of practice, which the complainant has not taken reasonable steps to pursue	Codes of practice with a complaints procedure requirement for agencies: • Credit Reporting Privacy Code – Equifax, illion, Centrix. However, if it is a correction request, it is unlikely to be useful to refer a complainant back to the complaints procedure to ask the credit

Section under which the Commissioner has discretion to decline to investigate	Factors we would consider
	agency to review its own refusal to correct information. However, it may still be useful for simple processing errors/failure to respond. • Health Information Privacy Code – this includes Health NZ/Te Whatu Ora, Hospitals, GP's and other health practitioners, ACC, health insurers etc. • Telecommunications Information Privacy Code.
S74(1)(e) Complainant has known about the breach for more than 12 months	• Have they been trying to resolve it directly with the respondent? If yes, this may be a good reason to accept the complaint despite the delay. • Is it a serious breach? • Is it just outside the 12-month period and are there other factors that make an investigation necessary or desirable (e.g., public interest). • If yes to all of the above, we still need to consider whether an investigation would be practicable/fair to the respondent (e.g., are there good records, are relevant staff still available and likely to recall the circumstances). • Was the delay due to factors outside the complainant's control (e.g., health issues). • Was the delay due to professional advice (or the respondent) misdirecting complainant on whether a complaint to OPC was an option.
S74(1)(f) The time that has elapsed is such that a complaint is no longer practicable or desirable	Under this section the complainant may have only found out about the breach within the last 12 months, so the complaint might not be excluded by section 74(1)(e). However, notwithstanding this an investigation may no longer be practicable. Examples: • Availability of staff • Records of the breach – (was the breach verbal or written?) • Evidence/witnesses • Likelihood that circumstances can be recalled by individuals involved • Whether complainant made any attempt to address with respondent and if so, how soon after finding out about the breach.

Section under which the Commissioner has discretion to decline to investigate	Factors we would consider
S74(1)(g) Aggrieved individual does not wish to pursue the complaint	Essentially, the complaint is withdrawn: • If the complaint is brought by a representative, it may be appropriate to confirm during the investigation that the aggrieved individual still wishes to pursue the matter. • Important to note that a complainant who withdraws in order to pursue a complaint in the Tribunal may not be able to do so. Inform a complainant who seeks to withdraw in these circumstances of the risk their complaint could be struck out and suggest they seek legal advice (see *Gray v Ministry for Children,* Strike out decision).[5]
S74(1)(h) The complainant does not have sufficient personal interest in the subject of the complaint	• A complaint from an individual (rather than at the Commissioner's own initiative) would normally need to be brought by or on behalf of an aggrieved individual or individuals. Note that in order to find an interference with privacy the individual who is affected by the breach must be harmed by the breach. • If a complainant does not have a personal interest, consider whether the complaint raises sufficiently serious issues that other action would be warranted. Consider referring to the Compliance Advisory Board (CAB) to assess this.
S74(1)(i) The subject of the complaint is trivial	• Refer to the compliance pyramid in the CARAF.[6] • Consider whether there is any public interest. • Consider the impact/importance of the issue for the individual concerned.
S74(1)(j) The complaint is frivolous, vexatious or not made in good faith	• Consider the conduct of both parties. • Is the complainant genuinely seeking to address a privacy concern? • A complaint may be trivial despite being technically well founded/a breach – e.g., a request for review of withheld information that is trifling/already known to complainant. • Vexatious – for example the complainant has habitually and persistently made numerous

[5] *Gray v Ministry for Children* (Strike-Out Application) [2018] NZHRRT 13 (11 April 2018).
[6] https://www.privacy.org.nz/about-us/what-we-do/caraf/

