



Australian Government

Office of the Australian Information Commissioner

Creating an Enquiry in response emails about lodgement of a new privacy complaint

When a complainant emails the OAIC seeking to lodge a complaint, there is often information missing and required documentation that would otherwise be obtained via the online lodgement process. This includes the important step that, if lodging via email without the manual complaint form, the complainant has not meet the requirements of the Privacy Act to lodge a valid complaint, and they have not provided the required consent to the OAIC for us to use their personal information.

As a result, emails of this nature are lodged as an enquiry with a standard email sent to the complainant advising of the steps they are to take to lodge a complaint.

Before actioning an email, please search the OAICIntake@oaic.gov.au mailbox to see that you have all correspondence from the complainant on this matter. Also conduct a Resolve search to ensure there is not already a complaint registered.

Creating an enquiry in Resolve

Select Find Client in the ribbon header on the homepage to search for the complainant. This will open the Search for Client window.

Use the Display Name field to put in all or part of the complainant's name noting the naming convention is Surname, Firstname. If a match is in the system, it will appear in the lower half of the window.

If a matching entry is found, click on it to open the Client Entry window and select New Case then General Enquiry.

If no entry is found for the complainant, you need to create a profile before you can create a new complaint. Use the New Client profile button to open a New Client – Client Entry screen

Complete all relevant information in the client entry and Save

This will enable you to select New Case and select General Enquiry

Complete the following:

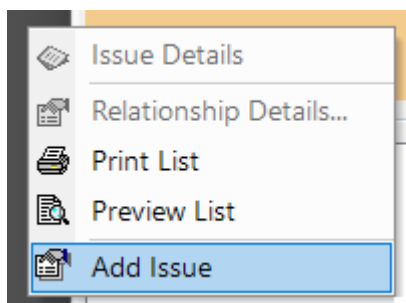
- How Received – select email from dropdown menu
- Enquirer Industry Sector – select individual from dropdown menu
- Target Industry Sector – select most relevant to respondent / industry E is enquiring about

Important: You will need to change the Received Date to reflect the actual date of the email. It will default to today's date.

In the Summary field, provide a brief description such as Seeking to lodge privacy complaint via email. See attached documents for correspondence

At this point you will need to save the Enquiry to get the remaining information to load (such as Case Number) and to enable you to add issues and finalise the Enquiry

Right click in the 'Issues' field at the bottom of the window and select 'Add issue'.




Select the Issue Description. If there is enough information to determine which APP applies, that should be your selection. If there is not enough information to identify the nature of the complaint, select Privacy Principles > APPs > Privacy Generally

select the Outcome as advice given – complaint procedure

You now need to email the complainant to advise of the steps they need to take. Once the email is sent, upload it and the complainant's original email to the OAIC to the documents tab of the Enquiry.

To finalise the Enquiry, work your way through the Open Actions by ticking the box to the left of the text. This will progress you through the actions to closure, including allocating the matter to yourself.

Action Name	Due Date
<input type="checkbox"/>  Record case details and attach documents	20-May-2025

Email content

Title: Your privacy concerns about **RESPONDENT NAME** (EN2X/XXXX)

Dear **Enquirer first name**

Thank you for your email below in relation to privacy concerns you have about **RESPONDENT NAME** (respondent).

Unfortunately we are currently unable to progress your matter as a privacy complaint as we require further information from you. You are requested to follow our complaints process to ensure that we obtain the required information. Further, as the OAIC has its own obligations under the *Privacy Act 1988* (Cth), we need to ensure you are adequately notified of and provide consent in relation to how your personal information may be used and disclosed.

We ask that you lodge your complaint on our online [privacy complaint form](#). By using this form you will also be able to upload the documentation we will require to assess your complaint. It is important to note that you must include a copy of your complaint to the respondent and the respondent's response (if available). Without this information we will be unable to progress your complaint.

Please note: If the respondent is a member of a recognised [external dispute resolution \(EDR\) scheme](#), you should lodge a complaint with the EDR in the first instance. If this step is not undertaken, we are likely to decline your complaint. If you have already undertaken this step, remember to upload your complaint to and response from the EDR.

You will receive an automatic acknowledgement and complaint reference number on completion of the online form. You can use this reference number in future communications with the OAIC about your complaint.

Important information

The OAIC has the power to investigate privacy complaints about [entities that are covered](#) by the *Privacy Act 1988*. However, section 40(1A) of the Privacy Act states that, unless appropriate, the Commissioner **must not** investigate a complaint if you did not firstly complain directly to the respondent.

If you have not taken the step to complain to the respondent before lodging a complaint with us, we are likely to decline your complaint until that is done.

More information about the complaint process can be found on our website:

[Complain to an organisation or agency | OAIC](#)

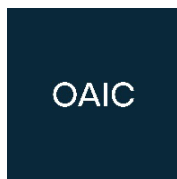
[What you can complain about | OAIC](#) and

[Lodge a privacy complaint with us | OAIC](#).

Your contact with us has now been finalised as an Enquiry with reference **EN2X/XXXXX**. Please quote this reference at the time of lodging your new complaint.

Yours sincerely

Your first name



Intake and Triage Branch

Office of the Australian Information Commissioner
Melbourne | GPO Box 5288 Sydney NSW 2001
P 1300 363 992 |

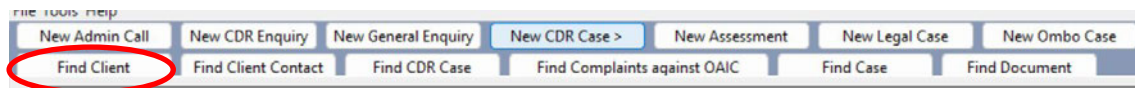


Creating a new Privacy Complaint

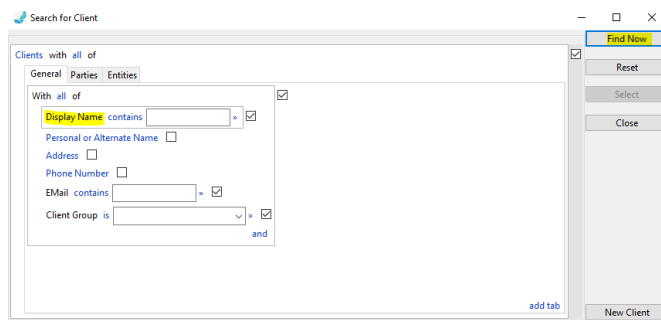
Manual privacy complaint entries are required where a complaint is lodged via email, post or fax.

To create a new Privacy Complaint file, you first need to create or select the complainant's profile

Not all options shown here will be available in your ribbon

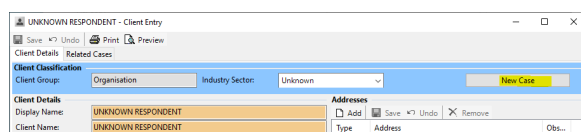


Select Find Client in the ribbon header on the homepage to search for the Applicant of the Privacy Complaint. This will open the Search for Client window.



Use the Display Name field to put in all or part of the complainant's name noting the naming convention is Surname, Firstname. If a match is in the system, it will appear in the lower half of the window.

If a matching entry is found, click on it to open the Client Entry window and select New Case then Privacy Complaint.



If no entry is found for the complainant, you need to create a profile before you can create a new complaint. Use the New Client profile button to open a New Client – Client Entry screen

Complete all relevant information in the client entry and Save

This will enable you to select New Case Complaint and select Complaint Type Privacy

You now need to register the respondent

Select the Find button next to the blank Respondent Name field

This will open the search function within Resolve. Use all or some of information provided by the Complainant in the Respondent Name field.

If the named client does not exist, you need to establish the legal entity that is the subject of the complaint. You can do this by:

- Checking the correspondence between the complainant and respondent (if provided). The entity name may be identifiable by the respondent's correspondence.
- Going to the webpage of the respondent and looking at their Privacy Policy. The opening paragraphs of the policy should show the legal name and, if they are known by another name, that second name. Either of those names may match the information provided by the complainant.
- An [ABR search](#) for a matching entity. This may return a legal name that is different to the name used by the complainant however the profile for the ABN should also reference the trading name used.

If the respondent has a business name that is different to the trading name, you should only register the legal name. The trading name can be added in the Alternate Names field to enable Resolve to search on the variations. This is important particularly for sole traders who have a legal name such as Surname, First name but a trading name of First name Surname.

If the respondent listed is an individual who is not a sole trader, DO NOT create a new client entry for this case. Use the existing Resolve client UNKNOWN – Individual. This will ensure that the respondent sector field is populated so that the case can be progressed past the assessment stage in the workflow.

This also applies when the respondent is not listed or is listed as 'unknown'. Use the existing Resolve client for that industry sector. E.g. *UNKNOWN – Retail*

If you need to create a new Respondent,

The screenshot shows a web application interface for searching clients. The main area is titled 'Clients with all of' and contains a search criteria box. The search criteria box has a tabbed interface with 'General', 'Parties', and 'Entities' tabs. The 'General' tab is active, showing a search criteria box with the following fields: 'Display Name contains' (with a search icon), 'Personal or Alternate Name' (checkbox), 'Address' (checkbox), 'Phone Number' (checkbox), 'EMail contains' (with a search icon), and 'Client Group is' (with a dropdown menu and a search icon). The search criteria box is followed by an 'and' connector. To the right of the search criteria box is a vertical sidebar with buttons: 'Find Now', 'Reset', 'Select', and 'Close'. At the bottom right of the sidebar, the 'New Client' button is circled in red.

Select relevant option (either org or agency) in the Client Group in the top banner – **this option CANNOT be changed** after this record is saved, so please select the correct option here

Client Classification
 Client Group: Organisation Industry Sector: Unions
Client Details
 Display Name: s22
 Alternate Names: Add Edit Remove
 Client Name: s22

Once added, open the respondent entry from the details you have including sector, correct entity name and abbreviations

Add industry sector

Classification
 Group: Organisation Industry Sector: Unions
Details
 Display Name: s22
 Alternate Names: Add Edit Remove
 Client Name: s22

If privacy policy states that R is bound by; required to comply with; or covered by (or other similar words) the Privacy Act, change the Privacy Act field to covered, and add a comment that includes the details from the privacy policy

Preferred Method of Contact:	Email
FOI Act:	Not covered
Privacy Act:	Covered

Add contact details provided in privacy policy (if available), or on website

Phone (BH):	s22	Phone (AH):	
Mobile:		Fax:	
Email Address:	s22		
Website:	s22		
Other Contact Details:			

Save the client using the save button at the top of the screen. This will return you to the Main screen and insert the new respondent

Completing case information

Toolbar

Header

Tabs

Header Information

The Header is the most important information about the case, including the type of case, the case number and which investigator the file is assigned to. Check that each of the fields is completed, noting that anything in yellow indicates it is a mandatory field.

Description	
Complaint Type	Options: <ul style="list-style-type: none"> Privacy
Method	This field is automatically completed by workflow actions and indicates the method used to complete the complaint while open and upon closure. <ul style="list-style-type: none"> To be determined – a new Privacy Complaint defaults to this method and is updated to as you move through the workflow. Preliminary Inquiry Investigation Decline
Case Type	Defaults to Primary

Description	
File security	This at is set manually to OFFICIAL which defines the security level of the physical file.
Case Number	Automatically populated on the first save of the case record.
Case Officer	This will default to the person who has created the record.
Target Date	Automatically populated for 3 months from the Complaint Date.
Stage	<p>This field is completed by workflow actions and indicates the stage of the complaint while open and upon closure.</p> <ul style="list-style-type: none"> • s.44 adhoc • Registration • Mail assessment • Preliminary Inquiries • Investigation • Finalisation • Close
File holder, destruction, and retention class	Automatically completed.
Start next stage	This should not be used as stages are updated by the workflow.
New related process	This is used when a related case type is required. This is not something that needs to be used during the creation of a record.
Move file	No longer used

Main tab

The Main tab is the front page of the case and shows a summary of important information.

Note: highlighted text is not available in a new complaint until Privacy is selected as complaint type

Description	
Complainant Details	This shows the name of the complainant as selected via the steps above. This section can also be used to open the complainant's contact page by clicking 'Open'.

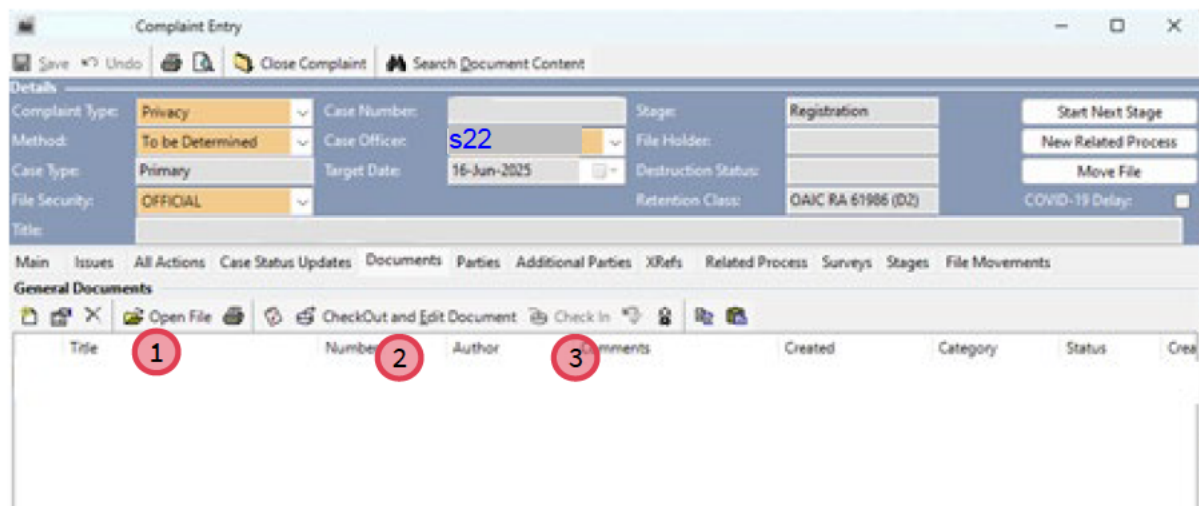
Description	
Respondent Details	This shows the name of the respondent and a relevant contact point if one has been added. This section can be used to open the respondent's contact page by clicking 'Open'. A contact point can be added by clicking on 'Find'. Further contact information will also be shown in this section
Agency Reference Number	This is not used
Received Date	Date the privacy complaint was received by the OAIC. It defaults to the date you have created the record and needs to be manually adjust to reflect the actual date received.
How received	Select the source of how the OAIC became aware of the matter.
Registered by	Defaults to the Case Officer at time of initial save.
MOU Flag	Select the appropriate values if the complaint relates to <ul style="list-style-type: none"> • My Health Record • Healthcare identifier • USI Registrar
Complained to R	You will need to read the complaint to determine this answer: <ul style="list-style-type: none"> • Yes • No
ER next step	Not needed during complaint registration
ER Commenced	Not needed during complaint registration
ER Outcome	Not needed during complaint registration
ER Outcome Date	Not needed during complaint registration
SmartForm number	This is automatically populated if the form is received via the submission of a form
Referral Source	Complete this if the complainant was referred to the OAIC. Select from: <ul style="list-style-type: none"> • PCEHR System Operator • State/Territory privacy regulator • State/Territory health regulator • Ombudsman (Cth) • Other
EDR Used	This is a mandatory field and indicates if the complainant had previously complained through the EDR scheme. Select from: <ul style="list-style-type: none"> • Yes • No <p>If yes, insert the name of the EDR used</p>

Description	
Code flag	<p>This field indicates if the complaint involves a Code. Select from:</p> <ul style="list-style-type: none"> • Australian Govt Agencies Privacy Code • Credit Code • Market and Social Research Privacy Code
PIC Assigned Officer date	Not needed during complaint registration
PIC Privacy Outcome Date	Not needed during complaint registration
PIC clock elapsed days	Not needed during complaint registration
Significant Incident	If this complaint relates to a significant incident such as a major data breach or a Commissioner Initiated Investigation (CII), select the appropriate incident
Complexity	<p>Select from:</p> <ul style="list-style-type: none"> • Low • Medium • High <p>Unless otherwise advised, Low should be selected</p>
Sensitivity	<p>Select from:</p> <ul style="list-style-type: none"> • Not sensitive • Media Interest • Member of Parliament • Ministerial • Safety concerns • Time critical • Whistle-blower <p>Unless otherwise advised, Not sensitive should be selected</p>
Note	Used through the life of the complaint to provide a brief indication of the status of the complaint
Next Action due date	The date this will be used to help monitor actions undertaken
Next Action	Used through the life of the complaint to provide next step
PRV Status	Not needed during complaint registration
PRV Outcome	Not needed during complaint registration
Summary	<p>This has an overview of the case for example it may contain a summary of the allegations and relevant APPs.</p> <ul style="list-style-type: none"> • Brief summary of the Complaint • Brief summary of actions taken • Any items of note • Keywords in summary (if applicable)
SmartForm Details	Automatically populated by the smartform on lodgement

Description	
Open Actions	Each action represents a step in a process that has been programmed into Resolve. This section displays all outstanding actions associated with the Privacy Complaint and allows the investigator to tick off steps in a process as they are completed. For example, a call that needs to be returned will appear as an uncomplete action and can be ticked as completed when that call has been made.
Issues	This section shows which provisions of the Privacy Act are relevant to the case. At the completion of the case, outcomes are added to each issue to show how each element has been resolved.

Documents tab

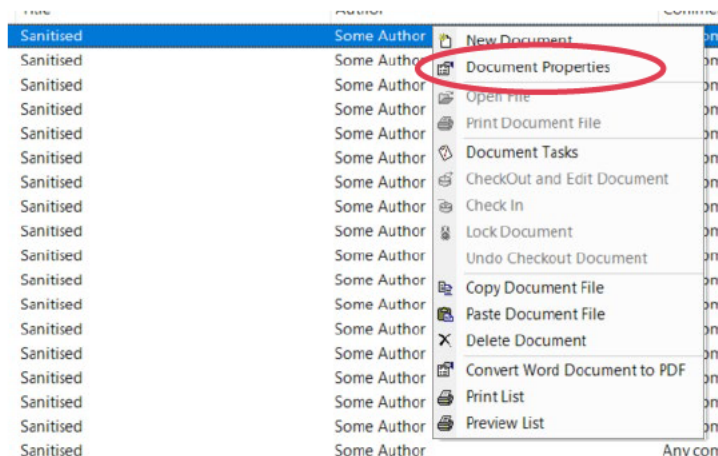
The Documents tab is where all documents relating to the case are saved. Copies of correspondence sent and received will need to be added to this tab. If generated correspondence via the action/task button (explained below), they will automatically appear here. Documents can be manually added by dragging and dropping files into the white space on the or copy and pasting files.



Description	
1. Open file	Read only copies of documents can be opened by clicking 'Open file' or by double clicking on the document. If you need to edit the document, use CheckOut and Edit Document
2. CheckOut and edit Document	To edit a document, you will need to click 'CheckOut and Edit Document' or right click on the file and select 'CheckOut and Edit Document'. No other user will be able to open and edit that document while it is checked out to you. You are unable to edit an uploaded document any other way
3. Check In	When you have saved and closed the edited document you will need to select 'Check In' or right click the document and select 'Check In'. <i>It is important to always check documents back into Resolve when you are done with editing them so other users can access them. If you don't check them back in you are at risk of losing them when you shut down/restart your laptop</i>

Document Details

More details about a document can be found by right clicking on a specific document and selecting document properties.

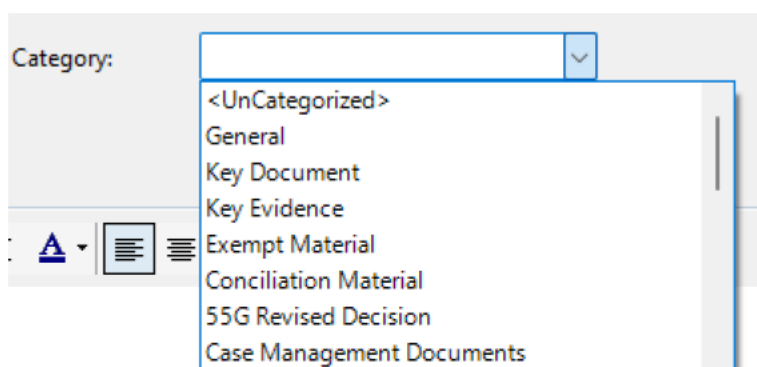


This will open a dialogue box that will enable you to edit the Document's title or enter a comment. Document titles should be reflective of the nature of the correspondence.

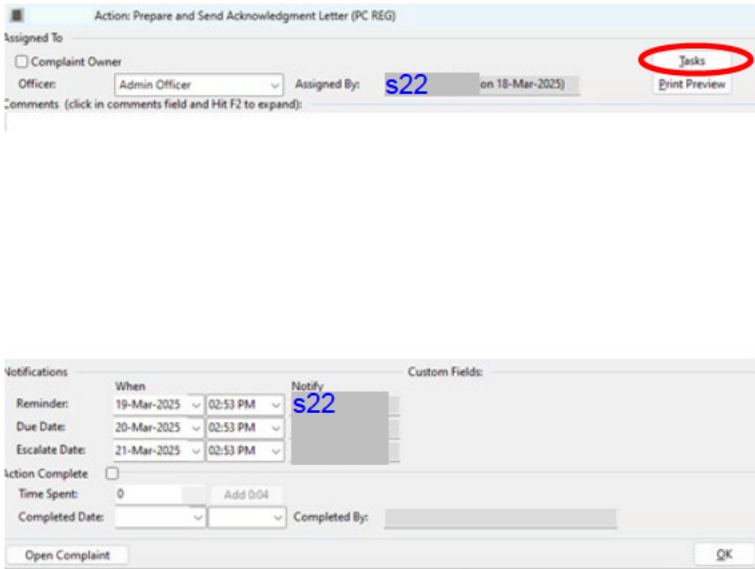
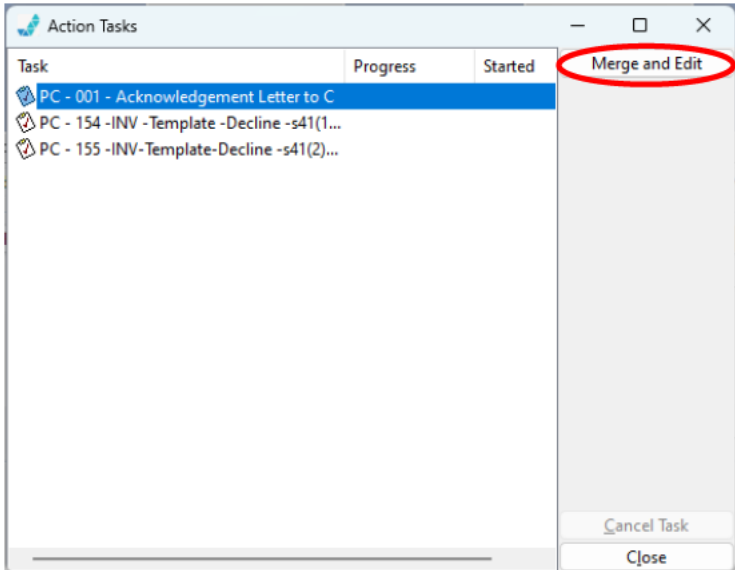
In this example, the original complaint was lodged via Post so the title reflects that

A screenshot of the 'Document Properties' dialog box. The 'Title' field is filled with '12 March 2025_Original complaint lodgement'. Below the title are tabs for 'Details', 'History', and 'Related To'. Under the 'Details' tab, there is a checkbox for 'Electronic (Computer Based) File' which is checked. The 'File Name' field contains '12.03.2025 - OAIC Intake.pdf'. The 'Author' field is empty. The 'Created By' field contains 's22'. The 'Created' field shows '18-Mar-2025' and '02:19 PM'. The 'Registered' field shows '18-Mar-2025' and '02:20 PM'. The 'Category' dropdown menu is open, showing 'Key Document' selected, and this dropdown is circled in red. At the bottom, there is a 'Comments' section with a rich text editor toolbar.

