Complaint or privacy breach: how do we deal with your enquiry?

This information sets out how our Compliance and Enforcement team triages systemic privacy issues raised with our Office.

	Privacy breach	Interference with a person's privacy
	A privacy breach under Part 6 of the Privacy Act 2020 focuses on whether there has been any unauthorised access, loss, or disclosure of personal information. A **notifiable** privacy breach occurs when the breach has, or has the likelihood, to cause serious harm to the people whose personal information has been impacted. This requires notification to the individuals impacted and to OPC.	Part 5 of the Privacy Act sets out how OPC will deal with a complaint from an individual about an **interference with their privacy**. This usually involves the breach of an information privacy principle and may require you to have suffered harm. These complaints, including about getting access to or correcting your own information, are dealt with separately by our Investigations and Dispute Resolution team. Read more about that process.
Which OPC team is involved?	Our Compliance and Enforcement team deals with notifiable privacy breaches and systemic privacy issues raised with our Office.	Our Investigations and Dispute Resolution team deals with an individual's complaint about their own privacy rights.
What if my case is both types of issue?	Although the two things can be related, they are separate, and decisions we make about how to respond to a privacy breach notification or other systemic issue does not prevent us from investigating a complaint from an individual about the same issue.	
For example	The Compliance and Enforcement team may assess that we do not need to take any enforcement action on a privacy breach notified to OPC.	The Investigations and Dispute Resolution team may still decide to investigate an individual's complaint that there was an interference with their privacy.

Step one: we receive a concern or enquiry about the way an organisation is handling personal information

For example:

"Dear OPC. I am concerned that ABC Limited is breaching the Privacy Act because their website is disclosing sensitive personal information. Please investigate it."

An enquiry like this will be managed by the Compliance and Enforcement team.

If your enquiry said that you were concerned that the website was disclosing information about you personally, this would be dealt with by OPC's Investigations and Dispute Resolution team.

Protected disclosures

If you raise a serious concern about your own workplace, you may be able to make a protected disclosure under the Protected Disclosures (Protection of Whistleblowers) Act.

Step two: Deciding how to address a concern

The Compliance and Enforcement team assesses each concern under OPC's Compliance and Regulatory Action Framework. This sets out how we prioritise to deliver the best privacy outcomes for the greatest public benefit with the resources we have available.

The Framework sets out the factors that we consider when deciding how to address a complaint or enquiry. These include:

- The nature and seriousness of a privacy issue, or potential impact including:
  - the harm caused, or likely to be caused, to the affected people
  - whether the matter involves sensitive information
  - the number of people potentially affected
  - whether disadvantaged, vulnerable, or a particular group of individuals may be adversely affected
  - whether there is an indication of a systemic issue, for example across a particular agency or sector.
- the level of public interest, or the educational or deterrent value of taking action
- the attitude and conduct of the agency concerned, including previous compliance
- statutory factors under the Privacy Act (the Act), including the requirement to take cultural perspectives into account

- the proportionality and appropriateness of taking regulatory action by investigating or making initial enquiries
- any other factors that OPC considers relevant in the circumstances.

Notifiable privacy breaches

Alongside the Compliance and Regulatory Action Framework, we may consider whether there was a privacy breach that should have been notified to us. As part of that, we consider the if the agency has reasonably assessed the likelihood of serious harm. The factors an agency must consider when assessing whether the breach is likely to have caused serious harm are set out in section 113 of the Act.

Types of serious harm include emotional and psychological harm, financial harm (including fraud), physical harm or intimidation and identity theft.

Why we may not take any action

We cannot address or investigate every complaint or concern received. The varied nature of factors at play may mean that similar issues have different levels of privacy risk and result in different decisions by our team.

Some of the reasons we may not take any action include:

- there is no evidence of serious harm occurring or being likely
- there is no sensitive personal information at risk
- the cause of the concern has already been resolved or contained
- the issue lies outside the scope of the Privacy Act e.g. commercial information or code of conduct issues.

Step three: Letting you know what we're doing

If we think that your issue is better addressed by the Investigations and Dispute Resolution team, we will refer it to them to assess. You will hear from either team about the outcome of your enquiry.

We may seek more information from you, such as finding out how you became aware of the issue, and any documented evidence you might have.

We will tell you whether the Compliance and Enforcement team is going to formally review the concerns raised, or if we are not intending to take any action based on the information

provided. We can't tell you what that action will be, won't provide you with updates about this and are unlikely to let you know about any outcomes of our work.

This is because section 206 of the Act requires us maintain secrecy about all matters that come to our knowledge as part of our work. We sometimes make public comments about the outcome our investigations, but we do not provide comments or information to others.

Step four: Further action and outcomes

If we decide further action is warranted, we may make initial enquiries with the agency involved. For example, we might ask if they are aware of the issue raised and what they have done in response. Our early information requests are made on a voluntary basis as we aim to work alongside the agency to understand the issues of concern.

We may also use other sources such as publicly available information and media releases.

Our initial information gathering will inform our assessment of the issue and guide our next steps which may include:

- working with the agency to provide education and guidance on their specific issue
- issuing general guidance on our website aimed at a specific sector or common issue
- commencing a formal investigation or inquiry.

Whichever action we decide to take, we aim to ensure that the privacy practices at the agency are improved to the point that the personal information it holds is adequately protected for the future.

We may initiate a formal investigation or inquiry where we consider there may be systemic issues occurring within an agency or sector, or the matter has failed to be resolved through lower-level interventions. These investigations also engage the Privacy Commissioner's powers to require information to be provided and to summons individuals and question them under oath.

Sometimes these investigations or inquiries result in the publication of a report, a compliance notice being issued or public comment being made about the agency and the issue considered in a media statement or decision note. Any public comment we make about a specific agency is made in line with OPC's Naming Policy. These outcomes are intended to provide lessons learned across sectors and agencies, not just to the agency involved in the investigation.