Section under which the Commissioner has discretion to decline to investigate	Factors we would consider
	complaints or requests for reviews against the same agency with the intention to annoy or harass the agency or for some other improper purpose. • Bad faith - is the complaint made for an improper purpose or is it motivated by factors not related to privacy or accountability under the Privacy Act?
S74(2) It appears to the Commissioner that having regard to all the circumstances of the case, an investigation is unnecessary	• Refer to the CARAF. • Consider the broader public interest/benefit of an investigation. • Consider the nature of the breach and the seriousness of the harm. *Conduct of the parties* • Has the agency already acknowledged the breach and taken steps to prevent it happening again? • Has the agency provided a fair and reasonable response? • Has the agency already offered what we would consider a reasonable resolution? • Has the complainant provided false or misleading information? *Outcomes* • Is the remedy or outcome expected, or sought by the complainant unrealistic, unachievable, or trivial? (e.g., they want a professional struck off their register or an employee dismissed, which OPC cannot action). • Is an investigation unnecessary because OPC will be addressing the issue through an alternative compliance mechanism (e.g., there is an Inquiry underway, or we will issue a compliance notice instead), or it is clear that the information requested is subject to a withholding ground or that the action complained about comes within an exception. *Contact issues* • The complainant has failed to respond after a reasonable number of attempts to make contact or the complainant has failed to advise OPC of a

Section under which the Commissioner has discretion to decline to investigate	Factors we would consider
	new address and telephone number and is no longer reasonably contactable. • The complainant does not know or has failed to provide the name of the agency complained about and/or the name of the individual with whom they interacted. *Access Complaints* • Have we investigated the same or a similar request for this information previously? Did we review the withheld information/refusal decision? If so, another investigation may not be necessary. However, consider whether the relevant withholding grounds were time sensitive (e.g., a refusal because the information could be sought under the Criminal Disclosure Act, or maintenance of the law due to an open investigation, which may now be closed). • Has the information been released? If so, we might only investigate an alleged delay if the delay actually affected the individual. However, we may take other action instead (e.g. send a compliance advice letter to the agency to remind it of its requirement to respond if there was a technical interference). • Is it an access request prompted by an underlying privacy issue that it would be better to address directly either through investigation or other compliance activity?
Section 81(3) The Commissioner may decide during the course of an investigation that further action is not necessary or appropriate	We must have notified the parties we are investigating before we can use this section. This is essentially the same as s71(2) under the Privacy Act 1993 and we would use it in the same way. For example: • Is there a dispute of facts that further investigation is unlikely to resolve? • Does settlement appear possible? • Has the complainant expressed a clear intention to proceed to the Tribunal regardless of the outcome of the investigation? • Has the complainant rejected a reasonable settlement offer or has either party declined to willingly participate in a conciliation process?

If, in accordance with section 74, the decision is not to investigate, the complainant must be advised of that decision, with reasons, as soon as practicable (section 73(2)).

If a decision is made to discontinue an investigation (either because we are satisfied that one of the grounds set out in section 74 applies, or further action is unnecessary or inappropriate, the parties must be notified of that decision, with reasons, as soon as practicable (refer to section 81(3)).

Referrals to Ombudsman, Health and Disability Commissioner or IGIS

Section 75

If it looks like the complaint, or part of the complaint, belongs more properly with the Ombudsman, the Health and Disability Commissioner ("HDC"), the Independent Police Conduct Authority ("IPCA") or the IGIS, then we **must**:

- consult with the relevant agency without delay
- decide what to do
- refer the complaint, or the relevant part of it, to the other agency without delay if we think it belongs there
- notify the complainant that we've done this.

N.B: Our agreed transfer protocol with the IPCA includes a preliminary step of seeking the complainant's consent to transfer. Note, we do not have this with the Ombudsman or HDC.

Also, if the Protected Disclosures Act applies to the complaint, we must first consult the discloser and the intended recipient (the list of possible recipients is broader than the list above). Discuss with your manager.

When will a complaint "more properly" belong with the Ombudsman?

A complaint or part of it will, or may, fall more properly under the Ombudsman's jurisdiction in the following cases:

- **Official information** – it is mainly about official information, rather than personal information (it may be more appropriate for the Ombudsman to initiate the investigation then partially transfer any personal information to OPC if necessary).
- **Administrative action** – it is mainly about the reasonableness of some administrative action by a government body or official – for example, if the complainant is unhappy with the substance of a particular decision or with how they were treated. (Note that the Ombudsman does not have jurisdiction under the Ombudsmen Act for Police, unless it is a refusal to release information under the Official Information Act 1982 ("OIA"). Any Police complaint needs to be transferred to IPCA.)