Document properties also enable you to categorise documents. The category selected appears as a column in the document list which allows you to sort to locate documents assigned a particular category. Privacy complaint categories are:



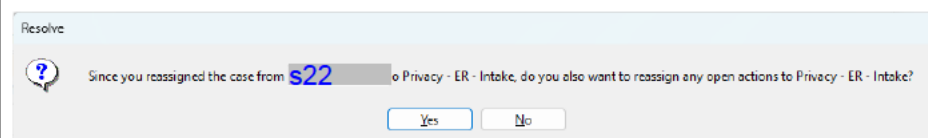
Complaint registration workflow actions

Description	
Register Case (PC REG)	<p>This action prompts you to record the case details. At this point you should complete all the available information into the Main tab noting that orange fields are mandatory to enable you to save the case. On saving, the Privacy Complaint will be allocated to you.</p>
Prepare and Send acknowledgement letter (PC REG)	<p>Open this action by double clicking on it. Select the Tasks button then the Acknowledgement Letter to C option. Press the Merge and Edit button and the recipient will appear based on the complainant information entered in the Main tab. The template will then populate in Microsoft Word using the remaining information you have entered on the Main tab. You can edit the letter as required, save it (use the X button on the top right of Microsoft Word) and check it back in via the Documents tab.</p>  

Description

Move to 'Privacy - ER - intake' basket (PC REG)

Once registration is finalised and you have sent the acknowledgement letter, complete this task. The case will be assigned to the Privacy - ER - Intake queue. A pop up will appear asking if you want to assign all open tasks to this queue also.



Selecting yes will complete this task and kick off the next stage of the complaint, Allocate complaint



Australian Government

Office of the Australian Information Commissioner

Making requests for information

Requests for information to the complainant are sent to obtain one or more of the following:

- A copy of the privacy complaint to the respondent and the respondent's response
- A signed authority to act (referred to as AtA or A2A) form if a representative has been nominated and no authority has previously been provided by the complainant
- Any other information that is relevant to the complaint.

1. Check the documents tab to ensure that the required information has not been provided since the assessment
2. If the document/s are required, complete the template email request by **deleting irrelevant dot points and filling in the date of the complainant's complaint**, and send to the complainant
3. If the contact is over 8 months old, amend the response timeframe to 14 days
4. Update:
 - the note field to 'Information requested'.
 - the next action date to the day after the response is due from the complainant
5. Upload the sent email to the documents tab
6. Right click on the email in the documents tab and click properties – rename the title to Email to C – Request for information
7. Go to the sent items of the oaicintake inbox and drag the email to the 'Email to C' folder

Email content

Email title: Information required to progress your contact with the OAIC (CP2X/XXXXX)

To firstname

Thank you for your contact with the OAIC in relation to concerns you have that XXX (respondent) interfered with your privacy. We are currently triaging your contact to ensure that we have all information needed to consider your contact as a complaint in accordance with the requirements of the *Privacy Act 1988* (Cth) (Privacy Act). The first step of our triage process will enable an assessment of your contact to be undertaken and once we have all required information, we will be able to decide if and how we are able to assist you.

Please note: Your complaint cannot proceed to allocation at this point in time. Upon receipt of the information requested below, we will be able to fully assess your contact and advise whether your contact meets the requirements of a complaint. If it does not meet the requirements of the legislation your complaint will be closed.

To assess your complaint, we require:

- Your complaint to the respondent. Your complaint form indicates you complained on **x date**. Please provide a copy of this correspondence
- Any response/s to the above mentioned complaint
- Any other relevant communication between you and the respondent

- Confirmation that your concerns have not yet been resolved by the respondent and reasons why you believe that further action is required
- As you have a representative, you must complete a written authority for them to represent you. You will need to complete and return the [authorisation form](#) to us before we can progress your complaint.

It is important that you address **all** of the points above. Should you provide incomplete responses, we will remain unable to progress your contact.

We require this information from you to action this matter in a timely manner and you are required to provide this information within **7 working days** of the date of this email. In the event we do not receive a response from you, we will finalise your complaint and take no further action.

The logo consists of a dark blue square with the white text "OAIC" inside.

First Name

Intake and Eligibility Branch

Office of the Australian Information Commissioner

Melbourne | GPO Box 5288 Sydney NSW 2001

P 1300 363 992 | **E** oaicintake@oaic.gov.au



Decline under s 41(1)(db) – complainant has not responded within the period specified, to a request for information

As a delegate, you can decide to decline to investigate a privacy complaint when the complainant has not responded to a request for information that OAIC has made of them. This is a decline under s 41(1)(db).

1. Check the documents tab to ensure that the required information has not been provided since the assessment
2. Search oaicintake@oaic.gov.au and early.resolution@oaic.gov.au using the complainant's email address and/or the case reference to ensure that there is no correspondence in either mailbox that relates to the request
3. If a response has not been provided, complete the highlighted fields in the template email below and send to the complainant
4. Upload the sent email to the documents tab
5. Go to the sent items of the oaicintake inbox and drag the email to the 'Email to C' folder
6. Finalise the complaint in Resolve by completing all outstanding actions. Refer to guidance on how to finalise complaints

Email content

Email title: Finalisation of your complaint with the OAIC (CP2X/XXXXX)

To firstname

I refer to your privacy complaint about Respondent name (shortened version of R if used), made under s 36 of the *Privacy Act 1988* (Cth) (Privacy Act). You allege that (R's name/shortened version) has interfered with your privacy.

On (x date) the Intake and Eligibility Branch wrote to you requesting information by (due date). To date we have not received the information from you.

Decision

I am satisfied under s 41(1)(db) of the Privacy Act that you have not responded, within a period specified by the Commissioner, to a request for information in relation to the complaint.

Section 41(1) of the Privacy Act gives the Commissioner the discretion to decide not to investigate a complaint if she is satisfied that the complainant has not responded, within a period specified by the Commissioner, to a request for information in relation to the complaint.

I am satisfied of the conditions for the exercise of the Commissioner's discretion at s 41(1) of the Privacy Act and the discretion is enlivened.

I have decided to exercise the discretion under s 41(1) of the Privacy Act to decline to investigate this complaint. The file is now closed.

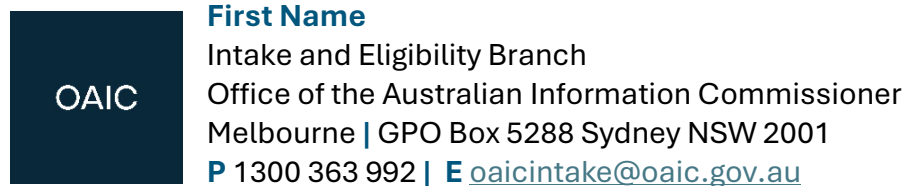
Additional information

It is open to you to submit a [new complaint to the OAIC](#) about this matter when it is more convenient, and when you are able to provide us with all of the required information. However, it is important to note that privacy complaints generally need be submitted to the OAIC within 12 months of the individual becoming aware of the alleged interference with their privacy.

Information about your review rights [here](#).

Yours sincerely

XX



Your review rights

Applying for a judicial review

You may apply to the Federal Court of Australia or the Federal Circuit Court for a review of our decision not to investigate or not to investigate further your complaint, if you think our decision is not legally correct under the *Privacy Act 1988* (Privacy Act).

You must apply to the court within 28 calendar days of us sending you our decision or determination. If we posted it to you, the 28 calendar days starts from the date we posted the decision to you.

The court won't review the merits of your complaint, but they may refer the matter back to us to reconsider — if they find our decision or determination was wrong in law or we didn't exercise our powers properly.

For more information about a judicial review, visit the Federal Court of Australia's website: <https://www.fedcourt.gov.au/>

Lodging a complaint with the Commonwealth Ombudsman

You may lodge a complaint with the Commonwealth Ombudsman if you think we've treated you unfairly, because the Commonwealth Ombudsman can investigate the administrative actions of an Australian Government agency.

If the Commonwealth Ombudsman finds your complaint is justified, they can recommend we reconsider or change our actions or decision or take any other action they think is appropriate.

For more information about making a complaint, visit the Commonwealth Ombudsman's website: <http://www.ombudsman.gov.au/>

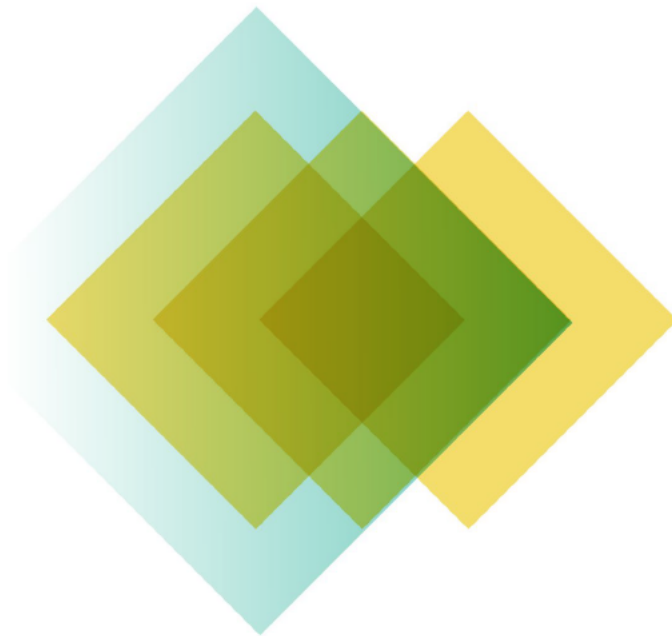


Australian Government

Office of the Australian Information Commissioner

Guidance for staff: Privacy in practice

How the OAIC manages its privacy obligations



24 June 2021

OAIC

Audience: OAIC staff

Location: Intranet - FYI

Review date: Annual

Version	Name	Changes	Date
1.0		Original document	November 2018
2.0	Legal	Revised	March 2021
2.1	Legal	Formatting updates	June 2021

Contents

Background	3
Does this guidance apply to me?	3
Our functions and activities	3
The OAIC as an APP entity	3
About the OAIC	3
Collection of personal information by the OAIC	4
Use of personal information by the OAIC	4
Disclosure of personal information by the OAIC	5
Our suppliers and partners	5
International dealings	5
Personal information holdings	6
How we manage our commitments under the APPs	6
Privacy Policy	8
Privacy management plan	8
Training, awareness, and culture	8
Access and correction	9
Complaints and enquiries	9
Risk management and reporting	10
Privacy Impact Assessments (PIAs)	10
Reviews for compliance and continuous improvement	11
Data breach management and notification	16
Our training and awareness programs 2020-21 FY and 2021-22 FY	17
When and how to conduct a PIA	18
Supplier management	18
Engaging suppliers	18
Identifying supplier risk prior to onboarding	19
Contract governance and assurance	21
Termination	21
Personal information inventory	21

Background

Does this guidance apply to me?

This guidance is for all personnel including statutory appointees, ongoing and non-ongoing employees, temporary agency staff, contractors, consultants, interns, work experience trainees and others who have access to personal information held by or on behalf of the OAIC.

General expectations of personnel

The OAIC recognises the high level of awareness that most personnel hold about the application of the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**) to operations. Our people are best placed to recognise risks and opportunities and to help us lead others with exemplary privacy practices.

Accordingly, we expect our personnel to take an active role in privacy management and compliance at the OAIC.

Please speak with your manager if:

1. You see a risk or an issue relating to our management of personal information;
2. You have identified an opportunity to improve the way we manage personal information;
3. You believe that any project on which you are working will have a significant impact on the privacy of individuals, as a PIA may be required in respect of that project.¹

Managers are expected to raise these matters with the Chief Privacy Officer promptly and to ensure that risks are appropriately documented in the OAIC's risk registers in accordance with our risk management policies, detailed below.

Our functions and activities

The OAIC as an APP entity

While the Privacy Act confers on the Commissioner a range of privacy regulatory powers, the OAIC too is an APP entity and has obligations to properly manage the collection, use and disclosure of personal information. This document describes how the OAIC manages its obligations under the Privacy Act.

About the OAIC

In the performance of its functions, the OAIC collects, uses, and discloses personal information. The OAIC has three primary functions, namely:

- privacy functions, conferred by the Privacy Act and other laws;

¹ Privacy (Australian Government Agencies — Governance) APP Code, s 12.

- freedom of information functions, in particular oversight of the operation of the *Freedom of Information Act 1982* (**FOI Act**) and review of decisions made by agencies and ministers under that Act; and
- government information policy functions conferred on the Australian Information Commissioner under the *Australian Information Commissioner Act 2010* (**AIC Act**).

Our routine collections, uses and disclosures required by these functions are described below and in [our privacy policy](#) on the OAIC website.

Collection of personal information by the OAIC

The OAIC routinely **collects** personal information relating to:

- Complainants, applicants, and authorised representatives when handling privacy and freedom of information (FOI) complaints and FOI reviews or taking other regulatory action under the Privacy or FOI Acts. This can include sensitive information.
- Respondents such as government officers or organisation contacts (for example, employees and witnesses) when dealing with a complaint under the Privacy Act, or a complaint, extension of time or application for IC review under the FOI Act.
- Job applicants, people who notify the OAIC about a data breach or report a matter for investigation.
- Individuals who wish to engage with us, for example by attending an event, joining a privacy or FOI network, or providing feedback, or when engaging in policy/advice work. This includes counterparts with regulators in other jurisdictions and overseas and other business contacts, and
- Individuals who provide feedback or other information to the OAIC via social networking services such as Facebook and Twitter.

Whilst we usually collect personal information directly from the relevant individual, at times, we collect personal information from a third party or publicly available source.

Use of personal information by the OAIC

The OAIC routinely **uses** personal information for the following purposes:

- To conduct privacy investigations, either in response to complaints or on the Commissioner's own initiative.
- To review decisions made by agencies and ministers under the FOI Act.
- To handle privacy and FOI complaints.
- To receive notices about eligible data breaches.
- To conduct privacy assessments.
- To monitor agency administration in relation to FOI and privacy.

- To allow the OAIC to properly manage its employment of staff or to assess the suitability of candidates for employment at the OAIC, and
- To engage with and provide advice to stakeholders in the public and private sectors and the Australian community.

Disclosure of personal information by the OAIC

The OAIC routinely **discloses** personal information in the following circumstances:

- To the respondent and the complainant, and where relevant, affected third parties, where a privacy or FOI complaint is made, or an FOI review is sought.
- To others as relevant where a notifiable data breach is reported to the OAIC and the notifier agrees to or would reasonably expect the OAIC to disclose the personal information.
- To the My Health Records System Operator where a breach is notified to the OAIC under the My Health Records Act.
- To another review body where a complainant, applicant or respondent seeks an external review of the OAIC's decision or makes a complaint to the Commonwealth Ombudsman.
- Where a party to a published decision, determination or report asks for their name to be published.
- To the media where an individual agrees for personal information relating to a complaint to be disclosed, or would reasonably expect it to be disclosed, and
- To other Australian or international regulators, or to external dispute resolution (EDR) schemes if the individual agrees and where the information will assist the OAIC or the other regulator or EDR scheme investigate a matter.

There is also regular disclosure of staff information, for example, when successful applicants are announced in the Gazette.

We only disclose sensitive information for primary purposes or for directly related secondary purposes which are reasonably expected or agreed to by the individual.

Our suppliers and partners

At times, we engage third parties to perform some of our activities, including to host our website servers and manage our information technology and human resources information. You can read more about our suppliers and management of suppliers in [Personal information inventory and Supplier management](#).

International dealings

The OAIC holds limited personal information about people residing overseas.

We transfer personal information outside of Australia in limited circumstances. Generally, this will occur only where required to properly handle a complaint or application. For example, where the

complainant or respondent is based overseas, where the respondent is Australian based but is a related body corporate to an overseas company and where a complaint is made to regulators or other bodies overseas in addition to the OAIC.

We exchange information with overseas contacts such as personnel of foreign regulators.

Personal information holdings

It is an obligation of our Chief Privacy Officer to maintain a record of the OAIC's personal information holdings.² The OAIC has mapped our personal information holdings to show where personal information resides in our systems. See [Personal information inventory](#) to read more about our holdings.

How we manage our commitments under the APPs

APP 1 — Open and transparent management of personal information

Ensures that the OAIC manages personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

Note: In respect of APP 1.2, the OAIC is also bound by the *Privacy (Australian Government Agencies — Governance) APP Code 2017 (APP Code)*. The APP Code is referenced in footnotes where relevant.

What we do and our expectations of personnel Governance and accountability

The OAIC recognises the high level of awareness that most personnel hold about the application of the Privacy Act and the Australian Privacy Principles (**APPs**) to operations. Our people are best placed to recognise risks and opportunities and to help us lead others with exemplary privacy practices. Accordingly, we expect our personnel to take an active role in privacy management and compliance at the OAIC.

Personnel are supported by three key roles with complementary accountabilities for privacy outcomes at the OAIC. These are the Chief Privacy Officer, Privacy Officers, and the Privacy Champion.

Privacy Champion

The OAIC has appointed a Privacy Champion (the OAIC's Deputy Commissioner), who holds accountability for the following actions:

- Promoting a culture of privacy within the agency that values and protects personal information.
- Providing leadership within the agency on broader strategic privacy issues.
- Reviewing and/or approving the agency's privacy management plan, and documented reviews of the agency's progress against the privacy management plan, and

² Privacy (Australian Government Agencies — Governance) APP Code 2017, s 10(5)(b).

- Providing regular reports to the agency's executive, including about any privacy issues arising from the agency's handling of personal information.³

How to contact our Privacy Champion:

Elizabeth Hampton
Deputy Commissioner

s22

Telephone: s22

Chief Privacy Officer and Privacy Officers

Within the OAIC the CPO is the primary point of contact for advice on privacy matters and co-ordinates a range of functions to help the agency comply with the Code.⁴ However, it is ultimately the OAIC that is required to comply with the Code and the Privacy Act. The OAIC is expected to provide the CPO and its Privacy Officers with the necessary resources, time, and support to allow them carry out their role effectively.

The Code sets out a list of the Privacy Officer functions that the OAIC must ensure are carried out. These functions will usually be performed by the CPO and the Privacy Officers but may also be performed by another person (or persons) in accordance with the existing processes or specific requirements of the agency. The Privacy Officer functions required under the Code include:

- Providing privacy advice internally. The CPO, for example, may give advice to colleagues on:
 - the development of new initiatives that have a potential privacy impact
 - the general application of privacy law to the agency's activities
 - what to consider when deciding whether to carry out a Privacy Impact Assessment (PIA)
 - what safeguards to apply to mitigate any risks to the privacy of individuals
- Liaising with the Executive and the agency at large about privacy matters in the OAIC and how to best undertake a range of functions to help the agency comply with the Code.
- Coordinating the handling of internal and external privacy enquiries, privacy complaints about the OAIC as an agency, and providing advice on requests for access to, and correction of, personal information. On receipt of a privacy enquiry or complaint, the CPO will talk to the manager and/or officer relevant to the enquiry or complaint. The CPO will generally refer privacy complaints to the Privacy Officers to assist with management of the complaint.
- Responsibility for maintaining a record of the OAIC's personal information holdings
- Assisting with the preparation of PIAs, which are required for all high privacy risk projects
- Measuring and documenting the OAIC's performance against its privacy management plan.

³ APP Code s 11(4)

⁴ APP Code s 10(4)

The CPO and Privacy Officers have additional functions including delivering privacy training to agency staff, proactively monitoring compliance, and managing the OAIC's response to data breaches.

How to contact our Chief Privacy Officer:

Chief Privacy Officer: Caren Whip

s22

Telephone: s22

The accountabilities of the Chief Privacy Officer and the Privacy Champion are documented in their respective performance management agreements.

Privacy Policy

Several key policies (external and internal) set out the OAIC's framework for the handling of personal information.

The OAIC's [privacy policy](#) is published on our website. It has a Flesch Kincaid Reading Ease score of 6 (meaning it can be comprehended by 11 to 12-year-olds). It is accompanied by a [summary of the policy](#).

The OAIC has a separate [human resources privacy policy](#). The Chief Privacy Officer is accountable for maintaining these policies.

All personnel are expected to comply with these policies and to raise any questions or concerns with their manager.

Privacy management plan

The OAIC has developed and implemented a privacy management plan and this is reviewed annually by the Executive.⁵

All personnel are expected to read the OAIC's current privacy management plan (**PMP**) ([D2018/011921](#)) and to action any responsibilities assigned to them under it. Managers are expected to monitor and report to the Chief Privacy Officer on the progress of these actions.

Training, awareness, and culture

About 80% of our staff are directly involved in the regulation of or providing advice on the APPs. As a result, there is a high level of awareness amongst personnel about privacy obligations and best practice. It is expected that most staff, after their induction and on-the-job training will generally have a relatively detailed understanding of the APPs.

When new employees are inducted, they attend face to face training with the OAIC's privacy officers. This training covers the privacy obligations of all personnel, and policies and procedures relating to

⁵ The APP Code requires the OAIC to have a PMP (s 9(1)) and to measure and document its performance against its PMP at least annually (s 9(3)).

privacy.⁶ The Chief Privacy Officer routinely updates content based on lessons learnt from complaints and enquiries data over the preceding period.