Sometimes complainants (or their lawyer or advocate) may make a complaint about a decision or process under principle 8 arguments. Assess carefully to determine whether it is a complaint about checking information before use, or a broader complaint about

administrative fairness. It may be useful to consult on a possible transfer of such a complaint to the Ombudsman.

In some cases, it may be appropriate for our office and the Ombudsman to run parallel investigations, where we deal with the privacy aspect and they deal with the other aspect, and with the two offices keeping in touch during our investigations.

However, our two investigations will often be working to two different statutory timelines. Further, this will require the complainant to deal with two different investigating agencies.

Usually, however, it will be better for just one agency to deal with the complaint, according to the nature of the complaint and which agency can best address it.

When will a complaint "more properly" belong with the HDC?

Examples of where a complaint will or may more properly belong with the HDC include:

- **Physical privacy** – complaints about physical or bodily privacy rather than the privacy of health information. For example, a complainant may be unhappy about a doctor not closing the curtains of a cubicle before a physical examination. It is likely HDC would be better placed to consider a complaint about physical privacy under the Code of Health and Disability Services Consumers' Rights.
- **Ethical obligations & competence** – a complainant alleging a breach of the privacy principles by a doctor or other health professional may be mainly concerned about the health professional's competence in relation to their ethical obligations around patients' privacy and information. If the complainant's concern is not mainly about the consequences of the breach for them, about any harm, but rather with the doctor's ongoing conduct, then it may be more appropriate to have the case dealt with by the HDC.

When will a complaint "more properly" belong with IGIS?

The IGIS provides oversight of the activities of the NZSIS and the GCSB. These two agencies have wide-ranging powers that can affect the privacy of individuals, and the role of the IGIS includes ensuring that those powers are used lawfully and appropriately. The IGIS has substantial powers to access documents and information held by the SIS and GCSB.

Privacy complaints to the Privacy Commissioner about the NZSIS and GCSB may therefore be more properly within the IGIS's jurisdiction when they involve broader issues relating to those agencies' surveillance and information-gathering activities.

Referral to IPCA

The Office of the Ombudsman does not have jurisdiction over Police under the Ombudsmen Act, only under the OIA. This means the Ombudsman can review a refusal to provide information under the OIA, but the IPCA needs to consider a "reverse OIA" where a complainant complains about information that Police decided to release under the OIA.

IPCA also considers Police conduct more generally, this could include, for example, employee browsing, or issues with release of information through Police vetting checks.

Regarding the process, seek the complainant's consent to consult on a transfer first. For further details refer to our agreed transfer protocol.

Referrals to overseas privacy agencies

The Privacy Act: section 76

If it looks like the complaint belongs more properly with an "overseas privacy enforcement authority" then:

- we **may** consult with the overseas agency about this
- after any such consultation we **must** decide where the complaint should be dealt with
- if we think it belongs with the overseas agency, and if both the agency and the complainant agree, we **may** refer the complaint, or part of it, to the overseas agency.

If we decide to take action on a complaint, consider whether it can be dealt with as an "Early Resolution" complaint

In order to ensure we are dealing with complaints efficiently we have identified some types of files that will be dealt with through a more streamlined early resolution process.

Generally early resolution complaints can be created as an enquiry file in our system.

Early Resolution: No Investigation

The team member on incoming can consider whether we need to open a complaint file or an enquiry file for a complaint that on preliminary assessment we do not intend to investigate. Discuss the proposed approach with the Manager, Investigations & Dispute Resolution ("MIDR"), or a Principal/Senior Investigator. The investigator needs to ensure any relevant legal analysis of the issues is recorded on the file. This could simply be in the correspondence with the complainant.

Early Resolution

Sometimes we receive a complaint where it appears possible to resolve the matter without formally investigating. For example, a small agency might not understand its obligations under principle 6 and we consider a phone call to explain and give advice might be sufficient to resolve the complaint. Ensure you are clear with the parties whether you are attempting to settle the complaint under section 77, which will open a pathway to the Tribunal, or not. If you are simply making a preliminary enquiry to check whether the agency is open to addressing the issue without further action by the Commissioner, ensure both parties are advised of this. You can file this as an enquiry but ensure that you are capturing the complaint in the metadata (e.g. declined to investigate reason = unnecessary, outcome = info released/resolved).