The OAIC recognises the need for annual refresher training on privacy obligations and good privacy practices. Online, as well as face-to-face awareness and training programs are provided to staff.

Aside from formal training and awareness activities, the OAIC aims to embed a strong culture of good privacy practice through leadership by example. Managers are expected to exemplify and manage good privacy practices through their day-to-day supervision and mentoring of staff, including through remote oversight.

Access and correction

Information for the public about how to access and seek correction of personal information held by the OAIC is on our website.

In many cases, personal information is updated during case management by way of an informal request with the case manager.

Our internal standard operating procedure for managing formal access and correction requests can be found on our '[Access our information](#)' page on the OAIC website.

Complaints and enquiries

Information about how to make a complaint or inquiry about the OAIC's handling of personal information is outlined in our privacy policies, accessible on the OAIC website.

Our internal processes for capturing and managing complaints and inquiries can be found on the Intranet. See for example, our Enquiries Line Resolve Guide [D2013/011438](#) and our Guide to assisting on the Enquiries Line ([D2013/011442](#)).

Privacy complaints about the OAIC

Where an individual complains to the OAIC under s 36 of the Privacy Act (in its capacity as a regulator), that the OAIC has interfered with their privacy, there is a risk that the OAIC will be perceived to be biased or may have a conflict of interest in investigating its own actions. That is, a reasonable observer might consider that the OAIC may not bring an impartial mind as the regulator, in regulating its own actions.

If a complaint is made about the OAIC's handling of personal information, it would be handled by a more senior officer than the officer to whom the complaint relates and would be conducted in accordance with the Australian Public Service Values, Code of Conduct and guidelines for handling misconduct.

In order to mitigate this risk, the OAIC has decided on a process by which it may seek the assistance of an appropriately qualified and experienced external consultant to conduct an independent investigation into the act or practice about which the complainant complains. The decision to outsource a s 36 privacy complaint against the OAIC to an external investigator must be made by the

⁶ APP Code s 16

Australian Information Commissioner or an Executive delegate. Additional information is available from 'Guidance for staff: 'Dealing with privacy complaints about the OAIC' ([D2021/000080](#)).

Review the OAIC [Service Charter](#) on how the OAIC deals with privacy complaints against the OAIC conducted at least every 12 months.

Risk management and reporting

The OAIC has a framework for identifying and managing privacy risks (and other types of risks). Risk management is an important part of our compliance with the *Public Governance, Performance and Accountability Act 2013*. Under this framework, all personnel play a role in the identification and mitigation of risks.

Personnel who become aware of a privacy risk in the OAIC's day-to-day operations or in a project or initiative should speak with their manager. Managers must ensure that risks are documented in the OAIC's risk registers in accordance with our risk management framework.

You can read more about risk management by clicking on these links:

- Risk management policy: [D2017/002862](#)
- Risk management procedures and framework: [D2017/002866](#)

The OAIC's risk registers are regularly reviewed by the Executive.

You can access the risk register for your Branch here: Regulation and Strategy Risk Register: [D2017/006758](#) and DR Risk Register: [D2017/006759](#)

Privacy Impact Assessments (PIAs)

All initiatives that may involve the collection or handling of personal information (for example, a new supplier, technology or process that impacts the handling of personal information by the OAIC or on its behalf) must be reviewed for privacy impacts and safeguards. Findings must be included in the relevant Executive brief, for sign off by the Executive.

Where the OAIC reasonably considers that a project involves any new or changed ways of handling personal information that are *likely to have a significant impact on the privacy of individuals*, the APP Code requires that a PIA is conducted on the project.⁷ The OAIC has an obligation to maintain and publish on its website a register of any PIAs it conducts⁸ and may determine to publish a PIA (or an edited or summary version of a PIA) on its website.⁹

All personnel should familiarise themselves with our approach to PIAs and escalate initiatives and projects accordingly. See 'When and how to obtain a PIA' below.

⁷ APP Code s12

⁸ APP Code s15

⁹ APP Code s13

Reviews for compliance and continuous improvement

The Privacy Champion and Chief Privacy Officer oversees an annual review of the OAIC's privacy practices, procedures, and systems, to ensure their currency and adequacy for the purposes of compliance with the APPs¹⁰ and to drive continuous improvement. The Chief Privacy Officer oversees review or assessment of the following:

- Privacy policy and privacy notices¹¹
- Privacy management plan and implementation¹²
- Privacy practices of teams across the OAIC, and
- The effectiveness of the OAIC's data breach response plan (tested against real incidents or simulation if no incidents have occurred).

The Privacy Champion oversees review or assessment of:

- Risk register
- Records management policies and guidance in relation to the OAIC's handling of personal information
- A privacy compliance review is an agenda item on the internal audit committee agenda at least every 12 months.

The timeliness and quality of the functions and activities we deliver are also measured by the Privacy Champion and Chief Privacy Officer from time to time to support continuous improvement.

APP 2 — Anonymity and pseudonymity

Requires the OAIC to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

What we do and expectations of personnel

In many cases, it is impracticable for the OAIC to perform its functions and activities without identifying the individuals with whom we engage. By way of example, we usually need a name and contact information to handle inquiries, requests, complaints, or applications or to act on a report. In limited circumstances, we can support individuals to remain anonymous or use a pseudonym in their interactions with us. For example, if someone contacts our enquiries line, personnel are expected not to ask for their name unless this information is needed to adequately handle the question.

¹⁰ APP Code s 17

¹¹ APP Code sub-s 17(a) and (b)

¹² APP Code requires the OAIC to have a PMP (s 9(1)) and to measure and document its performance against its PMP at least annually (s 9(3)).

APP 3 — Collection of solicited personal information

Outlines when the OAIC can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

What we do and expectations of personnel

The OAIC applies a data minimisation approach to all collections of personal information. This means that personal information collected should be kept to the minimum required to perform the activity. Where possible, no personal information should be collected.

All personnel are expected to use our forms and systems effectively to capture personal information in a consistent and appropriate way. Also, personnel with accountabilities for managing complaints and other relevant activities are expected to follow standard operating procedures for capturing consent, e.g., where a third party provides sensitive information.

APP 4 — Dealing with unsolicited personal information

Outlines how the OAIC must deal with unsolicited personal information

What we do and expectations of personnel

As the OAIC is bound by the *Archives Act 1983*, we generally cannot *automatically* delete unsolicited personal information. Depending on the situation, the personal information may have to be kept for a short time before being disposed of under Archives Act Normal Administrative Practice parameters. See the [Records Disposal Authority and Normal Administrative Practice \(NAP\) checklist](#).

In all instances, personnel must consult the Chief Privacy Officer if they believe that they have received unsolicited personal information, the collection of which would not be permitted under APP 3 or which may necessitate the issuing of a privacy notice, e.g., where unsolicited personal information about a complaint or review is received from a third party.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances the OAIC, when it collects personal information, must notify an individual of certain matters.

What we do and expectations of personnel

The OAIC typically meets its APP 5 obligations by issuing its [standard short privacy statement](#), linking to its detailed privacy policy. The statement is used on all complaint and review forms and when collecting contact information from new groups of stakeholders.

Personnel must ensure that the standard short statement is used when collecting personal information. It can be adapted if required, in consultation with the Chief Privacy Officer.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which the OAIC may use or disclose personal information that it holds.

What we do and expectations of personnel

The OAIC uses and discloses personal information to perform its functions and activities as detailed above. All personnel are expected to escalate to their manager if they believe that an initiative or other activity, they are undertaking does not comply with APP 6.

If a project or initiative involves any new or changed ways of using or disclosing personal information (including using or disclosing existing personal information holdings for secondary purposes), a PIA and/or other actions may be required. See 'When and how to obtain a PIA' below.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

What we do and expectations of personnel

APP 7 does not apply to the OAIC as it only applies to organisations.

APP 8 — Cross-border disclosure of personal information

Outlines the steps the OAIC must take to protect personal information before it is disclosed overseas.

What we do and expectations of personnel

It is quite rare for the OAIC to send personal information overseas. It does occur from time to time where necessary for the proper handling of a complaint or application, for example, where the complainant or respondent is based overseas.

The OAIC's privacy policy states that such international disclosures may occur, and therefore the OAIC considers that implied consent is received when the relevant party or parties provide their personal information. However, overseas disclosures are usually discussed with the relevant party or parties before the information is disclosed as an additional precaution.

All personnel are expected to discuss any planned overseas disclosures with the relevant party or parties before making the disclosure and to make a file-note of the discussion in Resolve.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

What we do and expectations of personnel

APP 9 does not apply to the OAIC as it only applies to organisations.

APP 10 — Quality of personal information

The OAIC must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. The OAIC must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

What we do and expectations of personnel

As stated in our [privacy policy](#), the OAIC has adopted the following routine practices to support its obligations under APP 10:

- We generally collect personal information in a consistent format using templates and forms.
- Whenever personal information is collected from a third party or a public source, we check its accuracy with the individual to whom it relates.
- We are timely in adding or updating personal information in existing records.
- We (via our Enquiries team) regularly audit our contact lists to check their accuracy, and
- We review the quality of personal information before we use or disclose it.

All personnel are expected to adopt these practices in their dealings with complainants, respondents, and other individuals.

APP 11 — Security of personal information

The OAIC must take reasonable steps to protect personal information it holds from misuse, interference, and loss, and from unauthorised access, modification, or disclosure. The OAIC has obligations to destroy or de-identify personal information in certain circumstances.

What we do and expectations of personnel

Reasonable steps

The OAIC's information security policy framework consists of the following key documents:

- Information Management Policy: ([D2017/001625](#))
- System Security Plan: ([D2017/007023](#))
- Risk Management Plan: ([D2017/007022](#))
- Standard Operating Procedures: ([D2017/007020](#))
- Security Documentation Framework: ([D2017/007021](#))

The OAIC's information security framework is supported by the OAIC's records manager who has accountability for overseeing information security practices within the OAIC.

In addition, regular independent information security reviews and audits are conducted. For example, in 2018, following commencement of the NDB scheme, the OAIC engaged an outside consultant to perform an information security review. Also, an audit of access controls will be conducted in 2018 and an audit of the OAIC's clean desk policy was conducted in 2017. The results of audits are usually provided to staff by way of an all-staff email to increase awareness and drive continuous improvement.

The OAIC routinely considers information security risks and controls when engaging new suppliers. For organisations that will be accessing personal information held by the OAIC (for example, to provide IT services in relation to OAIC's information systems) strict contractual measures such as additional non-disclosure agreements are used to protect the security and confidentiality of that personal information.

Where the OAIC uses Australian Government agencies as suppliers, they must comply with all applicable information security protocols under the Australian Government's Protective Security Policy Framework (**PSPF**). For more information on how the OAIC manages supplier risk, see 'Supplier management' below.

All personnel are expected to comply with the OAIC's clean desk policy, to use effective password practices, and to comply with relevant policies, such as the Usage of ICT Facilities Policy ([D2017/001580](#)) and the Remote Access and Mobile Devices Policy ([D2017/001030](#)).

Managers are expected to periodically check that access controls for personnel are appropriate and request changes if necessary.

Working away from the office

Telework is working away from the office. Staff who telework or work from home use information and communications technology to stay connected with colleagues and work systems. All staff are expected to comply with the OAIC's 'Working from home (WFH) Instructions and Guidance' ([D2020/005244](#)). This includes the 'Telework Policy and Remote Access' guidelines ([D2013/095066](#)).

Destruction and de-identification

The OAIC destroys personal information that is no longer required, subject to archiving obligations.¹³ Records documenting routine operational administrative tasks supporting the core

¹³ See [OAIC Privacy Policy](#) under "Storage and security of personal information".

business of compliance management for example, are destroyed seven years after the action is completed while records documenting general enquiries relating to the compliance management business of the OAIC are destroyed one year after the action is completed (see [Records Disposal Authority](#)).

Where archiving obligations prevent de-identification or destruction of personal information, it is OAIC policy to adopt other measures to limit privacy risks (such as archiving and limiting access to those personal information holdings).

All personnel must ensure that they comply with the [OAIC Records Disposal Authority](#) (and the [Normal Administrative Practice Checklist](#)) before destroying personal information as non-compliance may breach our obligations under the Archives Act.

APP 12 – Access to personal information

Outlines the OAIC's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 – Correction of personal information

Outlines the OAIC's obligations in relation to correcting the personal information it holds about individuals.

What we do and expectations of personnel (APP 12 and APP 13)

The OAIC has published its access and correction procedures in detail as part of its [privacy policy](#) and on the '[Access our information](#)' page on its website. The latter advises individuals to consider speaking to an OAIC officer via its enquiries line before making an FOI request, as in many cases personal information can be provided quickly (within 30 days) and informally. The OAIC requires the requester to verify their identity before access is given or the information is corrected. Where access is requested in an alternative format, the OAIC will attempt to meet all such requests to the best of our ability.

All personnel are expected to be familiar with these policies.

Personnel who support the enquiries line are expected to be aware of the detailed operating procedures which underpin APP 12 and 13 and the '[Access our information](#)' page on our website.

All other personnel are expected to refer access and correction requests to their Director.

Data breach management and notification

The OAIC's Data Breach Response Plan (**Plan**) can be found on the OAIC's FYI intranet (see HP Content Manager at [D2017/002187](#)). The Plan accords with the OAIC's published guidance ([Data breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988 \(Cth\)](#)). The Plan names the data breach response team members.

All personnel should be aware of the Plan and if they suspect that a data breach has occurred should escalate any suspected data breaches to their manager in the first instance.

As stated in the Plan, Directors should use their discretion in determining whether a data breach or suspected data breach requires escalation to the data breach response team. In making that determination, Directors should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a risk of serious harm to any of the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in OAIC processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then the Director should attempt immediate verbal contact with the Chief Privacy Officer, or if this is not possible, another primary response team member.

Our training and awareness programs 2020-21 FY and 2021-22 FY

The following email communications for all personnel will comprise an essential part of the OAIC's awareness and training programs.

Topic	From	Content
Data breach escalation and management	Chief Privacy Officer	Reminders about how to escalate a suspected data breach.
Data breach escalation and management	Chief Privacy Officer	Reports on the outcome of planned Data Breach Response Plan Tests.
Privacy/ security practices	Privacy Champion	Updates to all staff about results and learnings from any internal audits in relation to personal information handling.
Data Breach Notification report	Privacy Champion	Findings from latest OAIC DBN report shared with all staff in email communications or face-to-face training.
Privacy Awareness Week	Strategic Communications	Provide opportunities for reminders about the role and responsibilities of OAIC staff in protecting the personal information of individuals.

When and how to conduct a PIA

Threshold test for informing the Chief Privacy Officer of a new initiative

The Chief Privacy Officer must be consulted on all new projects handling personal information.

Threshold test for informing the Executive

The Executive is to be informed of *any new personal information handling processes* or where the OAIC proposes to use or disclose existing personal information holdings for *secondary purposes*. The Executive Brief template includes a section for privacy impacts and safeguards.

Threshold test for a PIA

A PIA is required under the APP Code where the OAIC reasonably considers that a project involves any new or changed ways of using or disclosing personal information that are likely to have a significant impact on the privacy of individuals.¹⁴

Escalation process

If you believe that your project or initiative (including the engagement of a new supplier) meets any of these thresholds, you should speak with your manager in first instance to determine any subsequent action(s) required.

PIA methodology

The OAIC follows its [Guide to undertaking privacy impact assessments](#).

The Chief Privacy Officer (in consultation with the Executive) will determine the effort and approach to be applied to the PIA and will provide advice to the Executive on the approach to publication (in accordance with the APP Code),¹⁵ if appropriate.

'[Privacy Impact Assessment: Working remotely in response to COVID-19](#)' has been developed to consider privacy risks associated with changes to working arrangements at the OAIC in response to the COVID-19 pandemic.

Supplier management

Engaging suppliers

The OAIC routinely considers information security risks and controls when engaging new suppliers.

For organisations that will be accessing personal information held by the OAIC (for example, to provide IT services in relation to OAIC's information systems) strict contractual measures such as

¹⁴ APP Code s 12

¹⁵ APP Code s 15

additional non-disclosure agreements are used to protect the security and confidentiality of that personal information.

Where the OAIC uses Australian Government agencies as suppliers, they must comply with all applicable information security protocols under the Australian Government's Protective Security Policy Framework (**PSPF**).

Identifying supplier risk prior to onboarding

If you are proposing to engage a new supplier (or, you are proposing to engage an existing supplier to deliver a new product or service), you must include the following information when you brief the Chief Financial Officer at contract creation stage:

Question	Risk Considerations
Threshold	
Will the supplier handle personal information while providing a service to the OAIC?	<i>If 'no', there is no need to complete the questions below.</i>
Privacy foundations	
Has the supplier demonstrated that it handles personal information in a manner that complies with the APPs?	<i>This is a high-level question which requires a holistic consideration of all responses below.</i>
Is the supplier subject to the APPs in their own right?	
Is the supplier an organisation or an agency?	
Does the supplier have a publicly available privacy policy which meets the requirements of the APPs?	
<i>Provide a copy.</i>	
Does the supplier have an operational privacy framework supported by a privacy function and a Chief Privacy Officer or privacy lead?	
<i>Provide evidence from supplier.</i>	
Does the supplier carry out periodic training and awareness in relation to privacy?	
<i>Provide evidence from supplier.</i>	
Does the supplier have a process in place for managing privacy complaints?	
<i>Provide evidence from supplier.</i>	
Does the supplier have a standard personal information collection notice?	
<i>Provide evidence from supplier.</i>	

Question	Risk Considerations
Privacy Impact Assessments	
<p>Does the supplier carry out Privacy Impact Assessments over internal programs?</p> <p><i>Provide evidence from supplier.</i></p>	
Third parties/subcontracting	
<p>Will the third party share personal information with another third party while offering services to the OAIC?</p>	<p><i>If 'no', there is no need to complete the other questions in this section. Proceed to 'Integrity of personal information'.</i></p>
<p>Does the supplier carry out Privacy Risk Assessments over third parties it shares personal information with?</p> <p><i>Provide evidence from supplier.</i></p>	
<p>Does the supplier have a process for monitoring the sharing of personal information with its third parties, and for periodically assessing their privacy and security controls?</p> <p><i>Provide evidence from supplier.</i></p>	
<p>If the supplier will disclose personal information to entities located outside Australia, does it assess their compliance with the APPs?</p> <p><i>Provide evidence from supplier.</i></p>	
Integrity of personal information	
<p>How does the supplier protect the personal information that it holds from interference, misuse, loss and unauthorised access, modification and disclosure?</p> <p><i>Provide evidence from supplier.</i></p>	
<p>Does the supplier have policies and procedures relating to data retention and destruction, including processes for identifying and destroying or de-identifying personal information (in electronic and physical form) that it no longer requires?</p> <p><i>Provide evidence from supplier.</i></p>	
<p>Does the supplier have a process for monitoring and correcting personal information that it holds?</p> <p><i>Provide evidence from supplier.</i></p>	

Question	Risk Considerations
Access and correction	
<p>Does the supplier have a process to allow individuals to access any personal information it holds about them?</p> <p><i>Provide evidence from supplier.</i></p>	
<p>Does the supplier have a process for allowing individuals to request the correction of personal information it holds about them?</p> <p><i>Provide evidence from supplier.</i></p>	

Contract governance and assurance

Responsibility for ensuring that contractual and other operational controls are operating effectively during the term of the contract (and beyond if relevant) lies with the Director of the team that engaged the supplier. Supplier risks must be escalated via the OAIC risk register.

Termination

At the cessation of the contract, the OAIC must ensure that controls in place to protect privacy and personal information at the conclusion of the engagement are effective, for example, by assuring that access to personal information is stopped and copies of personal information held by the supplier on behalf of the OAIC are returned or destroyed at appropriate time periods.

Responsibility for ensuring that these steps are taken lies with the Director of the team that engaged the supplier.

Personal information inventory

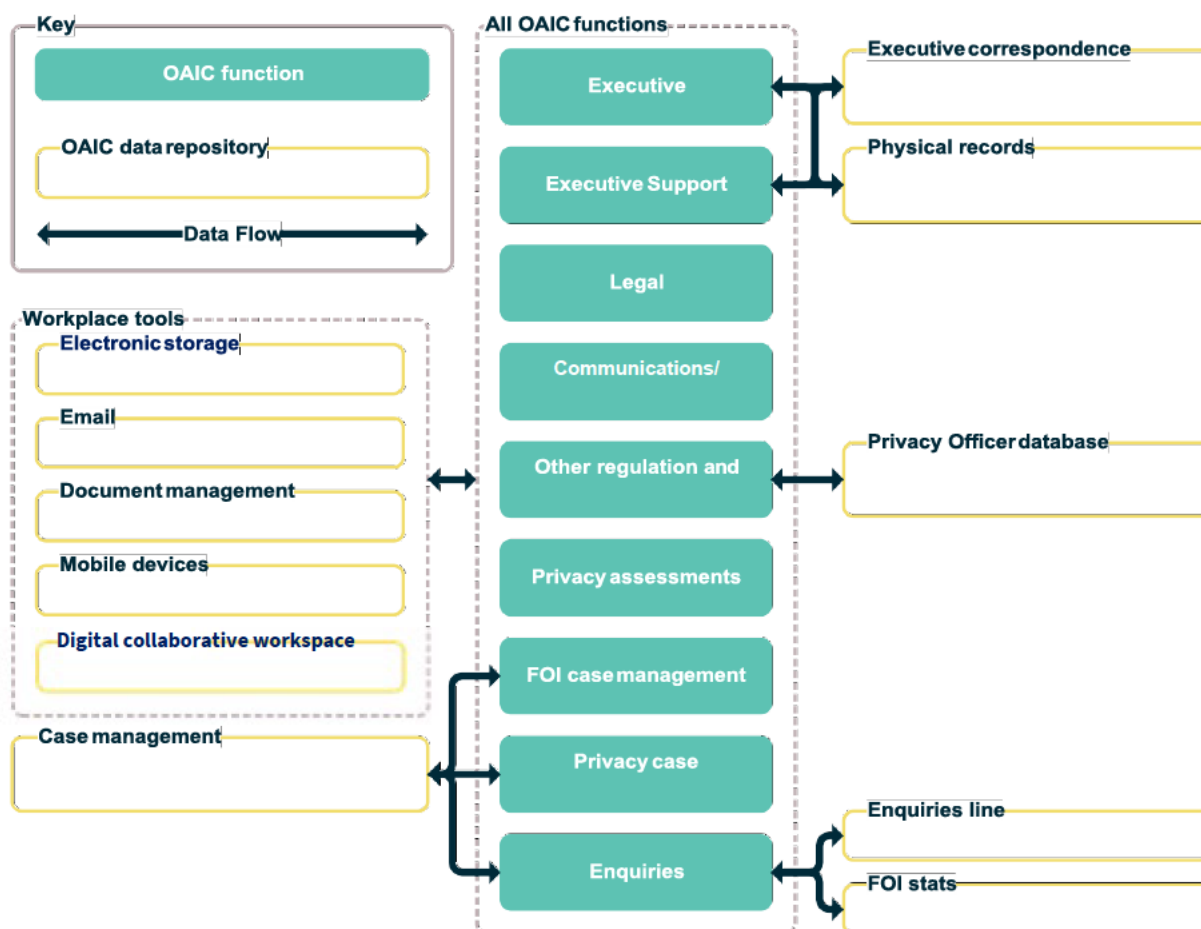
The OAIC has mapped our personal information holdings to show where personal information resides in our systems. Our [Personal Information Inventory](#) includes a detailed listing of all the OAIC's data repositories that contain personal information, along with:

- the types of personal information held in each repository;
- the purposes for which the personal information is used;
- the source of the personal information;
- whether personal information is shared with third parties;
- where the personal information is stored;
- how long the personal information is retained;
- who within the OAIC with accountability for the personal information;

- who within the OAIC has access to the personal information; and
- a contact person/team for each repository.

The Chief Privacy Officer is the owner of the Personal Information Inventory document.

The diagram below is a high-level summary of our Personal Information Inventory, with system names and third parties removed.



The Chief Privacy Officer is the owner of the personal information inventory document.



Australian Government

Office of the Australian Information Commissioner

Early Resolution Guidance on processing APP 12 requests



15 January 2021

OAIC

Contents

Change history	2
Background	3
When this guidance applies	3
Purpose	3
APP 12 – what does it say	4
Authority to refuse access under the FOI Act	5
Required or authorised to refuse access under another Act	6
Processing a request	6
Annexure A	19
Sample search and retrieval email	19
Annexure B	20
Sample APP 12 Decisions	20
Annexure C	28
Case note: Knowles v Secretary, Department of Defence [2020] FCA 1328	28

Change history

Version	Changes	Date
1.0	Original	January 2021

Background

When this guidance applies

This guidance applies to the acceptance and processing of Australian Privacy Principle (**APP**) 12 requests made of the Office of the Australian Information Commissioner (**OAIC**) in its capacity as an APP entity for the purposes of the *Privacy Act 1988* (Cth) (**Privacy Act**).

References to provisions in this guidance are those in the Privacy Act unless otherwise specified.

Relevant provisions – Privacy Act

Under s 6(1) “personal information” is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Section 6(1) further provides that an APP entity “holds” personal information if the entity has possession or control of a record that contains the personal information.

Australian Privacy Principle (**APP**) 12 states that if an APP entity holds personal information about an individual the entity must, on request by the individual, give the individual access to the information unless a specific exemption applies.

APP 12.2 provides that an agency is not required to give access to personal information if it is authorised to refuse access under the *Freedom of Information Act 1982* (**FOI Act**).

APP 12.5 provides that if an APP entity refuses to give access to personal information in the manner requested by the individual, it must take reasonable steps to give access in a way that meets the needs of the individual. Under the OAIC’s Australian Privacy Principles Guidelines (July 2019) (**APP Guidelines**), this can include giving a summary of the requested personal information to the individual.

APP 12.9 provides that if an APP entity refuses to give access, or to give access in the manner requested by the individual, the entity must give the individual written notice setting out a number of matters, including the reasons for the refusal, except to the extent that it would be unreasonable to do so, having regard to the grounds of refusal.

Purpose

This guidance material outlines:

- the text of APP 12
- how to interpret APP 12, and
- how to apply APP 12 when making a decision.

This guidance should be used by all staff who process APP 12 requests made of the OAIC. This document outlines the statutory time frames that apply to the OAIC and the steps that should be taken when processing an APP 12 request.

APP 12 – what does it say

An APP entity that holds personal information about an individual must, on request, give that individual access to the information (APP 12.1). The grounds on which access may be refused differ for agencies and organisations.

APP 12 also sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be given access to information. In particular, APP 12 does not prevent an APP entity from giving access to personal information under an informal administrative arrangement, provided the minimum access requirements stipulated in APP 12 have been met.

For agencies, APP 12 operates alongside the right of access in the *Freedom of Information Act 1982* (Cth) (**FOI Act**). The FOI Act provides individuals with a right of access to documents held by most Australian Government agencies, including documents containing personal information.

APP 12 requires an APP entity to provide access to ‘personal information’. It does not provide a right of access to other kinds of information. ‘Personal information’ is defined in s 6(1) as ‘information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in a material form or not’

Personal information of one individual may also be personal information of another individual. For example:

- information in a marriage certificate may be personal information of both parties to the marriage
- an opinion may be personal information of both the subject and the giver of the opinion

APP 12 requires an APP entity to provide access to all of an individual’s personal information it holds, even if that information is also the personal information of another individual, unless a ground to refuse access applies.

As to other requested information that is not personal information an agency could consider whether access to that information can be granted under the FOI Act, or on an administrative basis. Before refusing access to that other information, the agency should advise the individual to consider making the request under the FOI Act.

Agencies are not required to advise individuals to request personal information under the FOI Act rather than under an administrative arrangement or by relying on APP 12.

In some circumstances it may be preferable for an agency to suggest that an individual make an access request under the FOI Act. This is because an FOI access request can relate to any document in the possession of an agency (FOI Act, s 15(1)) and is not limited to personal information held in an agency record (APP 12.1).

The FOI Act contains a consultation process for dealing with requests for documents that contain personal or business information about a person other than the requester (FOI Act, ss 27, 27A).

An applicant who applies for access under the FOI Act can complain to the Information Commissioner about an action taken by an agency under that Act (FOI Act, s 70).

An applicant who is refused access under the FOI Act has a right to apply for internal review or Information Commissioner review of the access refusal decision (FOI Act, ss 54, 54L).

An agency is not required by APP 12 to give access to personal information if the agency is required or authorised to refuse access to that information by or under:

- the FOI Act (APP 12.2(b)(i))
- any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents (APP 12.2(b)(ii))

In summary, an agency is ‘required’ to refuse access by an Act that prohibits the disclosure of the personal information; and an agency is ‘authorised’ to refuse access by an Act that authorises or confers discretion on the agency to refuse a request for access to the personal information.

Authority to refuse access under the FOI Act

The grounds on which an access request can be declined under the FOI Act include:

- a document is an exempt document under Part IV, Division 2 of the FOI Act, for example, the document is a Cabinet document, is subject to legal professional privilege, contains material obtained in confidence, or a secrecy provision applies
- a document is a conditionally exempt document under Part IV, Division 3 of the FOI Act, for example, the document contains deliberative matter, or disclosure of the document would involve the unreasonable disclosure of personal information about another person and it would be contrary to the public interest to release the document at that time
- the individual is not entitled to obtain access to a document of the kind requested, for example, the document is available for purchase from an agency (FOI Act, ss 12, 13)
- providing access in the terms requested by a person would substantially and unreasonably divert an agency’s resources from its other operations (s 24AA)
- processing a person’s request would require an agency to disclose the existence or non-existence of a document, where that would otherwise be exempt information (s 25).

The FOI Act specifies consultation processes that may apply to requests made under that Act, for example, where a ‘practical refusal reason’ may apply (FOI Act, s 24) to the request, or where a requested document contains a third party’s personal or business information (FOI Act, ss 27, 27A). An agency is not required to undertake any of those consultation processes before refusing access on any of those grounds under APP 12.

A decision to refuse access under APP 12.2(b)(i) (on one of the FOI grounds listed above) is a decision made under the Privacy Act, not the FOI Act. As required by APP 12.9, the agency must provide the individual with a written notice that sets out the reasons for the refusal and the complaint

mechanisms available to the individual. The individual may have a right to complain pursuant to s 36 of the Privacy Act to the Information Commissioner about the refusal decision. However, the individual will not have a right to seek internal review or Information Commissioner review under the FOI Act.

Required or authorised to refuse access under another Act

APP 12.2(b)(ii) provides that an agency is not required to give access to personal information if it is required or authorised to refuse to give access by another Act that provides for access by persons to documents. An example is a statutory secrecy provision that requires or authorises that access be refused in certain circumstances.

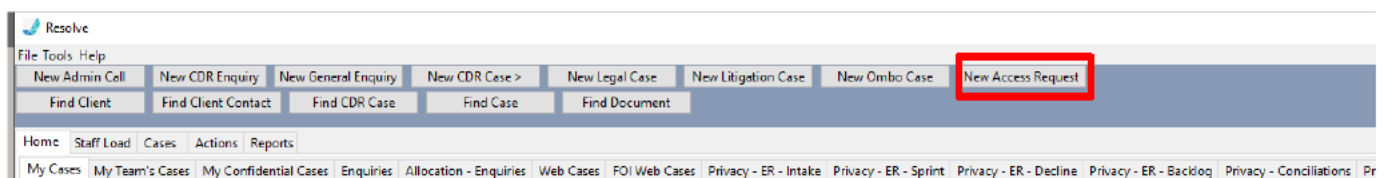
A further example is that the National Archives of Australia (**NAA**) is authorised to refuse access to certain 'exempt records' under the Archives Act 1983 (**Archives Act**). The Archives Act provides that the NAA must make available for public access Commonwealth records in the open access period that are in the care of the NAA and that are not exempt records (s 31 of the Archives Act). The categories of exempt records include information whose disclosure would constitute a breach of confidence, would involve the unreasonable disclosure of information relating to the personal affairs of any person, or would unreasonably affect a person adversely in relation to his or her business, financial or professional affairs (s 33 of the Archives Act).

Processing a request

Create a new Access request file in Resolve

On receipt of an APP 12 request a new Access Request file needs to be generated in Resolve.

In Resolve, click 'New Access Request' in the top menu ribbon:



A 'New Request Entry' will open:

The screenshot shows the OAIC case management system interface. It includes fields for Case Type, Case Number, Target Date, Priority, Case Officer, Retention Class, and COVID-19 Delay. A 'Requestor Details' section has a 'Find' button. Below this is a 'How Received' field, a 'Registered By' field, and a 'Summary' field. A 'Case Outcome' field is also present. An 'Open Actions' table is visible at the bottom right. Numbered callouts point to specific fields: 1 points to 'Case Type', 2 points to 'Find', 3 points to 'How Received', 4 points to 'Summary', 5 points to 'Open Actions', and 6 points to 'Case Outcome'.

1. Click on the 'Case Type' field and select 'APP 12' from the drop-down menu.
2. Click on find to locate the requestor details in Resolve and select the requestor. The requestor's details will populate the white field below. If the requestor's details are not in Resolve you will need to manually input the information.
3. Click on the 'How Received' field and select the appropriate option from the drop-down menu.
4. Copy and paste the scope into the Summary field directly from the request.
 - a. At this stage you can save your work. This will then generate the Resolve file number.
5. Complete the Action steps from 'Register Case', then 'Allocate to Case Officer', and 'Process Request'.
6. Once you have made your decision and provided the decision and any relevant records to the requestor select the 'Case Outcome': Granted, Not Granted, or Withdrawn.

You may then complete the final action and close the AR file.

Identifying the Scope

The first step when an APP 12 request is received is to identify the scope of the request.

For example, an individual may request access to a specific record that may contain their personal information. On the other hand, an individual may request access to 'all personal information' held by the OAIC.

It is important to identify the scope of the request as this will determine what searches you need to carry out to identify the relevant records and whether you need to consult with other staff members or other teams across the OAIC.

APP 12.4 – Dealing with an APP 12 request

APP 12.4 requires an agency to respond to a request within 30 days. The OAIC has previously held the view that this means that the response includes providing an acknowledgment of the request and providing access to the requested information (subject to any exceptions that may apply) within 30 days.

However, in a recent decision of the Federal Court¹ Snaden J held that APP 12.4 mandates two steps by which an APP entity must deal with APP 12 requests.² Snaden J found:

*[F]irst, by the provision of a response to the request; and, second, by the provision of access to the information as requested (subject to notions of reasonableness and practicality...). [APP 12.4] draws a distinction between “dealing with” a request by responding to it and “dealing with” a request by granting access to what is requested. **The 30-day deadline applies only in respect of the former.***³ (my emphasis)

This means that the OAIC is required by APP 12.4 to acknowledge receipt of the request within 30 days and the provision of access to the information requested can be done outside the 30-day time frame.

Whilst this means that where the OAIC does not provide access or a decision refusing access within 30 days, it is important to process the request in a timely manner. Best privacy practice requires that decisions on access requests are made within a reasonable time from receipt of the request.

Where the request is voluminous or complex, it will be appropriate to advise the individual that a decision may not be provided within 30 days and to assure the individual that the request will be actively progressed. You may wish to negotiate access to the information requested in tranches to ensure the matter is dealt with appropriately.

Search and retrieval of records

Once an APP 12 request has been acknowledged you should schedule time within the first week of receipt to identify where the information requested may be held.

Generally, APP 12 requests to the OAIC relate to complaint or IC Review file and the records sought will be held in those files. You may need to ask the relevant case officer for assistance in identifying records relevant to the scope of the request.

If you do need to ask other staff for assistance, a sample of a search and retrieval email can be found at Annexure A.

¹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328.

² *Knowles v Secretary, Department of Defence* [2020] FCA 1328 [67].

³ *Knowles v Secretary, Department of Defence* [2020] FCA 1328 [67].

Assessment of relevant records

APP 12 provides individuals with a general right to access their own personal information held by an APP entity. This general right is subject to exceptions, which for an agency are found at APP 12.2.

Once you have identified all records relevant to the scope of the request, you need to convert emails and Word documents to PDF and then combine all records into one document. Then you may assess the information for relevancy and whether the information is the personal information of the individual.

When assessing the information relevant to the access request, you should identify the information that may be:

- (a) outside the scope the request
- (b) the personal information about other individuals
- (c) deliberative or evaluative information, or
- (d) available in a generally available publication.

This information should be removed from an access grant before releasing the records to the individual.

Exceptions to providing access

By far the exception relied on most by agencies is APP 12.4(b)(i) whereby access may be refused on the grounds available under the FOI Act:

- a document is an exempt document under Part IV, Division 2 of the FOI Act, for example, the document is a Cabinet document, is subject to legal professional privilege, contains material obtained in confidence, or a secrecy provision applies
- a document is a conditionally exempt document under Part IV, Division 3 of the FOI Act, for example, the document contains deliberative matter, or disclosure of the document would involve the unreasonable disclosure of personal information about another person and it would be contrary to the public interest to release the document at that time
- the individual is not entitled to obtain access to a document of the kind requested, for example, the document is available for purchase from an agency (FOI Act, ss 12, 13)
- providing access in the terms requested by a person would substantially and unreasonably divert an agency's resources from its other operations (s 24AA)
- processing a person's request would require an agency to disclose the existence or non-existence of a document, where that would otherwise be exempt information (s 25).

Whilst the FOI Act specifies consultation processes that may apply to requests made under that Act, for example, where a 'practical refusal reason' may apply to the request,⁴ or where a requested document contains a third party's personal or business information,⁵ an agency is not required to

⁴ FOI Act, s 24.

⁵ FOI Act, ss 27, 27A.

undertake any of those consultation processes before refusing access on any of those grounds under APP 12.

A decision to refuse access under APP 12.2(b)(i) (on one of the FOI grounds listed above) is a decision made under the Privacy Act, not the FOI Act. As required by APP 12.9, the agency must provide the individual with a written notice that sets out the reasons for the refusal and the complaint mechanisms available to the individual. The individual may have a right to complain pursuant to s 36 of the Privacy Act to the Information Commissioner about the refusal decision. However, the individual will not have a right to seek internal review or Information Commissioner review under the FOI Act.

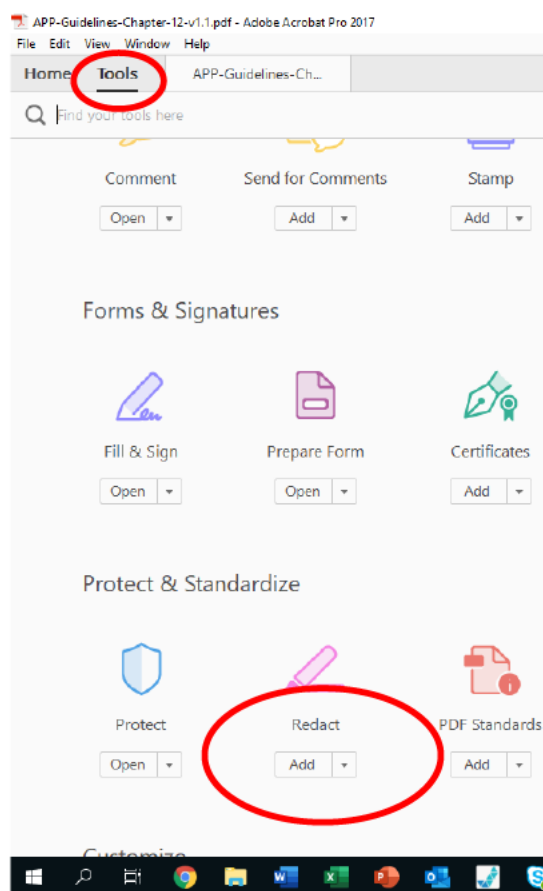
Redaction of information not in scope or otherwise not required to release

Once you have identified the information that is either irrelevant to the scope of the request or information that is not the individual's personal information, you will need to remove (or hide) that information by redacting it.

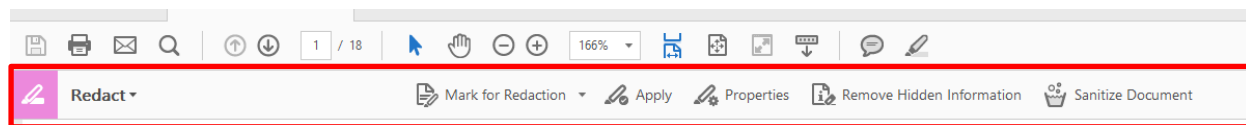
Redacting a document requires access to Adobe Pro 2017. There are limited licences available to the OAIC; however, some individuals in the Early Resolution team do have access to Adobe Pro as do the stand-up desks on level 2.

Redacting is a three-step process. First you need to 'Mark for redaction'. This involves the following steps:

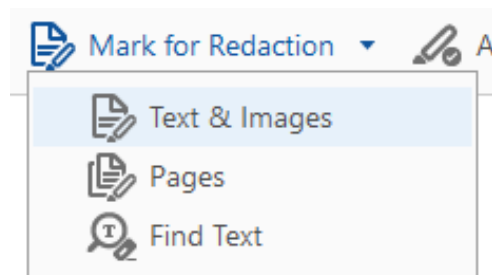
1. Go to 'Tools' in the document and scroll down to 'Redact'



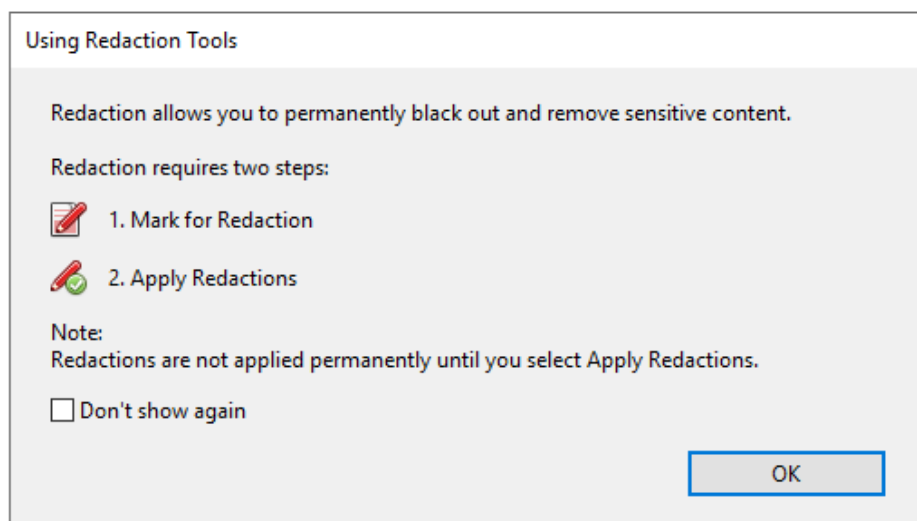
Once you have clicked on 'Redact' you will be taken back to the document you are working on. You will see a new ribbon at the top of the document:



Click on 'Mark for Redaction'. You will then see the drop-down menu:

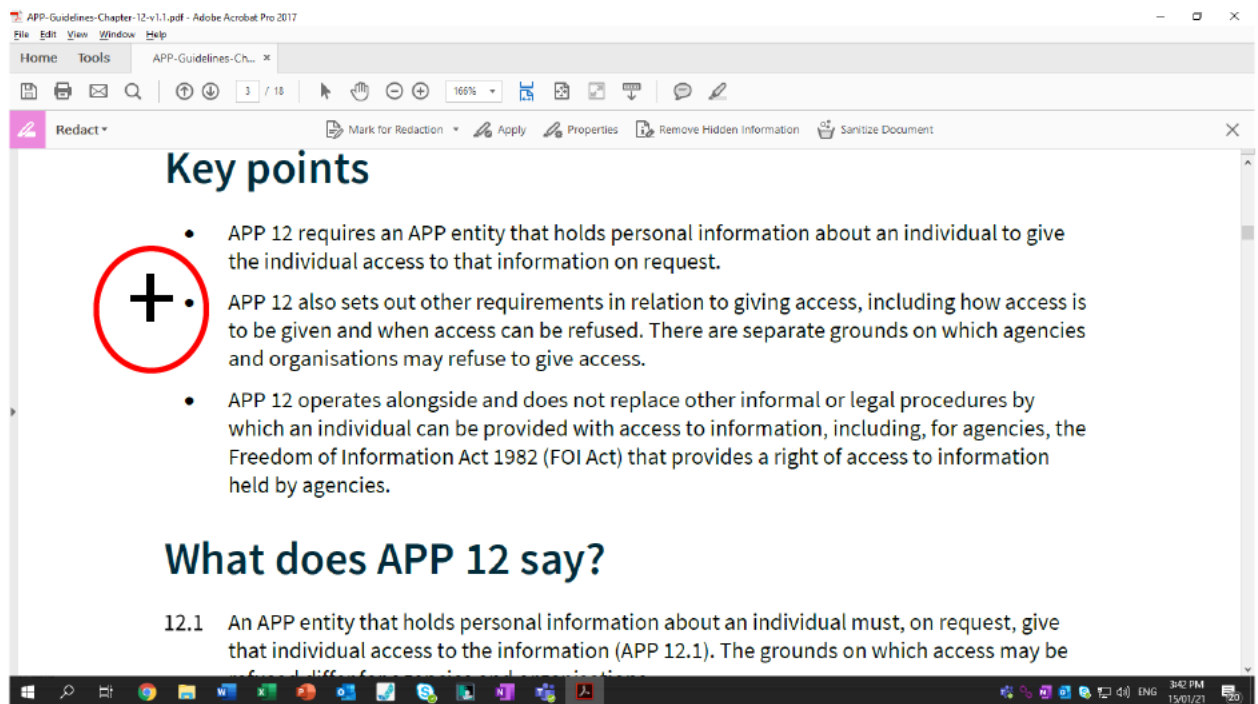


Select 'Text & Images'. You will then see the following text box:

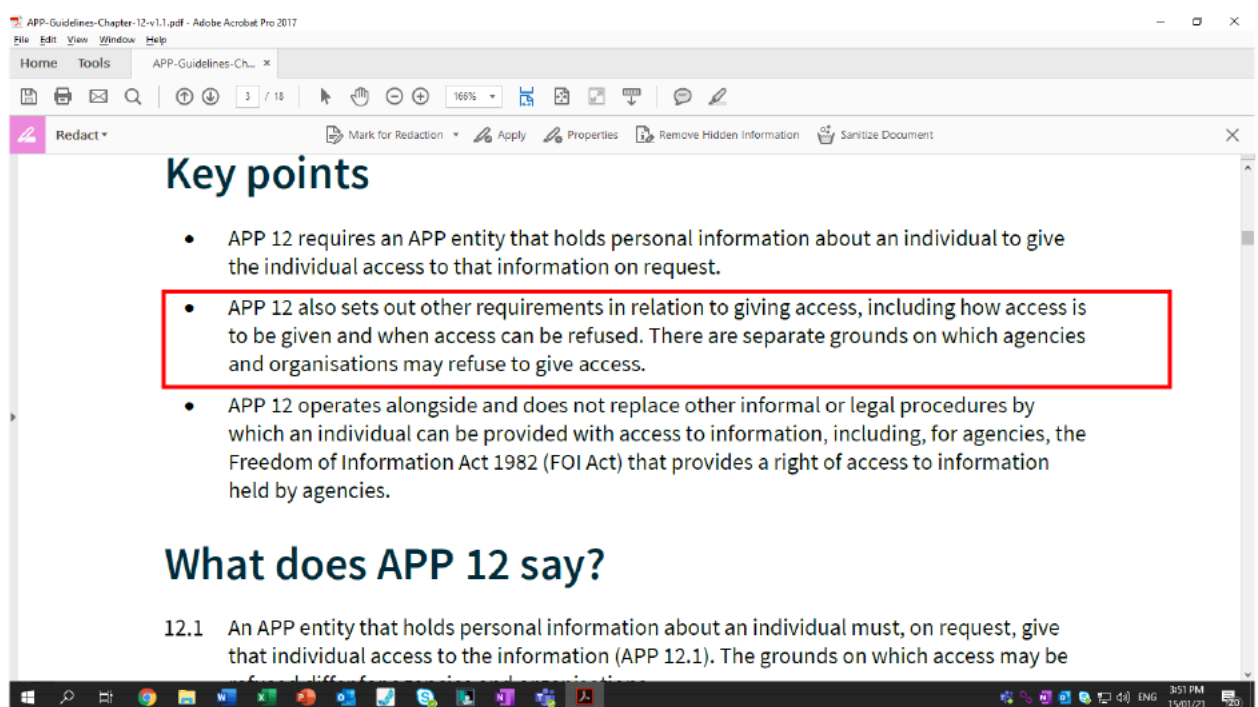


Click 'OK' and you are now ready to assess the information and mark up the document.

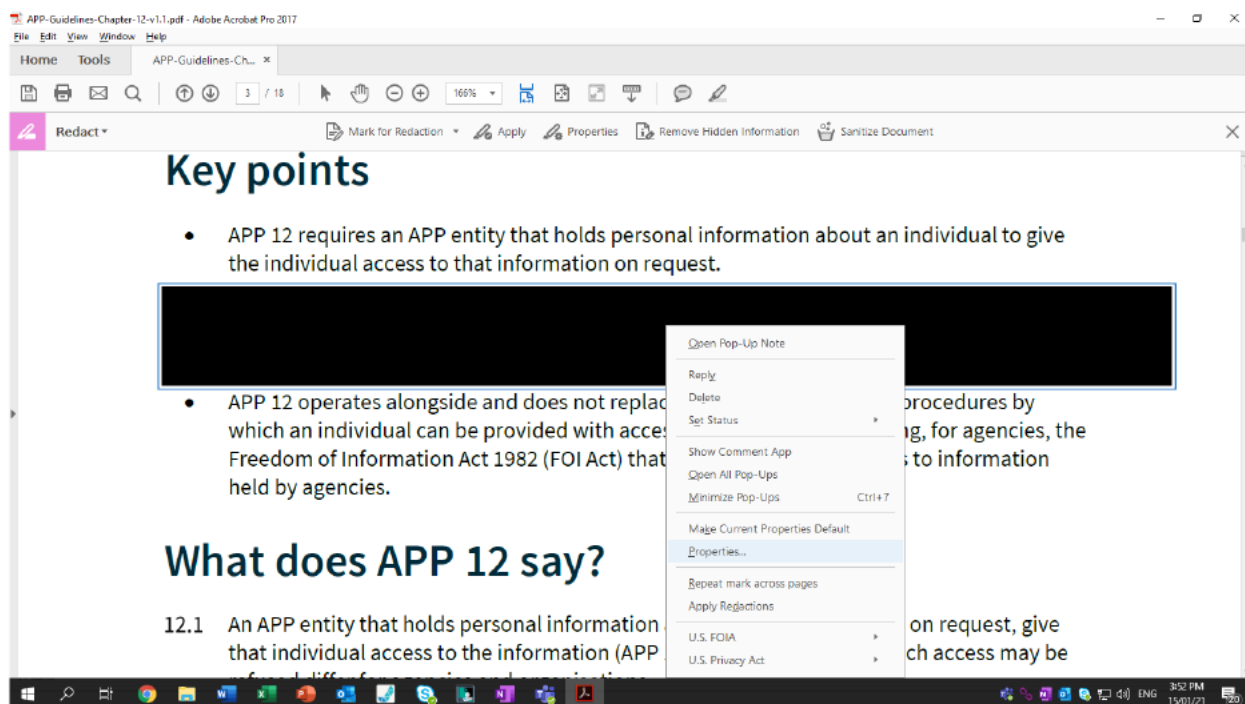
2. To mark up the document identify the information you want to redact. Place your cursor near the information until it forms a cross:



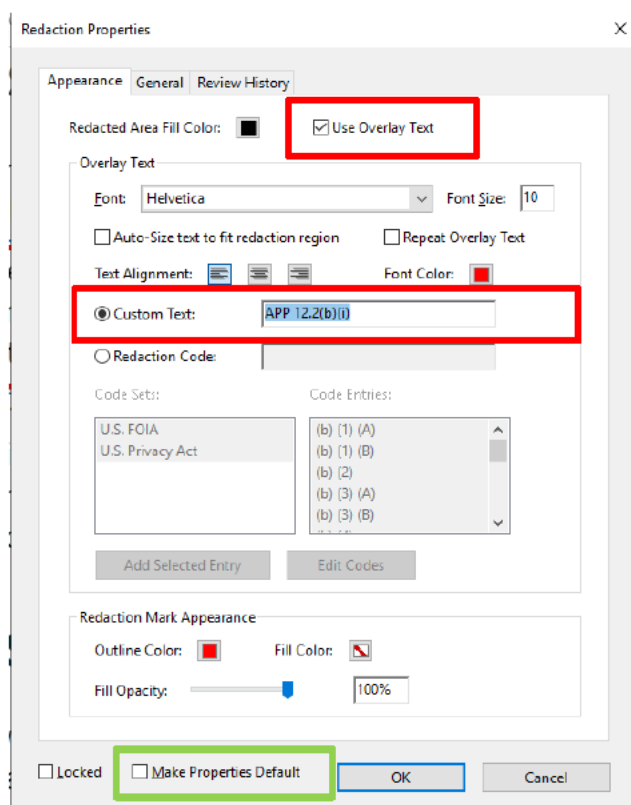
Then highlight the text you want to redact:



Within the selected area, right click and select 'Properties' from the drop-down menu:



Once you are in the properties box select the 'Use Overlay Text' tick box and type in 'APP 12.1(b)(i)' in the 'Custom Text' box:



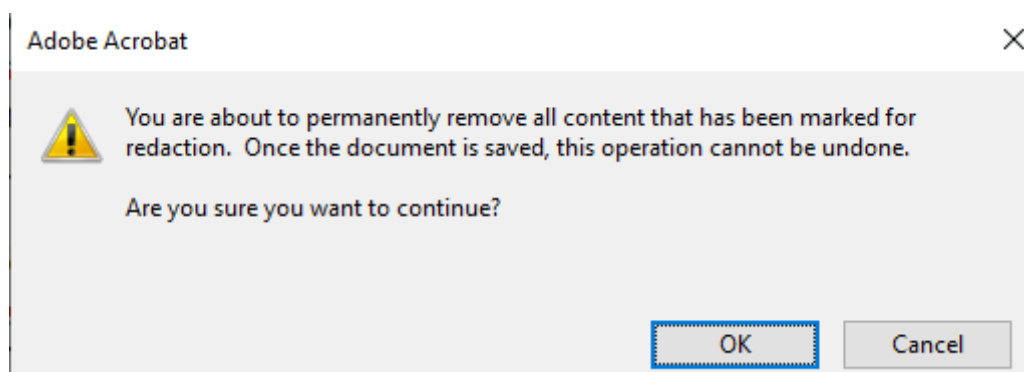
Press 'OK' to apply the properties to the document. For the sake of ease, you can set these properties as the default by checking the 'Make Properties Default' check box.

Proceed to review and mark up the entire document.

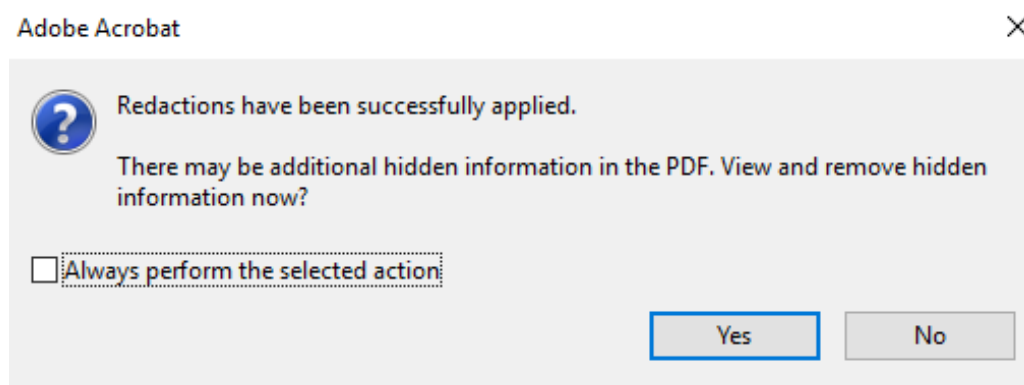
At this stage, the redactions have not been applied to the document. However, if you need your supervisor, or another team, to review the suggested redactions, you should save the document to your desktop and place on the relevant AR file. Once the document is in Resolve, delete the document from your desktop and work on the document as usual in Resolve.

Once you are satisfied that the appropriate redactions have been made the next step is to apply the redactions.

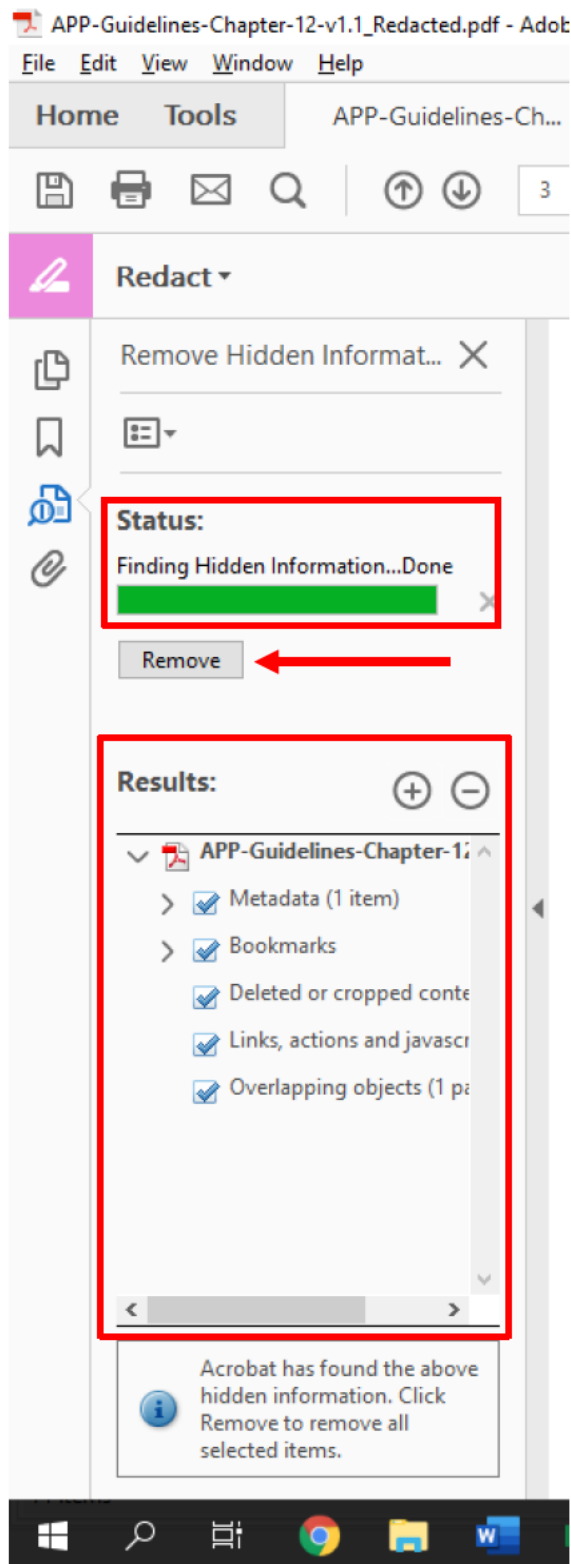
Select 'Apply' which is next to the 'Mark for Redaction' option you selected in step one. You will receive an alert:



Select 'OK' to proceed. You will then see another warning box:



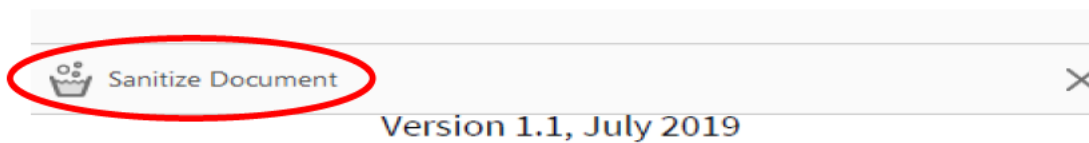
Select 'Yes' to continue. A side activity window will open on the left-hand side of the document:



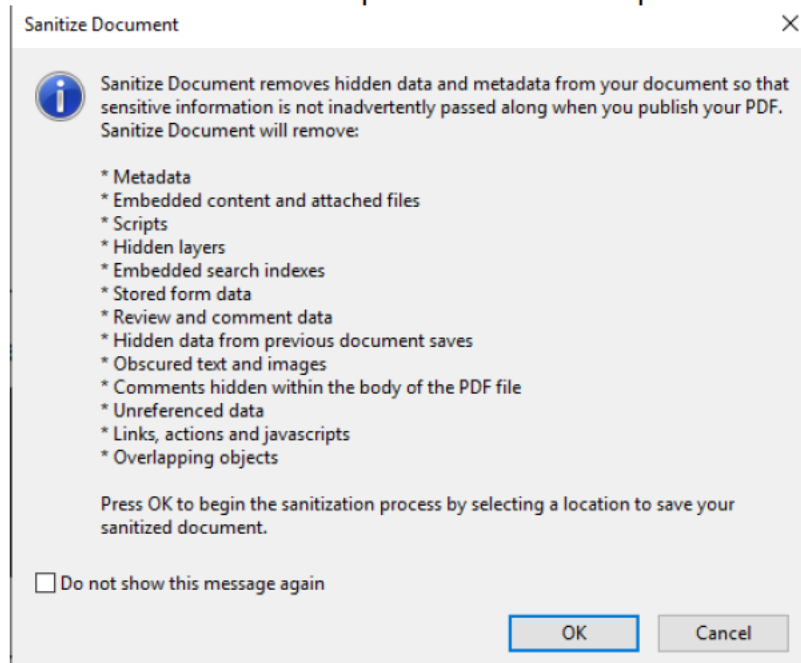
The 'Status' will show the progress of the application of the redactions and Adobe's search for hidden information. Once this is complete, select 'Remove'. This will remove the information listed in the 'Results' box below.

3. The third and final step in redacting the document is to Sanitise it.

Click on the 'Sanitize Document' option in the redaction ribbon at the top of the document:



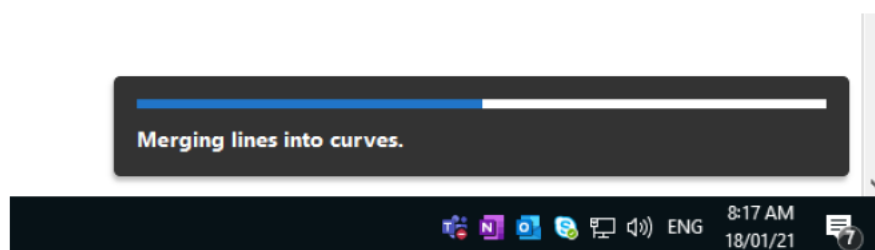
You will the see a box that explains the sanitisation process:



Click 'OK' to begin the sanitisation process. You will be asked to save the document.⁶ When you save the document include in the naming convention that this is the record to be released to the individual:

'AR20_00000 – Documents for release to A'

Once you have saved the document the sanitisation process will begin. You can see the progress here in the bottom right-hand corner of your screen:



⁶ As you will be working on the document in Resolve you will need to save the document to your desktop and move it into Resolve. Immediately delete this copy from your desktop once the document is in Resolve.

Decision

APP 12.9 requires an agency to notify an individual where it decides to refuse access to the personal information requested under APP 12.2 or to provide access to the requested information in the manner requested.

The decision should set out clearly:

- (a) the reasons for the refusal except to the extent that, having regard to the grounds of refusal, it would be unreasonable to do so; and
- (b) the mechanisms available to complain about the refusal; and
- (c) any other matter prescribed by the regulations.

It is important to note that the review rights available to an individual are slightly different to those available when the OAIC makes a decision under s 41 of the Privacy Act.

There are no internal review rights in relation to APP 12 decisions which differs from the right of internal review provided by the FOI Act.

Examples of APP 12 decisions are available at Annexure B.

APP 12 request check list

Date	Action	Completed
Click or tap to enter a date.	<ul style="list-style-type: none"> ➤ APP 12 request received ➤ Resolve file created ➤ Resolve case number: AR21/XXXX 	<input type="checkbox"/>
Click or tap to enter a date.	<ul style="list-style-type: none"> ➤ Scope identified: <i>[INSERT SCOPE]</i> 	<input type="checkbox"/>
Click or tap to enter a date.	<ul style="list-style-type: none"> ➤ Search and retrieval request sent and added to Resolve 	<input type="checkbox"/>
Click or tap to enter a date.	<ul style="list-style-type: none"> ➤ Relevant records received in PDF format, or ➤ Relevant records identified and converted to PDF format, combined into one PDF document and placed on Resolve 	<input type="checkbox"/>
Click or tap to enter a date.	<ul style="list-style-type: none"> ➤ Relevant records assessed for information outside of the scope, personal information of third parties and/or information that would be exempt under the FOI Act. PDF document marked for redaction 	<input type="checkbox"/>
Click or tap to enter a date.	<ul style="list-style-type: none"> ➤ Draft decision completed and placed on Resolve 	<input type="checkbox"/>
Click or tap to enter a date.	<ul style="list-style-type: none"> ➤ Draft decision and proposed redactions reviewed by Supervisor and approved 	<input type="checkbox"/>
Click or tap to enter a date.	<ul style="list-style-type: none"> ➤ Apply redactions and sanitise documents for release ➤ Finalise the decision and convert to PDF 	<input type="checkbox"/>
Click or tap to enter a date.	<ul style="list-style-type: none"> ➤ Send decision and documents to the Applicant ➤ Close Resolve file 	<input type="checkbox"/>

Annexure A

Sample search and retrieval email

Subject: AR21/XXXXX – APP 12 request

Dear [STAFF]

I refer to [APPLICANT]'s APP 12 request made to the OAIC.⁷

Under APP 12 [APPLICANT] has requested:

[INSERT SCOPE OF REQUEST]

Please search your Outlook, Content Manager and H:Drive for records within the scope of the request.

Please provide any record relevant to the scope of the request in PDF format by [GIVE 7 DAYS].

[EMAIL SIGNATURE]

⁷ If you consider that attaching the original request will assist the staff member please attach the request.

Annexure B

Sample APP 12 Decisions

Our reference: AR21/XXXXX

[APPLICANT]

[ADDRESS]

By email: [EMAIL@EMAIL.COM.AU]

Your access request under APP 12

Dear [APPLICANT],

I refer to your request for access to your personal information under APP 12 in Schedule 1 to the *Privacy Act 1988* (Cth) (**Privacy Act**), received by the Office of the Australian Information Commissioner (**OAIC**) on [DATE RECEIVED].

Your Request

In your request you seek access to the following:

[INSERT SCOPE]

Decision

References to provisions in this decision record are those in the Privacy Act unless otherwise specified.

Relevant provisions - Privacy Act

Under s 6(1) “personal information” is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Section 6(1) further provides that an APP entity “holds” personal information if the entity has possession or control of a record that contains the personal information.