Compliance Advice Letter

There will be some complaints where we may not consider investigation necessary, but some action is warranted. For example:

- The complainant wishes to raise issues but does not seek an investigation or facilitated settlement
- The complainant is not personally affected by the issue
- There is, or appears to be, a breach but no harm
- The complainant wishes to remain anonymous and the issue is broad enough the agency can consider it without their identity (e.g. a process/systemic issue, or a camera that is filming in a shared use zone). NB: a request to remain anonymous can sometimes signal a protected disclosure.

It might be appropriate to send a compliance advice letter or to relay our concerns to the agency in these circumstances. It may be appropriate to discuss this approach with the complainant first.

Although we cannot investigate an anonymous complaint as being an interference with privacy, it may be possible to accommodate a request to remain anonymous if we are sending a compliance advice letter. This would depend on whether we consider the agency would be able to act on the issue without knowing the identity of the person who brought it to our attention. If the complainant does not want to be identified or involved in the process, but we consider it is still an issue that warrants our involvement, the compliance advice letter should *not* include the complainant's name or other information which could reasonably identify the complainant.

Easy Access

A complaint about principle 6 will usually not require a detailed review or assessment before notifying. This means the complaint should be notified on receipt where possible. Some files may still need to be assigned for analysis first, or for an investigator to speak with the complainant to clarify the scope or issues, particularly if the individual has raised other privacy principles.

When assessing whether an access request can be notified immediately consider the following:

- There has been a specific, sufficiently detailed request for information (so it is clear what we can notify on).
- There is a copy of the request on file, or a copy of the response from the respondent which makes it clear the request has been made.
- The request was made more than 20 working days ago.
- Adequate contact details for both the complainant and the respondent have been provided.
- There are no "red flags" (e.g., repeat complainant which may require more detailed review of other files to ensure we aren't doubling up, other principles engaged, obvious health or comprehension issues that mean the complainant would benefit from a phone call or assignment to an investigator prior to notification, or any other matters that would make early notification without first speaking to the complainant/carrying out an assessment, undesirable.

Promoting conciliation and settlement

Overview

One of our key statutory functions is to try to settle complaints. We are therefore always trying – before, during and after any investigation – to reach a resolution of the complaint through some form of settlement.

OUR SETTLEMENT TARGET:

Our KPI is to settle **40 percent** of all complaints

Conciliation and settlement: Our statutory obligations and powers

Exploring the possibility of settlement and assurance without investigating a complaint

When assessing a complaint, consider whether settlement may be possible without first conducting an investigation pursuant to section 77.

Consider:

- Has the agency already acknowledged the breach?
- If the reason it has not resolved already is due to a dispute about the level of harm or quantum, proceeding straight to conciliation may be the most efficient way to resolve the complaint.
- Is there a clear or technical breach that does not appear to require investigation?
- Are the parties open to resolving their dispute in a conciliation?
- Has the agency or another regulator already investigated the matter and produced findings?

If there is a dispute of facts, or the agency does not consider its actions a breach, it is likely that an investigation would be useful before an attempt to settle. It could either assist the parties to have a more productive discussion if we first take some investigative steps or clarify whether there was in fact an interference that requires resolution.

If we cannot secure settlement, we can at that point either decide to investigate, or decline for either one of the reasons set out in section 74, or on the basis that investigation is unnecessary or inappropriate.

Obligation to promote settlement if a complaint has substance

If we do investigate and if we've concluded that the complaint has substance, we **must** use "best endeavours" to try to achieve a settlement.

For access complaints this is set out in section 91 and for other investigations, in section 94.

What does the "best endeavours" standard require of us?

The High Court has treated the "best endeavours" standard as being the same as "reasonable endeavours" *(see below)*.