Australian Privacy Principle (**APP**) 12 states that if an APP entity holds personal information about an individual the entity must, on request by the individual, give the individual access to the information unless a specific exemption applies.

APP 12.2 provides that an agency is not required to give access to personal information if it is authorised to refuse access under the *Freedom of Information Act 1982* (**FOI Act**).

APP 12.5 provides that if an APP entity refuses to give access to personal information in the manner requested by the individual, it must take reasonable steps to give access in a way that meets the needs of the individual. Under the OAIC's Australian Privacy Principles Guidelines (July 2019) (**APP Guidelines**), this can include giving a summary of the requested personal information to the individual.

APP 12.9 provides that if an APP entity refuses to give access, or to give access in the manner requested by the individual, the entity must give the individual written notice setting out a number of matters, including the reasons for the refusal, except to the extent that it would be unreasonable to do so, having regard to the grounds of refusal.

Findings

I have located [# OF RECORDS] records which contain your personal information.

Of the records held by the OAIC found to be within scope, I have decided to grant access [STATE WHAT YOU ARE GRANTING ACCESS TO].⁸

[I have refused access to your personal information held in 12 records in full.]⁹

[I have refused access to information held in the records released where that information is not your personal information as defined by s 6(1) of the Privacy Act.]¹⁰

I set out my reasons for refusing access as follows.

Reasons for decision

I have decided to [**grant access in full/refuse access**] to the personal information held in [THE NUMBER OF RECORDS] records for the following reasons.

[In relation to document numbers [INSERT DOCUMENT NUMBERS] access is refused pursuant to APP 12.2(b)(i). This is because [INSERT REASONS FOR REFUSAL].]

[In relation to document numbers [INSERT DOCUMENT NUMBERS], these records contain redaction of information that is either not your personal information or is information not within the scope of your APP 12 request.

Your options

Your review rights are provided below.

⁸ If you are granting access to all records you need go no further.

⁹ Use this option if you are refusing access under APP 12.2(b)(i).

¹⁰ Use this option if you have redacted other individual's personal information.

Judicial review

If you consider that the OAIC erred in law in the relevant decisions, you may wish to seek judicial review of the decision. The court will not review the merits of your request but may refer the matter back to us to reconsider — if they find our decision or determination was wrong in law or we didn't exercise our powers properly.

For more information about a judicial review, visit the Federal Court of Australia's website: <https://www.fedcourt.gov.au/>

Privacy complaint

You may make a privacy complaint to the OAIC as a regulator under s 36 of the Privacy Act. Further information about privacy complaints can be found at <https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us/>

Ombudsman complaint

If you have a complaint about the outcome of your access requests, or the way in which they have been handled, you may write to enquiries@oaic.gov.au or contact the Commonwealth Ombudsman on 1300 363 072.

Freedom of Information

Alternatively, you may make a Freedom of Information (FOI) request. To make an FOI request you must:

- make the request in writing
- state that it is an application for the purposes of the *Freedom of Information Act 1982* (Cth)
- provide information that clearly identifies the documents/information you seek
- provide details about how notices can be sent to you (this can include an email address)
- send your request to foi@oaic.gov.au, fax it to (02) 9284 9666, or post it to OAIC.

Yours sincerely

[Signature]

[Title]

[Date]

Our reference: AR21/XXXXX

[APPLICANT]

By email: [EMAIL@EMAIL.COM.AU]

Your access request under APP 12

Dear [APPLICANT],

I refer to your request for access to your personal information under APP 12 in Schedule 1 to the *Privacy Act 1988* (Cth) (**Privacy Act**), received by the Office of the Australian Information Commissioner (**OAIC**) on [DATE RECEIVED].

Your Request

In your request you seek access to the following:

[INSERT SCOPE]

Decision

References to provisions in this decision record are those in the Privacy Act unless otherwise specified.

Relevant provisions - Privacy Act

Under s 6(1) “personal information” is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Section 6(1) further provides that an APP entity “holds” personal information if the entity has possession or control of a record that contains the personal information.

Australian Privacy Principle (**APP**) 12 states that if an APP entity holds personal information about an individual the entity must, on request by the individual, give the individual access to the information unless a specific exemption applies.

APP 12.2 provides that an agency is not required to give access to personal information if it is authorised to refuse access under the *Freedom of Information Act 1982* (**FOI Act**).

APP 12.5 provides that if an APP entity refuses to give access to personal information in the manner requested by the individual, it must take reasonable steps to give access in a way that meets the needs of the individual. Under the OAIC’s Australian Privacy Principles Guidelines (July 2019) (**APP Guidelines**), this can include giving a summary of the requested personal information to the individual.

APP 12.9 provides that if an APP entity refuses to give access, or to give access in the manner requested by the individual, the entity must give the individual written notice setting out a number of matters, including the reasons for the refusal, except to the extent that it would be unreasonable to do so, having regard to the grounds of refusal.

Findings

I have decided to provide you access to the four records held by the OAIC falling within the scope of your request.

I set out my reasons for my decision below.

Reasons for decision

On receiving your request, to ensure all reasonable steps were taken, [STAFF MEMBER] undertook searches for records within the scope of your request.

[STAFF MEMBER] reviewed our files in relation to your request and searched their Outlook files, local hard drive, case management system, Content Manager system and paper files. [STAFF MEMBER] located the **attached** records relevant to the scope of your request.

I have reviewed the relevant files and the records identified as relevant to your APP 12 request. I agree that the records are relevant to your request and I provide you access to the records.

Your options

Your review rights are provided below.

Judicial review

If you consider that the OAIC erred in law in the relevant decisions, you may wish to seek judicial review of the decision. The court will not review the merits of your request but may refer the matter back to us to reconsider — if they find our decision or determination was wrong in law or we didn't exercise our powers properly.

For more information about a judicial review, visit the Federal Court of Australia's website: <https://www.fedcourt.gov.au/>

Privacy complaint

You may make a privacy complaint to the OAIC as a regulator under s 36 of the Privacy Act. Further information about privacy complaints can be found at <https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us/>

Ombudsman complaint

If you have a complaint about the outcome of your access requests, or the way in which they have been handled, you may write to enquiries@oaic.gov.au or contact the Commonwealth Ombudsman on 1300 363 072.

Freedom of Information

Alternatively, you may make a Freedom of Information (FOI) request. To make an FOI request you must:

- make the request in writing
- state that it is an application for the purposes of the *Freedom of Information Act 1982* (Cth)
- provide information that clearly identifies the documents/information you seek
- provide details about how notices can be sent to you (this can include an email address)
- send your request to foi@oaic.gov.au, fax it to (02) 9284 9666, or post it to OAIC.

Yours sincerely,

[SIGNATURE]

[TITLE]

[DATE]

Our reference: AR21/XXXXX

[APPLICANT]

By email to: [EMAIL@EMAIL.COM.AU]

Your APP 12 request for access to a document

Dear [APPLICANT]

I refer to your email to the Office of the Australian Information Commissioner (**OAIC**) dated 1 July 2020, in which you requested access to the following document under Australian Privacy Principle (**APP**) 12 of the *Privacy Act 1988*:

[INSERT SCOPE]

I have looked for the document you requested, that is, a document [DESCRIBE THE DOCUMENT REQUESTED]. I did not find a document meeting this description.

To look for this document I searched the case management file for [RESOLVE FILE NUMBER]. This case file holds all the documents relevant to your [IC review application/privacy complaint] dated [DATE].

I am therefore refusing you access to the document you requested on the basis that the OAIC does not have this document in its possession.

Your options

Your review rights are provided below.

Judicial review

If you consider that the OAIC erred in law in the relevant decisions, you may wish to seek judicial review of the decision. The court will not review the merits of your request but may refer the matter back to us to reconsider — if they find our decision or determination was wrong in law or we didn't exercise our powers properly.

For more information about a judicial review, visit the Federal Court of Australia's website:

<https://www.fedcourt.gov.au/>

Privacy complaint

You may make a privacy complaint to the OAIC as a regulator under s 36 of the Privacy Act. Further information about privacy complaints can be found at <https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us/>

Ombudsman complaint

If you have a complaint about the outcome of your access requests, or the way in which they have been handled, you may write to enquiries@oaic.gov.au or contact the Commonwealth Ombudsman on 1300 363 072.

Freedom of Information

Alternatively, you may make a Freedom of Information (FOI) request. To make an FOI request you must:

- make the request in writing
- state that it is an application for the purposes of the *Freedom of Information Act 1982* (Cth)
- provide information that clearly identifies the documents/information you seek
- provide details about how notices can be sent to you (this can include an email address)
- send your request to foi@oaic.gov.au, fax it to (02) 9284 9666, or post it to OAIC.

Yours sincerely

[SIGNATURE]

[TITLE]

[DATE]

Annexure C

Case note: Knowles v Secretary, Department of Defence [2020] FCA 1328

Case citation	<i>Knowles v Secretary, Department of Defence</i> [2020] FCA 1328
Court/Tribunal	Federal Court of Australia
Date	17 September 2020
Parties	Kieran John Murray Knowles Applicant Secretary, Commonwealth Department of Defence Respondent
Court reference	VID416/2017
Legislation cited	<i>Administrative Decisions (Judicial Review) Act 1977</i> (Cth) – ss 3, 5, 6, 7, 10 and 16 <i>Federal Court of Australia Act 1976</i> (Cth) – s 21 <i>Freedom of Information Act 1982</i> (Cth) <i>Judiciary Act 1903</i> (Cth) – s 39B <i>Privacy Act 1988</i> (Cth) – Sch 1; Pt V; Pt VIB; ss 6, 6A, 13, 15, 36, 40, 41, 52, 55A, 80W, 96 <i>Regulatory Powers (Standard Provisions) Act 2014</i> – Pt 7; ss 118, 119, 120 and 121
Catchwords	ADMINISTRATIVE LAW – judicial review – decisions made by the respondent in relation to applications made under the <i>Privacy Act 1988</i> (Cth) (hereafter, the “ Privacy Act ”) for access to and correction of certain information – various species of relief sought – whether Privacy Act mandates provision of access to information within 30 days – appropriateness of declaratory relief – whether existence of other remedies for the review of administrative decisions should incline the court against granting prerogative or other relief – whether private information might be corrected by associating or attaching other documents to it – whether a demand that information be destroyed qualifies as a request for correction under the Privacy Act – further amended originating application dismissed with costs
Privacy Act	<i>Privacy Act 1988</i> (Cth) – Sch 1; Pt V; Pt VIB; ss 6, 6A, 13, 15, 36, 40, 41, 52, 55A, 80W, 96
Paragraphs of interest	All
Case note	Author: Delaney Smith

Contents

<u>Case note</u>	30
<u>Citation</u>	30
<u>Parties</u>	30
<u>Court</u>	30
<u>Date of judgment</u>	30
<u>Statement of material facts</u>	30
<u>Procedural history</u>	33
<u>Summary of the court's analysis</u>	33
<u>The court's decision</u>	39
<u>Orders made by the court</u>	39
<u>Court judgment</u>	40

Case note

Citation

Knowles v Secretary, Department of Defence [2020] FCA 1328.

Parties

Kieran John Murray Knowles

Applicant

Secretary, Commonwealth Department of Defence

Respondent

Court

Federal Court of Australia

Date of judgment

17 September 2020

Statement of material facts

In 2011, the Applicant was the subject of communication/s between the Respondent and Department of Veterans' Affairs (**DVA**) (see: ***DO and Department of Veterans' Affairs* [2014] AICmr 124¹¹ (OAIC Determination)**).¹²

In May 2016, the Applicant made an application under Australian Privacy Principle (**APP**) 12 of sch 1 of the *Privacy Act 1988* (Cth) (**Privacy Act**) for access to his personal information held by the Respondent and later a further request for access to documents under the *Freedom of Information Act 1982* (Cth) (**FOI Act**).¹³

On 25 November 2016 (**25 November APP 12 request**), the Applicant sent an email to the Respondent titled 'PI access under [APP] 12'.¹⁴

The Respondent acknowledged the November request the following week. The Applicant subsequently emailed the Respondent enquiring about 'the due date for a decision (just so we lock this down)'. The Respondent advised the Applicant:

¹¹ This decision was set aside by *TYGJ and Information Commissioner* [2017] AATA 156 and subsequently affirmed by *AIT18 v Australian Information Commissioner* [2018] FCAFC 192.

¹² *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [6].

¹³ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [7].

¹⁴ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [8].

Dear [Applicant]

... we will endeavor to action your request... as soon as possible [however] I am unable to provide an expected date for a response...¹⁵

On 1 December 2016, the Applicant sent the Respondent and email stating:

I believe... that legislation wise, the required processing period is 30 calendar days...¹⁶

On 22 December 2016, the Respondent provided a partial grant of access to some documents within the scope of the Applicant's request and advised by email:

[The Respondent has] asked... other areas [in the Respondent]... to review their records and identify what relevant personal information they may hold. Further [the Respondent]... asked them to advise their agreement to release, including reasons if they consider documents should be redacted or not released.

Unfortunately, [the Respondent has] not yet received responses to [its] requests. At this stage [the Respondent was] unable to provide an expected date for further response however [the Respondent] will keep [the Applicant] updated. Just to clarify, [the Respondent] is not refusing access.¹⁷

The Applicant responded later that day and provided the Respondent further time to complete his request.¹⁸

On 23 December 2016, the Respondent sent emails to various areas throughout the Respondent seeking assistance in responding to the Applicant's November request (**Assistance Request Emails**).¹⁹

On 30 January 2017, the Applicant sent a further email to the Respondent.²⁰ Soon after, the Applicant lodged a privacy complaint with the OAIC about the Respondent's response (or partial) response to the 25 November 2016 APP 12 request (**OAIC complaint**). The Applicant claimed the Respondent interfered with his privacy by failing to provide him access to his personal information by filing to provide access to the information requested within 30 days.²¹

The Respondent sent the Applicant the requested information in tranches during February 2017. In response to the Respondent's February 2017 emails, the Applicant made claims that the Respondent failed to provide access to all the information he sought.²²

¹⁵ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [9].

¹⁶ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [10].

¹⁷ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [11].

¹⁸ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [12].

¹⁹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [13].

²⁰ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [14].

²¹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [15].

²² *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [16-17].

On 2 March 2017, the Applicant again emailed the Respondent requesting the Respondent to attach or associate with his personal information a s 52 of the Privacy Act determination (**2 March APP 13 Request**).²³

On 3 March 2017, the Applicant emailed the Respondent demanding it destroy what the Applicant described as ‘defamatory claims’ about him from the Respondents records (**3 March Demand Email**). The information the Applicant demanded to be destroyed is held in an email from the Respondent to the Applicant dated 2 March 2017 whereby the Respondent addressed the Applicant’s claim regarding the conduct of the officer dealing with his requests.²⁴

On 6 March 2017, the Respondent distributed the 2 March APP 13 Request and asked various departments within the Respondent to take steps to address the request and provided a copy of the OAIC determination.

On 9 April 2017, the Applicant requested an update on the progress of his APP 13 requests. The following day, the Respondent replied to the Applicant and advised him that the OAIC determination had been sent to four departments within the Respondent and that it had asked those departments to include a copy of the determination in the Applicant’s records. The Respondent confirmed that two departments had included the determination in the Applicant’s records, one department had not made any annotation and the remaining department was currently processing the request.²⁵

Later in 2017, the Applicant commenced proceedings in the Federal Court against the OAIC.²⁶ The proceedings related, among other things, the OAIC complaint.²⁷ The proceedings were ultimately summarily dismissed. The reference to the APP 12 request as noted at paragraph [19] of the 2017 proceedings is a reference to the Applicant’s 30 January 2017 complaint to the OAIC relating to his 25 November 2016 APP 12 request.²⁸

The OAIC ultimately closed the Applicant’s complaint under s 41(2)(a).²⁹ Snaden J in his decision stated that ‘there is no evidence that [the Applicant] has sought to challenge that [decision], nor that he complained to the [OAIC] in respect of the [Respondent’s] response (or failure to respond) to his 2 March APP 13 request or his 3 March Demand email’.³⁰

The Applicant sought declaratory relief to record that the Respondent contravened APP 12 and APP 13 by not providing him access to his personal information within 30 days and by failing to respond to his APP 13 requests within 30 days.

²³ ‘DO’ and Department of Veterans’ Affairs [2014] AICmr 124. This determination was subsequently set aside by the AAT (see: *TYGJ and Information Commissioner* [2017] AATA 1560) and the Full Federal Court upheld the AAT decision (see: *AIT18 v Australian Information Commissioner* [2018] FCAFC 192).

²⁴ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [20-22].

²⁵ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [27-28].

²⁶ *Knowles v Australian Information Commissioner* [2018] FCA 1212 (Tracey J)

²⁷ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [30].

²⁸ *Ibid.*

²⁹ See: CP17/00171.

³⁰ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [33].

Procedural history

This was an originating application.

Summary of the court’s analysis

APP 12 – access to personal information

Snaden J held that he was not persuaded that the Applicant’s claims about the Respondent’s conduct (that it contravened the Privacy Act by failing to address his 25 November APP 12 Request within 30 days and that its handling of the request was tainted by bad faith) was well founded.³¹

His Honour addressed both the 30-day time frame and the Applicant’s claim regarding bad faith. In relation to the 30-day time frame set out in APP 12.4 the court held that the requirement at APP 12 is not that:

‘... access to requested personal information must be granted within 30 days; it is that the request must be responded to within that timeframe.’³²

The court stated that the Respondent had in fact responded to the Applicant’s request within 30 days and that this issue was not in dispute between the parties and that the Respondent provided documents in partial satisfaction of it within 30 days.³³

The court found that the terms of APP 12 reinforce that division. Relevantly, the court found:

‘Paragraph 12.4... is headed “Dealing with requests for access”. It mandates two measures by which an APP Entity must deal with requests for access to information under APP 12: first, by the provision of a response to the request; and, second, by the provision of access to the information as requested (subject to notions of reasonableness and practicality...). The instrument draws a distinction between “dealing with” a request by responding to it and “dealing with” a request by granting access to what is requested. The 30-day deadline applies only in respect of the former.’³⁴

The court stated that even if it had taken a different view about the appropriateness of declaratory relief to address this aspect of the Applicant’s complaint, it would not have been persuaded that the Respondent had contravened APP 12, or any other part of the Privacy Act, by failing to provide the Applicant access to his personal information within 30 days to his access request.³⁵

Further, the court held that the Respondent’s response to the 25 November Request and its handling of the request did not amount to bad faith and found that the Respondent had not acted unlawfully by responding to the 25 November Request in a manner that bespoke bad faith.³⁶

³¹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [65].

³² *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [66].

³³ *Ibid.*

³⁴ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [67].

³⁵ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [68].

³⁶ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [69-74].

APP 13 – correction of personal information

In 2014, the OAIC ruled on a complaint that the Applicant had made about the Department of Veterans' Affairs (**DVA**).³⁷ The Commissioner determined that DVA had interfered with the Applicant's privacy and declared that DVA were to provide the Applicant with an apology and to conduct a review of its privacy complaint management process (to be conducted by an external provider).³⁸

By his 2 March 2017 APP 13 request, the Applicant sought correction of the Respondent's records insofar as the related to the statements of opinion that were inconsistent with the OAIC Determination.³⁹

The conduct engaged in by the Respondent in response to the 2 March APP 13 Request was not contested: certain records of the Respondent were annotated by having attached to the record/s a copy of the OAIC Determination. The Applicant contends that that course was not open to the Respondent. The Applicant maintained that the Respondent should have, in the first instance, made a decision one way or the other as to whether or not it would correct the personal information it held. The Applicant claimed that the Respondent was obligated to tell him as much and provide him reasons justifying that course. Then, and only then, was it open to the Applicant to ask the Respondent to associate a copy of the OAIC Determination with the relevant record/s.⁴⁰

Snaden J stated that APP 13 required the Respondent to respond to the 2 March APP 13 Request within 30 days and that, while the statutory requirement could be clearer, there seemed to be some merit in the Applicant's claims that that required, within 30 days, an indication from the Respondent as to whether it would or would not correct the Applicant's personal information as requested.⁴¹

His Honour also noted that the Applicant, while apparently familiar with the provisions of the Privacy Act that offer him a statutory right to make a complaint about the Respondent's acts or practices, the Applicant had not in fact availed himself of those rights.

In relation to the Applicant's claims that the Respondent unlawfully annotated his records, the court held that the Respondent was compelled to take reasonable steps to correct the personal information it held and was about the Applicant. The court stated:

"Correction", in that sense, required the taking of steps to ensure that that information was "accurate, up to date, complete, relevant and not misleading"...⁴²

The court referred to the Applicant's request that was aimed at the opinions of DVA and the Respondent's records in which those opinions were recorded. The court stated that it was difficult to see how records that contained (or otherwise referred to) those opinions might be thought to have been inaccurate, out of date, incomplete or irrelevant. The Applicant's contention was that the opinions were unsubstantiated and this view (until it was set aside) was validated by the OAIC

³⁷ Although this decision does not name DVA, as this is an internal document and staff are aware of the Applicant's complaints and relevant determinations, DVA is named in this case note.

³⁸ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [76] referring to 'DO' and *Department of Veterans' Affairs* [2014] AICmr 124.

³⁹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [77].

⁴⁰ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [79].

⁴¹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [83].

⁴² *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [90].

Determination. However, the court found that this does not demonstrate that the Respondent's records inaccurately recorded the opinions or that the opinions had since been altered or qualified such that the records in question were no longer up to date or were otherwise incomplete, or irrelevant in some way.⁴³

The court went on to state that APP 13 does not require an APP entity to take any particular steps by way of correction of information. The court stated:

*'there is, in my view, no reason why a record that is misleading because it records an opinion that has subsequently been the subject of judicial or quasi-judicial criticism or repudiation might not be "corrected" – that is to say, rendered not misleading – by annexing to it a record of that criticism or repudiation.'*⁴⁴

In response to the Applicant's submission that the association of the OAIC Determination was something that could only be done at his request and only following a decision by the Respondent that it would not take steps to correct the record and reasons for the refusal, the court stated it disagreed with the Applicant's submissions.⁴⁵

His Honour stated that he did not accept that the Respondent misunderstood its obligations or otherwise acted inconsistently with them in relation to the 2 March APP 13 Request. Snaden J went on to find:

*"it is apparent that the [Respondent] resolved to correct the records [the Applicant] asked it to correct. That it did so is hardly surprising given the existence... of the OAIC Determination which rendered the opinions about [the Applicant]... unsustainable. The [Respondent] did not communicate its resolution to [the Applicant] and it probably should have. But regardless, it was entitled to see to that correction by the means it adopted... Indeed, doing so was at least superficially consistent with what [the Applicant] had requested. Having opted to take that course, the [Respondent] was not obliged to provide [the Applicant] with a notice under paragraph 13.3 of APP 13, and [the Applicant] was not entitled to initiate the process for which paragraph 13.4 of APP 13 provides."*⁴⁶

The court then turned its mind to the 3 March Demand email. In this email, the Applicant demanded that the Respondent destroy certain information contained in an email from the Respondent to him. The Applicant submitted that he had made an APP 13 request regarding that information and that the Respondent failed to process his request within 30 days.

In coming to its decision, the court considered the character of the 3 March Demand Email and the exchange that precipitated the request. The exchange began on 2 March 2017 with the Applicant's 2 March APP 13 Request. The Respondent replied to that request asking for a copy of the OAIC Determination. The Applicant responded and provided a link to the Determination and made inferences that the Respondent ought to have known about the Determination and threatened to 'eventually' subpoena the Respondent, to subject the Respondent staff member to cross examination

⁴³ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [91].

⁴⁴ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [92].

⁴⁵ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [93-94].

⁴⁶ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [94].

and expose the staff member's 'disgraceful behaviour' on a permanent court record'. The Applicant also suggested that the staff member was 'lazy or ignorant'.⁴⁷

In response to the Applicant's provocations the Respondent replied by apologising to the Applicant for any appearance of laziness or ignorance and that the staff member was not the Respondent's Privacy Officer nor was he legally trained in privacy matters.⁴⁸

The court took particular notice of one paragraph in the Respondent's response to the Applicant:

*'I understand that I am currently the focal point of your frustrations with [the Respondent] and you hold me personally responsible for [the Respondent's] responses to date – I assume your expletives and threats are only a reflection of this frustration and do not imply a serious threat to my health or safety.'*⁴⁹

By the Applicant's 3 March Demand Email, the Applicant described those comments as 'defamatory' and demanded that they be 'destroy[ed]... from [the Respondent's] records'. The Applicant also threatened the staff member with action against him if the Applicant's demand was not met. The court considered whether the staff member's remark was in fact the Applicant's personal information; however, it did, with reluctance accept that the remark did constitute the Applicant's personal information and proceeded on that basis.⁵⁰

Hi Honour summarised the issue in the following way:

'It was a statement of opinion about what [the Respondent's staff member] understood was conveyed by the intemperate language of [the Applicant's] earlier emails: specifically, that [the Applicant] was frustrated; but not to the point that he posed a threat to [the staff member's] health or safety. That conclusion appears very much to align with reality: [the Applicant] was plainly frustrated with the manner in which the [Respondent] had responded to his prior requests for information but there is no evidence that that frustration risked expression in the form of physical threats or aggression aimed at [the staff member]. It is difficult to see how [the staff member's] opinion was wrong, much less defamatory.'

The court then considered whether the 3 March Demand Email equated to a request for correction under APP 13. The court found that although the Applicant clothed his demand in the language of the Privacy Act and his demand that the Respondent 'destroy these defamatory claims from [the Respondent's] records about threatening behaviour' was expressly said to be required under APP 13. However, Snaden J found that those words alone are not sufficient to constitute the email as a request for correction of information under APP 13.⁵¹

Snaden J went on to state that there are two ways in which an APP entity may be obliged to correct (or consider correcting) personal information held about a person. The first is if the entity has occasion to consider, of its own volition, that the information is inaccurate, out of date, incomplete,

⁴⁷ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [101-103].

⁴⁸ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [104].

⁴⁹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [105].

⁵⁰ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [107-108].

⁵¹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [109].

irrelevant or misleading. The second is that the entity receives a request from an individual for the correction of their personal information.⁵²

The court was not satisfied that the 3 March Demand Email was in fact an APP 13 request from the Applicant. Specifically, the email did not request the correction of anything. Snaden J held that:

*‘[the email] was little (if anything) more than a demand that records be “destroyed”, couched in objectionable language that appears to have been calculated only to bully or belittle [the Respondent’s staff member]. The 3 March Demand Email does not employ the term “correction”, nor any analogue of it...’*⁵³

*‘... I am not satisfied that the [Respondent’s] failure to respond to the 3 March Demand Email amounts in any way to a contravention of APP 13 (nor to an interference with [the Applicant’s] privacy.’*⁵⁴

Declaratory relief

The Applicant sought declaratory relief from the court record that the Department contravened APP 12 by not providing him with access to his personal information within 30 days of his request, and that the Respondent acted in bad faith in attending to that request in the manner that it did.⁵⁵

The court’s power to grant declaratory relief in matters that it has jurisdiction to determine is not in question. That power exists by virtue of s 16(c) of the ADJR Act and s 21 of the *Federal Court of Australia Act 1976* (Cth), if not inherently by reason of this court’s status as a superior court of record: *Ainsworth v Criminal Justice Commission* (1992) 175 CLR 564 (“**Ainsworth**”), 581 (Mason CJ, Dawson, Toohey and Gaudron JJ).⁵⁶

Although the Applicant’s claims for declaratory relief lacked substance the court identified that he contended he had a right to have his 25 November APP 12 request dealt with within 30 days and in a manner unpolluted by bad faith. The Applicant claimed that those rights were infringed by the manner by which the Respondent handled the request.⁵⁷

Declaratory relief may assume one or both of two forms:

1. it could state that the Applicant possessed the rights he identified and/or
2. that the Respondent infringed those rights by dealing with his request as it did.⁵⁸

The court held that it would be an inappropriate exercise of the court’s discretionary power to grant the relief sought by the Applicant. In *Ainsworth* (at 582) the majority made the following observation about declaratory relief (references omitted in original):

[D]eclaratory relief must be directed to the determination of legal controversies and not to answering abstract or hypothetical questions. The person seeking relief must have “a real

⁵² *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [110].

⁵³ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [111].

⁵⁴ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [112].

⁵⁵ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [56].

⁵⁶ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [57].

⁵⁷ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [58].

⁵⁸ *Ibid.*

interest” and relief will not be granted if the question “is purely hypothetical I”, if relief is “claimed in relation to circumstances that [have] not occurred and might never happen” or it “the Court’s declaration will produce no foreseeable consequences for the parties”.⁵⁹

Snaden J was not persuaded that there was any utility in granting declaratory relief in respect of the Applicants APP 12 and APP 13 requests. The 25 November APP 12 Request was addressed, it was futile to grant relief in relation to the APP 13 request and the granting of relief would do little more than validate the Applicant’s opinion that the Respondent ought to have acted on the 3 March Demand Email in accordance with APP 13. The court was satisfied that the Applicant received what he was entitled to receive and he did not challenge his successful prosecution of the APP 12 request. The Applicant simply seeks to validate his view that it was not handled as it ought to have been. The court stated:

‘Even assuming that he is right about that, it is difficult to see how declaratory relief from this court might benefit him in any legal sense.’⁶⁰

The court commented further on the utility of granting declaratory relief in this case:

I am not satisfied that the circumstances that here present warrant an exercise of the court’s discretion to grant declaratory relief (under any of the various sources of the court’s power to grant it). However much it might vindicate [the Applicant’s] criticisms of the Department, declaratory relief would be legally pointless.⁶¹

...

I do not consider that the circumstances here warrant an exercise of the court’s discretion to grant declaratory relief. There is no utility in granting what is sought. Declaratory relief is granted to record the existence or otherwise of a particular state of affairs and, thereby, to resolve a justiciable controversy. Here, [the Applicant] seeks little (if anything) more than an advisory opinion from the court. That is not an appropriate exercise of the remedy.⁶²

...

The relief that is sought would achieve nothing more than to vindicate [the Applicant’s] opinion that the Department ought to have responded to or acted upon (or was required under APP 13 to respond to or act upon) his 3 March Demand Email, and/or to serve as advice to the Department that that view is correct. ... that view is not correct; but even if it were, declaratory relief is not a remedy that is appropriately deployed in the service of those ends. Although it would undoubtedly validate [the Applicant’s] criticisms of the Department’s failure to respond to his 3 March Demand Email, declaratory relief in the form sought would be legally pointless (in the sense that it would not serve to vindicate any presently-existing legal rights, nor otherwise resolve any presently-existing justiciable controversy).⁶³

⁵⁹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [59] citing *Ainsworth v Criminal Justice Commission* (1992) 175 CLR 564 [582].

⁶⁰ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [62].

⁶¹ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [64].

⁶² *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [82].

⁶³ *Knowles v Secretary, Department of Defence* [2020] FCA 1328, [115].

The court's decision

Application dismissed with costs.

Orders made by the court

THE COURT ORDERS THAT:

1. The applicant's further amended originating application dated 30 September 2019 be dismissed.
2. The applicant pay the respondent's costs in a sum to be assessed in default of agreement, in accordance with the court's Costs Practice Note (GPN-COSTS).

Court judgment⁶⁴

FEDERAL COURT OF AUSTRALIA

Knowles v Secretary, Department of Defence [2020] FCA 1328

File number:	VID 416 of 2017
Judgment of:	SNADEN J
Date of judgment:	17 September 2020
Catchwords:	ADMINISTRATIVE LAW – judicial review – decisions made by the respondent in relation to applications made under the <i>Privacy Act 1988</i> (Cth) (hereafter, the “ Privacy Act ”) for access to and correction of certain information – various species of relief sought – whether Privacy Act mandates provision of access to information within 30 days – appropriateness of declaratory relief – whether existence of other remedies for the review of administrative decisions should incline the court against granting prerogative or other relief – whether private information might be corrected by associating or attaching other documents to it – whether a demand that information be destroyed qualifies as a request for correction under the Privacy Act – further amended originating application dismissed with costs
Legislation:	<p><i>Administrative Decisions (Judicial Review) Act 1977</i> (Cth) – ss 3, 5, 6, 7, 10 and 16</p> <p><i>Federal Court of Australia Act 1976</i> (Cth) – s 21</p> <p><i>Freedom of Information Act 1982</i> (Cth)</p> <p><i>Judiciary Act 1903</i> (Cth) – s 39B</p> <p><i>Privacy Act 1988</i> (Cth) – Sch 1; Pt V; Pt VIB; ss 6, 6A, 13, 15, 36, 40, 41, 52, 55A, 80W, 96</p> <p><i>Regulatory Powers (Standard Provisions) Act 2014</i> – Pt 7; ss 118, 119, 120 and 121</p>
Cases cited:	<p><i>Ainsworth v Criminal Justice Commission</i> (1992) 175 CLR 564</p> <p><i>Australia Pty Ltd v Minister for Infrastructure and Transport</i> (2014) 221 FCR 165</p> <p><i>Australian Competition and Consumer Commission v MSY Technology Pty Ltd & Ors</i> (2012) 201 FCR 378</p>

⁶⁴ Errors and emphasis in original.

Construction, Forestry, Maritime, Mining and Energy Union v Milin Builders Pty Ltd [2019] FCA 1070

Cruse v Multiplex Ltd & Ors (2008) 172 FCR 279

Dranichnikov v Minister for Immigration and Multicultural Affairs (2003) 197 ALR 389

Knowles v Australian Information Commissioner [2018] FCA 1212

Saitta Pty Ltd v Commonwealth (2000) 106 FCR 554

SCAS v Minister for Immigration and Multicultural and Indigenous Affairs [2002] FCAFC 397

Tooth & Co Ltd v Council of the City of Parramatta (1955) 97 CLR 492

Warramunda Village v Pryde (2001) 105 FCR 437

Knowles v Australian Information Commissioner [2018] FCA 1212

Saitta Pty Ltd v Commonwealth (2000) 106 FCR 554

SCAS v Minister for Immigration and Multicultural and Indigenous Affairs [2002] FCAFC 397

Tooth & Co Ltd v Council of the City of Parramatta (1955) 97 CLR 492

Warramunda Village v Pryde (2001) 105 FCR 437

Division: General Division
Registry: Victoria
National Practice Area: Administrative and Constitutional Law and Human Rights
Number of paragraphs: 118
Date of hearing: 14 October 2019
Counsel for the Applicant: The applicant appeared in person
Counsel for the Respondent: Mr A D Pound
Solicitor for the Respondent: HWL Ebsworth Lawyers

ORDERS

VID 416 of 2017

BETWEEN: KIERAN JOHN MURRAY KNOWLES

Applicant

AND: SECRETARY, COMMONWEALTH DEPARTMENT OF DEFENCE

Respondent

ORDER MADE BY: SNADEN J

DATE OF ORDER: 17 SEPTEMBER 2020

THE COURT ORDERS THAT:

1. The applicant's further amended originating application dated 30 September 2019 be dismissed.
2. The applicant pay the respondent's costs in a sum to be assessed in default of agreement, in accordance with the court's Costs Practice Note (GPN-COSTS).

Note: Entry of orders is dealt with in Rule 39.32 of the *Federal Court Rules 2011*.

REASONS FOR JUDGMENT

SNADEN J:

1. For at least the last four years, the applicant, Mr Knowles, has been in dispute with the respondent—or, perhaps more broadly, with the commonwealth department that the respondent administers (hereafter, the “**Department**”)—concerning Departmental records that pertain to him. The background to that dispute is not material; but it has spawned a raft of applications and related litigation under various commonwealth statutes. The present matter is the latest front upon which that private war rages.
2. By a further amended originating application dated 30 September 2019, Mr Knowles prosecutes a number of challenges to various decisions made (and other conduct or omissions engaged in) by or on behalf of the Department in connection with applications that he has made or purported to make under what are known as the Australian Privacy Principles (hereafter the “**APPs**”), for which sch. 1 of the *Privacy Act 1988* (Cth) (hereafter, the “**Privacy Act**”) makes provision. Particulars of those applications, the relief that is sought in respect of them and the statutory sources of this court’s power that Mr Knowles seeks to invoke in order to obtain that relief are identified below.
3. For the reasons set out herein, I decline to grant the relief that Mr Knowles seeks. His further amended originating application of 30 September 2019 will be dismissed with the usual order as to costs.

1. EVIDENCE AND BACKGROUND FACTS

4. The material facts are substantially (if not wholly) uncontroversial. They emerge from the evidence that the parties led, all of which was received (in some cases, eventually) without successful objection. Mr Knowles read an affidavit that he affirmed on 24 September 2019. The respondent read an affidavit of Ms Catherine Nicole Hooper, affirmed on 18 January 2018. Additionally, the parties prepared a statement of agreed facts, which was filed on 6 February 2018 and received into evidence at the hearing. A bundle of documents—the content of which was the subject of discussion and, ultimately, agreement at the hearing—was also received into evidence.
5. The following facts emerge without significant controversy from that body of evidence.
6. In 2011, Mr Knowles was the subject of a communication (or possibly multiple communications) between the Department and another Commonwealth government department (hereafter, “the Other Department”), the identity of which it is prudent not to reveal (as these reasons will later explain). It is not necessary to recite the substance of those communications (although some insight as to them emerges below). It suffices to note that they recorded some information or opinions about Mr Knowles to which Mr Knowles took (and continues to take) exception.
7. In May 2016, Mr Knowles sought to ascertain what records the Department possessed that contained information personal to him (including about the communications referred to in the previous paragraph). To that end, he made an application under the Privacy Act and, later, under the Freedom of Information Act 1982. Those applications are not presently relevant, except insofar as they provide some context for the events that are.

8. On Friday, 25 November 2016, Mr Knowles sent an email to the Department headed “PI Access under App12”. That email (hereafter, the “25 November APP 12 Request”) was relevantly in the following terms (errors original):

Dear Defence Privacy Officer,

Since Defence seems intent to stymie access under FOI, I now request access under the Privacy Act - APP12, to PI of mine.

An APP entity that holds personal information about an individual must, on request, give that individual access to the information (APP 12.1).

APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be given access to information. This includes FOI, which is a separate process and does not impede on application via the Privacy Act.

An APP entity ‘holds’ personal information ‘if the entity has possession or control of a record that contains the personal information’ (s 6(1)), and extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with.

APP 12 requires an APP entity to provide access to ‘personal information’, as defined in s 6(1), being any information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

APP 12 requires an APP entity to provide access to all of an individual’s personal information it holds, even if that record may not exclusively deal with that individual's personal information.

APP 12 requires that personal information be given to an individual ‘on request’. APP 12 does not stipulate formal requirements for making a request, or require that a request be made under signature. An entity cannot require an individual to follow a particular procedure, use a designated form or explain the reason for making the request.

APP 12.4(a)(i) provides that an agency must ‘respond’ to a request for access within 30 calendar days. The 30 day time period commences on the day after the day the agency receives the request. The agency must respond by giving access to the personal information that is requested, or by notifying its refusal to give access.

An APP entity must give access to personal information in the manner requested by the individual, if it is reasonable and practicable to do so (APP 12.4(b)). **I request supply via electronic email**

An agency cannot impose upon an individual any charge for providing access to personal information under APP 12 (APP 12.7). This includes a charge for the making of the request to access personal information and/or a charge for giving access to requested personal information, such as charges for copying costs, postage costs and costs associated with using an intermediary.

I therefore request all records, held by Defence, that contain my PI. I expect record search will be conducted for the periods *Oct 2011 to March 2012 and May 2016 to Oct 2016 inclusive*.

To help narrow the search for Defence, these would be records in CAF, DCAF, JHC, HQAC, and RAAF Security Police repositories, and relate to issues contained in [a document that was identified but need not here be repeated], *and may mention the following personnel as author, receiver, or sender of said documents:*

...[there then followed a list of names that need not be recited]...

This is not to say these records will include the personal information of the aforementioned, as where public servants' names or positions or other material that only reveal only a public servant performing their public duties does not involve the disclosure of information concerning their personal affairs. Essentially what is disclosed is that the person took part in the passage of official information, and constitutes official information, not personal information.

While not limiting what is recognised as personal information of mine, search terms that could be used to identify records include:

...[there then followed a list of search terms that need not here be repeated]...

I hope this will help resolve Defence's bad faith unethical stonewalling on access noting that nothing prevents these processes running concurrently (and still Defence is not lifting a finger to search under FOI still, at least this way you'll can get started doing under the Privacy Act, as is required on application).

I note that I previously verified my identity via this email address with Defence Privacy.

Regards

Kieran Knowles

9. The following week, Mr Ian Heldon—the Department's Assistant Director Administrative Review, Complaints and Resolution—acknowledged receipt of Mr Knowles's 25 November APP 12 Request. Mr Knowles then enquired of Mr Heldon as to "...the due date for [a] decision (just so we lock this down)". Mr Heldon relevantly responded as follow:

Dear Kieran,

While we will endeavour to action your request for access to information as soon as possible I am unable to provide an expected date for a response. We will keep you updated. If you are dissatisfied with Defence's handling of your request you can complain to the Office of the Australian Information Commissioner.

...

10. Later that day (Thursday, 1 December 2016), Mr Knowles sent Mr Heldon another email, noting (relevantly, errors original):

I believe Ian that legislation wise, the required processing period is 30 calendar days for APP 12 decisions. Certainly I will activate my review rights should neither response nor reasonable excuse not be received by 27 December 2016 (30 calendar days falls on 26th, but it'd be unreasonable to have due date on Boxing Day, so have added an extra day for you) - unless you can provide evidence as to why it should be some other date.

...

11. On Thursday, 22 December 2016, Mr Heldon sent Mr Knowles another email, to which was attached some documentation provided in partial satisfaction of his 25 November APP 12 Request. In that email, Mr Heldon noted additionally as follows (relevantly, errors original):

...

I have asked the other areas in Defence which you nominated in your request to review their records and identify what relevant personal information they may hold. Further I have asked

them to advise their agreement to release, including reasons if they consider documents should be redacted or not released.

Unfortunately, I have not yet received responses to my requests. At this stage I am unable to provide an expected due date for a further response however I will keep you updated. Just to clarify, Defence is not refusing access.

If your dissatisfied with Defence's handling of your request you can complain to the Office of the Australian Information Commissioner....

12. Later that evening, Mr Knowles sent an email to Mr Heldon in the following terms:

Good Afternoon Ian,

I'm pleased you have taken the opportunity to inform yourself of the obligations imposed by the Privacy Act under Australian Privacy Principle 12. It's a welcome about face compared to previous responses In recognition of this, I am happy to provide Defence - in recognition of the impact of the Christmas/New Years stand-down - an extension of two weeks, making the new deadline Monday 9th January to provide the outstanding material and to complete this PI access request.

May you have a Merry Christmas and a Happy New Year, and I hope this more professional and ethical approach now taken, will continue.

I will also provide copy of this to the OAIC desk officer handling the related FOI IC review, as I believe this will assist in progressing that matter too.

Regards

Kieran Knowles

13. On Friday, 23 December 2016, Mr Heldon sent a series of emails to various colleagues throughout the Department, by which he sought assistance in responding to Mr Knowles's 25 November APP 12 Request. Those emails (hereafter, the "Assistance Request Emails ") assume some significance in this matter.

14. In the early morning of Monday, 30 January 2017, Mr Knowles sent another email to Mr Heldon. It is convenient to set out the terms of that email in full (errors original):

Ian,

It seems you deliberately wish to cause offence.

I gave you an extended deadline to complete this outstanding APP12 process, for your "outstanding enquiries", which was required to be completed by Monday 9th January.

That deadline passed without completion or update.

I allowed the end of the month to run, to see if you made any effort to update or complete, and you did not do so.

Defence has still deliberately failed to comply with its obligations under the APP12 provision of the Privacy Act - partial completion is still a breach of the Privacy Act, the obligation is that all relevant records must be provided.

Do you have any excuse you wish to make, before this matter is actioned on?

Disgusted by this unlawful behaviour by Defence.

Kieran Knowles

15. Approximately an hour later, Mr Knowles made a complaint to the Office of the Australian Information Commissioner concerning the Department's response—or partial-response—to his 25 November APP 12 Request. By that complaint (hereafter, the "**OAIC Complaint**"), Mr Knowles charged the Department with having contravened an APP (and, thereby, with having interfered with his privacy for the purposes of the Privacy Act) insofar as it did not answer his 25 November APP 12 Request within 30 days. The OAIC Complaint made reference to the Department having, in the past, "...repeatedly and deliberately interfered with [Mr Knowles's] privacy and [his] right to see how it has dealt with [his personal information]" and concluded as follows:

I request formal acknowledgement of this privacy complaint against Defence, and that it be dealt with promptly, noting the numerous refusals by Defence to adhere to privacy and FOI law.

Let me be crystal clear - I will use all legal means to ensure the legislation is complied with, and that further intentional delays are given the judicial scrutiny they deserve. I would think you would be aware that playing games with me, has a history of not working out so well for you (even when you stack the deck).