> "A best endeavours obligation is a substantial one, reflecting the importance that the legislation attaches to settlement, but it also recognises that there is no single correct approach. There is much room for subjective judgement about how and when to promote settlement, and each case depends on its facts. … I think it appropriate to approach the issue by asking, as [the Commissioner] invited me to do, whether a reasonable Commissioner could have conducted herself as the Commissioner did here. That approach assumes that best endeavours is synonymous with reasonable endeavours, which need not be correct, but the assumption favours the Commissioner and I do not think anything turns on the distinction."
>
> *Henderson v Privacy Commissioner* [2010] NZHC 554 at [98]

The High Court found in that case the Commissioner did not use best endeavours to settle the complaint and could not have reasonably concluded that she was unable to secure a settlement when it was referred to the Director. The Commissioner had failed to advise the respondent of both an invitation to settle and a substantive settlement offer made by the complainant and did not consider calling a compulsory conference.

Promoting conciliation from the outset

As the High Court noted in the *Henderson* case, the scheme of the Privacy Act's complaints provisions requires us, from the very beginning of the complaints process, to be proactive in trying to resolve the complaint through conciliation. The Act makes it clear we can try to settle without investigating, and the individual will still have a pathway to the Tribunal.

> "… the Commissioner must be alert to the possibility that the parties may be willing to settle at an early stage, before the complaint has been investigated and before the Commissioner is able to offer any guidance on the merits; an obligation to promote conciliation and settlement arises at the outset."
>
> *Henderson v Privacy Commissioner* [2010] NZHC 554 at [101]

In line with that principle, we place a lot of emphasis on early resolution and settlement. Our aim is to settle complaints, if appropriate, after we've made an initial assessment and contacted the parties to clarify the issues.

In particular, a key question the Investigator will need to ask of the complainant very early on is what would resolve the complaint for them.

Tools we can use to try to reach a settlement

There are several tools we can use to promote settlement of a complaint:

1. First teleconference with the complainant and respondent
2. Case management conference
3. Power to call compulsory conference.

The Privacy Act gives us the power, under section 85, to call a compulsory conference of the parties, in order to try to resolve the dispute.

We can only invoke this power when we are investigating. We **cannot** use it if we are exploring the possibility of settlement under section 77.

We do **not** invoke this power when we convene a case conference at the start of an investigation. Case conferences can be held (usually by telephone) to clarify the issues in a dispute and work out a process and timetable for our investigation.

What the Act says: Section 85, "Compulsory conferences"

(1) The Commissioner may call a conference of the parties to a complaint by—

  (a) sending each of them a notice requesting their attendance at a time and place specified; or

  (b) by any other means agreed by the parties concerned.

(2) The objectives of the conference shall be—

  (a) to identify the matters in issue; and

  (b) to try to obtain agreement between the parties on the resolution of those matters in order to settle the complaint.

(3) Where a person fails to comply with a request under subsection (1) to attend a conference, the Commissioner may issue a summons requiring the person to attend a conference at a time and place to be specified in the summons.

(4) Section 159 of the Criminal Procedure Act 2011 applies to a summons under this section as if it were a witness summons issued under that section.

Settlements and "party autonomy": It's up to them

It's up to the complainant to decide what will resolve their complaint. We can make suggestions – such as an apology, a change in the respondent's processes, or compensation – but we can't require a complainant, or a respondent, to agree to any particular settlement.

If we conclude that the complaint has substance, we're then required by the Privacy Act to use best endeavours to secure a settlement.

Assessing the potential for a settlement

Complaints tend to be much easier to settle at an early stage and there is often a real willingness to resolve them on the part of both sides.

Some complaints simply won't be amenable to early settlement, even if the complaint itself seems to be a relatively minor matter.

This can depend on various factors, but often the indicators would include:

- a complaint where the parties' views and expectations are at opposite ends of the spectrum.
- a complainant with unrealistic expectations about the level of a monetary settlement.
- a respondent that is unwilling to accept and recognise a breach.
- parties whose behaviour towards the other is aggressive or inappropriate, where there is a significant power imbalance or safety concerns.

Giving guidance to the parties and managing expectations

Be clear about whether you are trying to facilitate a settlement under section 77, or whether you are investigating with an option of conciliation at any time.

The investigator's role includes managing the expectations of both sides in order to achieve a resolution that is acceptable to both. This process may include telephone diplomacy and negotiation, or face-to-face conciliation where the investigator meets with both parties or meets with each of them separately.

The investigator should have an overview of what would be a reasonable outcome in the context of the parties' expectations. We're not obliged to support any unreasonable expectations that a party might have and must ensure that we maintain our independence and impartiality at all times.

It's appropriate at all points of the process to provide the parties with reality checks about the effect of the law, the limitations of our process, and the potential consequences if a complaint isn't resolved through our process.

Specific settlement measures

Settlements will often include:

- an apology
- an assurance that the breach won't be repeated
- a promise to take action, like training staff and adopting privacy policies
- money, goods, services or other remediation
- an agreement to release information.

However, although those are common types of settlement outcomes, we've also seen a wide and creative range of measures over the years – for example, flowers, gift baskets and, in one case, an overseas holiday for the complainant and their partner. It's a matter of what will resolve the complaint for the particular complainant and respondent. (See Roth at PVA74.5 of Privacy Law and Practice for examples of settlements.)

The power of an apology

It's hard to overstate the significance that an apology can often have for complainants. If given in good faith and taken by the complainant to be genuine, it can go a very long way to resolving a dispute for them, by demonstrating to the complainant that their problem has been taken seriously and that the respondent agency will take real steps to prevent any repetition.

The Privacy Act now expressly protects apologies from being used as evidence against an agency in any civil proceedings brought under the Act (section 100). This is intended to support agencies to offer prompt, genuine and sincere apologies without concern as to how this may impact on their legal position if the complaint cannot be resolved between the parties. The ability for the Tribunal to take account of an apology when assessing remedies to be awarded against the agency has been expressly retained.

Giving guidance on financial settlement amounts

Although conciliation usually doesn't involve a financial settlement, we're often asked by the parties what would be an appropriate financial settlement for a particular complaint.

We don't give detailed guidance, as conciliation is about the parties' deciding what will resolve the complaint for them. It's also in the nature of privacy breaches that they vary widely, depending on the particular case, so it's difficult to assign a dollar figure to any particular breach. However, we can give the parties **examples** of specific settlements and the type or level of breach or harm in each case.

Guidance from Tribunal awards

Awards in the Tribunal will give some guidance about appropriate settlement awards.

For a useful discussion of Tribunal awards and relevant principles, see *Hammond v Credit Union Baywide* [2015] NZHRRT 6.

We also have information on our website that you can refer the parties to at any point of the process.

Investigations and determinations

Introduction

The Privacy Act gives investigators a significant amount of autonomy in handling complaints. Rather than a large number of detailed procedural rules, there are instead a relatively small number of significant legal checkpoints and boundaries – such as requirements to formally notify the parties when commencing an investigation and give the respondent an opportunity to respond to the complaint, and the requirement to seek comment before making an "adverse comment" (which will include any provisional finding that the respondent has breached a privacy principle or rule).

Subject to those checkpoints and boundaries (which are discussed further below), our investigators are empowered to make enquiries and reach conclusions about whether there has been an interference with privacy. The Commissioner expects them to exercise discretion, to tailor their investigation to what is needed to resolve the particular case, and to seek guidance from senior staff when necessary.

The investigator should tailor the process to the needs of resolving the particular complaint.

Natural justice and good decision making

Investigators need to comply with the public-law principles of procedural fairness and natural justice and have a reasonable basis for the decisions that they make.

These principles require our investigation processes be reasonable and fair to all parties, and our findings must have a reasonable basis (both factually and legally). Making sure that we inform the relevant party of our findings and the reasons why, and provide them opportunity to comment – even where the statutory "adverse comment" rule does not apply (for example, if we reach the conclusion that a respondent's decision to withhold personal information from the complainant was justified) – help to ensure that our processes are fair and the findings we reach are sound.

That does not mean that we always have to correspond with a party in writing or invite a written response from a party. In general, you should invite a written response only if:

- you are notifying the respondent of the complaint and advising them of their right to respond in writing; (discussed further below)
- you need more information, or
- you've made assumptions and you need to check that these assumptions are correct, or
- you anticipate making, or are proposing to make, an adverse comment about that party's rights or obligations.

If we've found that a respondent agency has breached the Privacy Act the statutory "adverse comment" rule will require us to present this to them in writing as a preliminary view and to invite them to respond in writing within a reasonable time.

If we've reached a view that a complaint doesn't have substance, the "adverse comment" rule is unlikely to apply (unless our view is based on a finding that is adverse to the complainant – for example, adverse credibility findings or findings of unreasonable complainant conduct). However, aways consider what the public-law principles of procedural fairness and natural justice require in any given situation – offering an opportunity to comment before making a final view will often be appropriate and need not be cumbersome nor add undue delay to the investigation.

The framework for your investigation

Identify the correct respondent/s

- It is for us to determine the appropriate respondent on a complaint, and it is important that we get this right as it can affect whether the aggrieved person can pursue an effective remedy in the Tribunal.
- Usually, identifying the respondent organisation will be straight-forward and the organisation will be the best agency to notify.
- However, from time to time it may be appropriate for us to also notify an individual employee, director, member, or agent. It is important that we identify this early and make an appropriate decision about whether to notify an individual in addition to an organisation.
- If you have any concerns about the correct respondent, talk to your senior, the MIDR, or the legal team.

Notification and the respondent's right to respond

- Once we have decided to investigate, we must notify the respondent and the complainant of this (*sections 73 (2)* and *80*). If the complaint is being made on behalf of one or more aggrieved individuals, or by someone other than the aggrieved individual, ensure that they are also notified appropriately.
- The notice to the respondent must set out the details of the complaint and we must provide the respondent agency with an opportunity to give a **written response** to the complaint within a reasonable time *(section 80(2))*.
- Your notification letter to the respondent agency should:
    - tell them that a complaint has been made
    - tell them who the complainant is and, if the complainant is different to the individual alleged to be aggrieved, the identity of the allegedly aggrieved individual
    - tell them what events we are investigating
    - tell them what privacy principles, or Code of Practice rules, are involved

    - ask them to respond in writing to the complaint
    - give them a reasonable time to respond to the complaint.
- When notifying an individual, you must include the information above and **also** tell them that they may be personally liable.
- If, in the course of your investigation, you are of the view that a different – or additional – principle or rule is relevant, you must notify the respondent of that, tell them they have the right to make a written response within a reasonable time, and you must then consider that response (see *DHRP [NKR] v ACC* [2014] NZHRRT 1, HRRT No 002/2012, at [29], [30]).
- Further, if you identify that the complaint (or part of it) may relate to a different respondent (or you believe now that it is appropriate to notify an individual employee, member or agent), you must notify that agency or individual in accordance with section 80.

Information gathering

- You should consider what information you need in order to reach a view on the complaint.
- Information requests can be made to the respondent in the initial notification. We can also request information from the respondent, complainant, or third parties throughout the investigation process.
- It is a legal requirement to comply with an information request made under section 87. We must extend any time limit for complying with a section 87 notice if one of the grounds in section 87(3) applies (section 87(5)).

Burden of proof

- The Privacy Act doesn't assign any evidentiary burden to a particular party, and the High Court has held specifically that the respondent does not have the burden of establishing that an exception applies (see *Henderson v Privacy Commissioner* [2010] NZHC 554).
- However, if we ask a respondent agency for evidence of their assertion that an exception applies, but they refuse to engage with us or don't give us the information, we're entitled to form a conclusion on the basis of the information we have. If in that case we find that the alleged action or omission *did* occur, but we have insufficient information to conclude that an exception applies, then we are entitled to conclude that there has been a breach.

Promoting conciliation and settlement

- Our obligation to promote conciliation and settlement continues throughout the investigation.
- If we think it may be possible, we **may** use "best endeavours" to settle the complaint at any time during the investigation (section 83).

Timeliness

- We are required to conduct the investigation in a timely manner (section 81).
- Always ask for responses to be provided by a certain date.
- If an agency or an individual cannot respond within the timeframe provided, we may give an extension (and must give an extension to a section 87 request if any of the grounds set out in section 87(3) apply). Any extension should be for no more than a reasonable time. We can't keep files open indefinitely.

Right to be heard before any "adverse comment"

- If our assessment is that the complaint has substance (or we are proposing to determine an appropriate charge, issue an access direction, refer the complaint to the Director, or to an appropriate authority), we **must** give the respondent a chance to respond to this before we reach a final view and notify the parties of our determination (section 210).
- To discharge the "adverse comment" obligation, we should:
    - notify the party in writing of our preliminary finding, including our reasons for it
    - invite them to respond in writing
    - give them a reasonable time to respond.
- If our assessment is that a complaint doesn't have substance, the "adverse comment" rule is unlikely to apply (unless our view is based on a finding that is adverse to the complainant – for example, adverse credibility findings or findings of unreasonable complainant conduct). We must still consider what the public-law principles of procedural fairness and natural justice require – offering an opportunity to comment before making a final view may be appropriate and need not be cumbersome nor add undue delay.

Discontinuing an investigation

- We may decide to discontinue an investigation if we are satisfied there would have been good grounds to decline to investigate under section 74, or if further action is unnecessary or inappropriate (section 81(3)). An overview of the section 74 grounds is set out earlier in this guide.
- Further action may be unnecessary or inappropriate if:
    - the complaint is settled between the parties.
    - the complainant fails to respond to our routine investigative enquiries and the deadline we gave the complainant for this has passed (we should make it clear that we may discontinue if we do not get a response).
    - the agency has made the complainant a reasonable offer but the complainant has rejected it.
    - resolving disputed facts would be difficult and time-consuming and to little advantage, or resolving the facts may not even be possible at all.
- If we decide to discontinue an investigation, we must notify the parties of this and provide reasons (section 81(4)).

Notifying the parties of our findings on the complaint

- As soon as practicable after the investigation is finished, we must tell the complainant and respondent what the result of the investigation is and why - (Do we think that there has been an interference with the privacy of an individual or not? What is the basis for our findings?), and about any further action we propose to take (Sections 91, 93, and 94).
- **Remember**: do not copy correspondence from one party to the other.
- Where this notification triggers the six-month limitation period for commencing proceedings in the Tribunal, we should advise the parties of that. We provide "section 98" notices to complainants as set out below.

Obligation to use best endeavours to secure a settlement and assurances

- If we determine that a complaint has substance, we **must** use our "best endeavours" (reasonable efforts) to secure a settlement (section 91(2) and (3), and section 94(2) and (4)).
- We **must** also seek an assurance from the respondent that the breach won't be repeated (section 91(4), and section 94(3)).

Other determinations and reporting significant breaches of duty or misconduct

- If settlement is not reached, depending on what the complaint is about we may:
    - determine an appropriate charge on a charging complaint (section 93(2)).
    - issue an access direction on an access complaint (section 91(5)(a) and 92)).
    - refer the complaint to the Director.
    - take other appropriate action (section 91(5)(c), section 93(6) (if the charge is not reduced), section 94(4)(b)). This may include, for example, a warning or compliance advice letter, referring the matter to another agency, or making public comment (any decision to name an agency must be made in accordance with OPC's naming policy).
    - take no further action on the complaint and close our file.
- We **must** report any significant breaches of duty or misconduct to the appropriate authority (section 96).

Closing our file

- Our communication to the parties that we will be taking no further action or we have reached the end of our process will impact the complainant's ability to take proceedings in the Tribunal and the respondent's ability to file an appeal to an access direction.
- There are specific legislative time limits, so we need to ensure our records are accurate and our correspondence is clear.

- You must inform the complainant or the respondent agency (for an access direction) of the timeframe to take proceedings in the Tribunal when you give notice that you are closing the file. (Note, this only applies where we have notified the parties – if we declined to either investigate or try to settle then they have no pathway to the Tribunal.)
- You must also ensure you provide the complainant with a "section 98 notice" and in your correspondence with both complainant and respondent advise of the section you are notifying your decision to take no further action under.
- The section 98 notice can be sent as an email or a letter. Bear in mind the complainant must submit this notice to the Tribunal if they file proceedings. For that reason, it is probably preferable that the notice is separate from your substantive view, particularly if you are discussing sensitive information (e.g., harm, matters not included in the investigation or findings that go against the complainant).
- Once you have closed the file, consider whether others could learn from this case. We have a number of avenues to disseminate learnings and key messages to others, such as case notes.