16. By a series of emails sent in early February, Mr Heldon provided to Mr Knowles the remaining information that he had sought by his 25 November APP 12 Request. In reply to one of those emails, Mr Knowles responded in the following terms (errors original):

Dear Ian,

It is rather appalling that Defence clearly hoped I would just forget and that you sat on this material - from the limited records provided (which do not contain any material between CAF Office and the other involved areas of Defence, despite repeated reference to said records, including a HIB which can not have "disappeared" given archive practices for such material), some redacted without specific explanation (contrary to Defence standard practice of specifying for each redaction the claimed grounds for doing so) this material has been in Defence's immediate possession following internal enquiries back mid-2016 - rather than release it as you were obligated to do within a reasonable time period (which as per the OAIC rules, was still 30 days within request made).

The missing records (not missing as in actually missing, but clearly being withheld unlawfully), which cannot be missing due to record keeping practices for correspondence between CAF Office and other areas of Defence (you forget I worked in the C Suite as SO to DCAF for a number of months - I am familiar with that office's practices and requirements here), in particular any records coming out of CAF's Office and any briefings or other related records back (which, by necessity, must contain my PI and therefore fall within scope) are required to be provided and there is no possibility they have simply "disappeared" from records (Archive Act requires such records are retained).

I specifically requested these records, yet none have been provided, nor has any explanation for their absence been given.

For just once, can you play this with a straight bat and provide the records required. I know you have them, you know you have them, and by sitting on them, you only give weight that wrongdoing was deliberately done at the time.

I should also advise you, given some of the factually untrue claims made in the some of these documents provided, I will seek correction under APP13 (or more accurately, annotation required to be placed on said records, based on evidence directly proving certain claims to be false, that those allegations were falsely made as part of a intentional harassment and defamatory campaign by [the Other Department] - that are repeated in the internal correspondence as facts when they are not – in breach of APP10) at a later date. Defence should, however, not wait given its obligations under the Privacy Act, and start to effect its own review as to the accuracy of said records, and make sure they are up to date (it's in your own interests given it's clear where this will end up, but this is just advice, and you can certainly ignore it if you want to dig your own hole further - frankly we could have had this done and dusted ages ago - but the irony of Defence trying to cover its backside is that it is actually leading you further towards scrutiny you clearly wish to avoid).

Now, are you going to provide the outstanding PI records, or do you want to spend yet more time and resources trying to hide them, when you would be well aware you' ll have to hand them over eventually - all this unethical and illegal behaviour is doing is kicking the can down the road to delay the inevitable (if I was going to just give up in the face of Defence's unlawful obstructions, it would have happened months ago - but I have the time, money and will to stick with it, as I would have thought was pretty obvious by now).

For as long as it takes, I will have Defence account for all the ways it used my PI in these disgraceful breaches of privacy (I think Defence needs a refresher in PI and Privacy law - any opinion or comment about an identifiable individual, whether true or not, is PI – this idea that Defence never disclosed or used PI to multiple individuals both within and without Defence is simply unsustainable - false claims were repeatedly distributed, to the detriment of my standing within the Defence community, pretty widely, and Defence failed to retract these when those false claims were shown without substantive evidence - Defence conducted a witch hunt on little better than rumour and I was subjected to harassment by senior ADF personnel because of it, partially because of personal relationships senior ADF individuals had with senior staff at [the Other Department], who wanted to knock me down a whole clothesline of pegs for exposing their corrupt practices). The list of individuals who were communicated false claims (as if they were factually correct), without any notification or right of reply being given (in breach of administrative law) to me, now runs multiple pages - absolutely there will be multiple individuals (who only dealing with their part) who were never advised those claims were false and will still believe those false allegations are true, when senior Defence personnel knew they were not (but never did correct the record), is a massive travesty.

I am just not going to give up. So why don't you exercise some common sense and just supply all the records required, prove there is nothing to cover up, and avoid future escalating embarrassment (it is not my objective to damage the ADF or the ADO, but by god, I am not going to protect you, and if you force things down that path of ever increasing scrutiny, you are going to have to cop the exposure and liability that comes with it).

Again Ian, Defence has nothing to lose by dealing with this ethically, but much risk in not doing so (ask [the Other Department] how their illegal behaviour is going for them - one officer even got her previous lying under oath uncovered, these things tend to kick up linked stuff people would rather wish hidden).

Regards

Kieran Knowles

17. In reply to another of Mr Heldon's early-February 2017 emails, Mr Knowles responded as follows (errors original):

Hi Ian,

Given you've breached the Act/PPs multiple times already, I'm sure you are aware I already have [lodged a complaint with the office of the Australian Information Commissioner].

There is a set period for providing the required records, Defence cannot ignore that. It's not a case of providing what you want, when you want, when you feel like it.

It might take years (maybe even a decade), but I will progress this matter through the OAIC, the AAT and the Federal Court if that's what it takes (and indeed there is some benefit of doing so, given that the only way such unlawful conduct will cease is if continuously reinforced that such conduct is unlawful).

You know the obligations here, I know the obligations here, and that any short term benefits you think you are deriving by acting unlawfully now, will be insignificant to the long term losses you are exposing Defence to.

I know I would quite appreciate the opportunity to force certain Defence personnel involved here to give evidence under oath - perjury is a risky business for individuals, especially those knowingly acting unlawfully.

Given you made no mention of waiting on other material, and passed off your earlier email today as closure of this matter, until this point was pressed, you'll be pressed to sell that con.

You should be aware that when a respondent acts in a high-handed, malicious, oppressive or insulting manner, especially when warned by the Applicant prior, it exposes further liabilities. Honestly, the incredible arrogance of Defence here will be costly for you.

Regards

Kieran Knowles

18. In the evening of Thursday, 2 March 2017, Mr Knowles wrote again to Mr Heldon. Again, it is prudent to set out the terms of that email (hereafter, the "2 March APP 13 Request") in full (errors original):

Dear Ian,

As you should be aware the Privacy Commissioner issued a Determination in my favour a few years back upholding a privacy complaint against [the Other Department] in relation to a number of false claims [the Other Department] made about me to Defence about me being a serious and imminent risk to self and others, and falsely alleging I was in a psychotic state.

As stated in that Determination:

* "The [Other Department] (the Department) interfered with the complainant's privacy by disclosing his personal information, in breach of Information Privacy Principle (IPP) 11.1 of the Privacy Act 1988 (Cth) (the Privacy Act)"

* " 'Personal information' is defined in s 6(1) of the Privacy Act as: information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." [these uncorrected opinions about me that Defence has recorded in multiple records, without qualification or annotation,

based on [the Other Department]'s fraudulent and malicious claims constitute personal information about me, held on record by Defence, and come within the scope of the Privacy Act]

* The Commissioner rejected that these false allegations/disclosures by [the Other Department] to Defence were covered by or justified by IPP 11.1(a), saying 'the Department has not provided any explanation or information demonstrating how the complainant was aware, or was reasonably likely to have been aware, that information of that kind was usually passed to the ADF or the Department of Defence.'

* The Commissioner rejected that these false allegations/disclosures by [the Other Department] to Defence were covered or justified by IPP 11.1(c) saying "If I were to accept that the complainant's communications could be characterised as a serious and imminent threat to either the life or health of himself or that of another person, I am nevertheless not satisfied that the disclosure of that conduct to the Department of Defence was necessary to protect him or any other person from that threat. It is particularly unclear how the Department could have considered it was necessary to disclose the complainant's personal information to his employer in order to prevent or lessen the serious and imminent threat to the life or health of a...staff member [of the Other Department], when the security assessment report recommended the Department consider mediation and/or the appointment of a specialised single point of contact as soon as practically possible. If the Department considered the threat to be serious and imminent, then disclosure to the police, in accordance with reported standard Departmental practice, would seem the appropriate course of action to address the situation. It is also unclear why when making such a disclosure it would be relevant to disclose details of the complainant's compensation claims. I am not persuaded on the information before me, that any threat that may have existed at that time mandated disclosure to ADF medical staff or Defence's Head of Joint Health Command in order to prevent or lessen it... I am satisfied that the complainant's conduct did not constitute a serious and imminent threat. In my view, on the totality of the information before me, any belief that the Department may have held that the complainant's conduct posed a serious and imminent threat was not reasonable. The circumstances presented here do not meet the threshold required for IPP 11.1(c) to be applicable and the Department was therefore not entitled to rely on it."

* The Commissioner rejected that these false allegations/disclosures by [the Other Department] to Defence were covered or justified by IPP 11.1(d) saying "The Department submitted that its disclosure of the complainant's personal information was at a minimum authorised, if not required, by the Work Health and Safety Act 2011 (WHS Act)... The WHS Act did not commence until 1 January 2012 and was therefore not in effect at the time of the Department's disclosure. As the WHS Act does not operate retrospectively, it cannot be relied on by the Department. The Occupational Health and Safety Act 1991 was in place at the time of the Department's disclosure. I am not satisfied that any obligations the Department may have under that legislation may be relied on to permit the disclosure under IPP 11.1(d). Even if a duty of care existed as asserted by the Department and that duty of care could have been categorised as a law for the purposes of IPP 11.1(d), it is not clear that authorisation to disclose would permit disclosure to the complainant's employer under the exception in IPP 11.1(d) of the Privacy Act. No specific legislative reference to the range of persons personal information may be disclosed to in the discharge of such a duty of care has been identified. Nor it seems was this disclosure in keeping with standard practice (the Department's standard practice would normally involve disclosure to the police). In my view, the Department's actions were not consistent with the notion that it was discharging a perceived duty of care. Accordingly, on the information available to me, I am satisfied that the Department cannot rely on the exemption contained in IPP 11.1(d)."

* The Commissioner rejected that these false allegations/disclosures by [the Other Department] to Defence were covered or justified by IPP 11.1(e) saying "The Department submitted on 28 March 2012 that the disclosures were reasonably necessary for the enforcement of the Defence Force Disciplinary Act 1982 (DFDA) and referred in particular to sections 33 and 60, which deal with 'assault, insulting or provocative words' and prejudicial conduct respectively. If I were to accept that the term 'enforcement of criminal law' or 'enforcement of a law involving pecuniary penalty' in IPP 11.1(e) includes disciplinary action taken by the Department of Defence under the Defence Force Discipline Act 1982 (DFDA), I am not aware of any type of arrangement between the Department and Defence, that existed at the time of the alleged improper disclosures, to the effect that these agencies shared information relevant to Defence's law enforcement functions under the DFDA. Nor has any information been presented to me to indicate that the complainant was the subject of an investigation of a service offence at the time of the disclosures. I am not satisfied that disclosure of the complainant's information to ADF medical officers could reasonably be expected to be necessary for the enforcement of any disciplinary action under the DFDA. The Head of Joint Health Command is, amongst other things, responsible for the provision of health care to members of the ADF. The ADF Senior Medical Officer also has a role in the provision of health care to ADF personnel. Even if there was an intention to disclose for the purpose of law enforcement, I am not satisfied that it was reasonably necessary to disclose that personal information to ADF and Department of Defence medical staff... Accordingly, I am satisfied that the exception contained in IPP 11.1(e) was not available to the Department in relation to its disclosures to an ADF Senior Medical Officer and the Head of Joint Health Command. "

* "The Department was not entitled to rely on the exceptions in IPP 11.1 (a), (c), (d) or (e) in disclosing the complainant's personal information to an ADF Senior Medical Officer on 20 October 2011... The Department was not entitled to rely on the exceptions in IPP 11.1 (a), (c), (d) or (e) in disclosing the complainant's personal information to the Department of Defence's Head of Joint Health Command on 20 October 2011"

* "I declare in accordance with s 52(1)(b)(i)(B) of the Privacy Act that the complainant's complaint is substantiated and that the Department breached IPP 11.1 by disclosing the personal information of the complainant."

As these false allegations by [the Other Department] were found without merit (Defence health personnel, after conducting intrusive review by multiple medical staff, found no substantiation of [the Other Department]'s false and malicious claims) and were held to be unlawful, these false claims recorded without qualification or annotation by Defence in multiple records held by them, across Security, Medical, Personnel and Executive records, are well overdue for correction. APP 13 requires an APP entity to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. Despite the defamatory nature of these allegations and that a kangaroo court QA was done in secret against me, which all fizzled out due to the fraudulent nature of these allegations and the utter lack of evidentiary weight to back these abuses of power, not correction of these fraudulent claims recorded as if they were true by Defence had occurred - even though many years have passed.

I therefore now formally require Defence to correct these records to specifically annotate every record held by Defence where these defamatory and false claims are recorded by Defence, to specifically advise that these defamatory and false claims by [the Other Department] were not only unlawful but also found to be unsubstantiated. It is a malicious slur on my record that they have been left uncorrected, to the extent that someone not completely across the whole history, may see one of those records in isolation and be misled as to thinking they actually

had some merit. An annotation on each individual piece of these records where these defamatory and false claims (that was held to be unlawful for [the Other Department] to make) to specify that this is not the case is the minimum ethical requirement for Defence to do.

Failure of Defence to do so will initiate legal action.

These annotations should also explicitly note that a Determination found these claims by [the Other Department] a breach of the Privacy Act and therefore unlawful. I will give you the reasonable period of 30 days to advise me of your decision, and 60 days to complete this task. Again, failure to do so will result in legal action. While my preference is destruction of these records that contain malicious and false claims by [the Other Department], that Defence not only made unlawful disclosures to [the Other Department] in return to but used to run an abuse of process because of personal relationships certain senior Defence staff had with certain senior...staff [of the Other Department] (bastardisation for a favour), I understand that such records will be the subject of ongoing legal action, so will accept comprehensive annotation (which is the absolute minimum required here).

I would advise you that playing games here just allows me to re-open the original breaches of the Privacy Act by Defence (despite claims by Defence, there was no legislative coverage for the disclosures by Defence to [the Other Department], of confidential medical information, as it was unrelated to any compensation claim and therefore outside any legal access arrangements and at that time not even a policy document covered the disclosures made by Defence), but since I receive a gain either way, feel free to be the unethical fuckhead you've been to date. I will take advantage of it.

Regards

Kieran Knowles

19. The following morning, Mr Heldon replied, requesting that Mr Knowles provide him with "...a copy of the determination which [was referred to in the 2 March APP 13 Request] or at least a reference which would allow [the Department] to make enquiries to obtain a copy."

20. Mr Knowles responded to that email that afternoon in the following terms:

Ian,

Determinations of the Privacy/Information Commission (OAIC) are all publicly available. The OAIC publishes them at <https://www.oaic.gov.au/privacylaw/determinations/#pagelist>

There has only been one Determination against [the Other Department] [there then followed a hyperlinked URL that needn't be republished here]

As a "Privacy Officer" it is inherent you must have a passing knowledge of the Privacy Act and the OAIC - both of which advise about the public publication of Determinations, and a quick Google search would have given you this information even if you were so ignorant of these facts. (although you appear to think your job is all about ignoring and subverting the Privacy Act and its obligations on Defence, not ensuring compliance).

Furthermore Determinations are published on Austlii and the LexisNexis legal database.

If you want me to be your administrative officer, because you are too lazy or ignorant to do your job, I suggest you start paying me.

Stop fucking around - unless you eventually want a subpoena to be cross-examined and your disgraceful behaviour to be on permanent court record (tends not to go down so well if you ever want to do anything else in your life).

Kieran Knowles

21. Mr Heldon responded later that evening in the following terms:

Dear Kieran,

Thank you for providing a link to the OAIC determination which I have now read.

I apologise if you believe that I am being lazy, ignorant or behaving disgracefully. I'm not as you suggest a 'privacy officer' nor legally trained in privacy although by default I have ended up managing the Defence privacy inbox in addition to my role managing APS employee grievances. The directorate where I work co-ordinates responses to requests received across several complaint related inboxes.

My previous interactions with you have been in this coordination role. In hindsight I should have been clear about this at the outset. I passed your complaints/requests to the relevant areas in Defence and then collected their responses and passed them to you. I have no decision making power in relation to Privacy or the ability to direct areas such as Air Force or Joint Health Command to take any particular action. I can't see what records they hold and I rely on the information I am provided by them.

I understand that I am currently the focal point of your frustrations with Defence and you hold me personally responsible for Defence's responses to date - I assume your expletives and threats are only a reflection of this frustration and do not imply a serious or imminent threat to my health or safety.

I believe that I have always responded to you in a cordial and respectful manner although I acknowledge not always in your expected timeframe or with the outcome you are seeking. I have strived to balance your requests along with my core responsibility managing a small internal complaint handling team whose workload often impacts on timeliness. If you would prefer not to interact with me then I can try to identify an alternate point of contact within Defence for you.

I provide the above as explanation of my role and the actions I have taken to date when corresponding with you. None of what I have said should be construed as a reflection on Defence's broader responsibilities and obligations under the Privacy Act and Australian Privacy Principles.

You may well respond with further expletives and threats about taking some action against me. I'll just continue to try to coordinate a response to your requests – unless you advise that you want an alternate point of contact.

In response to your current request I intend forwarding a copy of the OAIC determination to Air Force (Personnel and Executive records), Joint Health Command (Medical records), Australian Government Security Vetting Agency (Security records) and Service Police (Policing Records) and request they annotate their records as you have requested including attaching a copy of the OAIC determination

Regards,

Ian Heldon

Acting Director Complaints and Resolution
HR Services Branch
Defence People Group
Department of Defence

22. Half an hour later, Mr Knowles responded as follows (errors and emphasis original):

Stop being hysterical Ian - you'd be hard pressed to make out a criminal threat or threatening behaviour, and you are welcome to try arsehole.

You have continually taken the piss, been intentionally obstructionist, and deliberately dragged your heels and been unhelpful. Damn right I hold you accountable for that.

If you continue to make defamatory comments about me making threats or exhibiting anything other than frustration to be expected from your deliberately obstructionist behaviour, I warn you now that I will commence legal action against you personally for intentional defamation. You should be aware that as per the Legal Services Directive, the Commonwealth will not fund defamation action on your part, so it'll be you personally responsible for your disgusting unethical behaviour.

Anyone can be fake token forms of address while being deeply disrespectful and offensive in their conduct - you can fuck off with your claims you have treated me "respectfully", because the evidence proves otherwise. You have ignored your legal obligations on multiple occasions, on the few times you have given token lip service I have treated you with respect, in all other cases where you have acted fraudulently or with intentional disrespect by action, you have also been treated accordingly.

If you what to put it to the test, feel free to debate it in a court room, because you'll come out smarting.

So pull your head in dickhead - you want respect, you had to act with integrity and honesty. You are not entitled to any, if you do not give any - and you are well aware as I am you have been constantly playing games with intentional infliction of unethical behaviour below the standards required by the APS Code of Conduct.

As Dr Jeremy E Sherman said:

"You're being disrespectful!" is an arresting accusation made as though you should never be disrespectful, as though everyone always deserves total respect. Being respectful is treated as synonymous with being nice, disrespectful as with sinning.

And yet none of us can or should respect everything and everybody equally. To do so would be to surrender our powers of discernment, of evaluating the quality of one person's views and actions as cleaner or better than another's.

Some say the way out is to disrespect ideas and actions but not people, and yet, as you may have noticed, we can't draw a clean line between people and the ir behavior, at least not one they'll regard as clean. Snubbing my thoughts and actions could easily snub me. When the citizens of Syria voice their opposition to Bashar a-Assad, their president for using Scud missiles against them, he'll feel personally snubbed, disrespected as a person, and well he should. The extreme proves the problem. A pure ban on disrespect is unworkable. We need a different approach to disrespect. Disrespect is not the sin it's made out to be.

I reserve for me and everyone else our powers of discernment, the right to employ the full spectrum from the highest respect to the lowest, from honoring a person as inherently credible, to taking their word and actions with a grain of salt, to monitoring them skeptically, to doubting them outright, to ignoring them, to fighting them, to fighting them to the death as I think befits Assad, the ultimate show of disrespect.

It is more dishonest and unethical to be fake polite, while intentionally being immoral, unethical or disrespectful by action, than it is just to be plainly so. This is the act of the psychopath who games the system of social interaction, the "Mean Girl" who pretends butter doesn't melt in her mouth, while being the biggest bully in the school.

Actions speak louder than words, and those who hide their unethical behaviour behind tokenistic platitudes deserve all the scorn such immoral fakery deserves.

If you don't retract your defamatory statements, I will follow up on them.

Under APP13 I require you to destroy these defamatory claims from Defence records about threatening behaviour you just made (note [the Other Department] tried the same stunt and lost, so try your luck dickhead), such comments are opinions about me that constitute personal information about me, and therefore fall within the scope of the Privacy Act. Furthermore they are defamatory and any distribution or repetition make you personally liable.

You want to dance with me snake, you better make sure you are fully covered, and I am telling you you are not. But thanks for giving me the opportunity to open action against you personally if you fail to remedy.

Kieran Knowles

That email (hereafter, the “**3 March Demand Email**”) also assumes significance in the present matter.

23. I pause to note that there is nothing in the evidence to suggest that Mr Knowles and Mr Heldon had any particular history beyond the various requests or complaints that Mr Knowles had made concerning his access to Departmental records. Although Mr Knowles plainly appears to have felt a sense of frustration about the manner in which Mr Heldon (or the Department more generally) had managed his requests, there is nothing in the evidence that explains why Mr Knowles was driven to send Mr Heldon such obviously and wildly inappropriate communications. For present purposes, nothing turns upon the relationship between Mr Knowles and Mr Heldon, nor upon the regrettable—frankly, astonishing— language that Mr Knowles chose to employ in the prosecution of his grievances. Nonetheless, I offer those observations lest it be thought that there is some hitherto unexplored evidence about the relationship between Mr Knowles and Mr Heldon that might contextualise Mr Knowles’s gratuitous incivility. There is not.
24. Perhaps appropriately after the exchanges outlined above, Mr Heldon played no further role of significance—certainly none that the evidence discloses—in the Department’s responses to Mr Knowles’s 2 March APP 13 Request and 3 March Demand Email. Responsibility in that regard seems to have vested instead in Mr Peter Bavington, the Department’s Director of Complaints and Resolution.

25. By email dated 6 March 2017, Mr Bavington distributed throughout various areas within the Department a copy of Mr Knowles's 2 March APP 13 Request and requested that steps be taken to address it. Relevantly, Mr Bavington's email was in the following terms (errors original):

Mr Knowles request is below (the determination he refers to is attached).

I request you review records you hold concerning ex-FLTLT Knowles and make any necessary corrections or annotations. If you do not consider that the records held are inaccurate, out-of-date, incomplete, irrelevant or misleading you may consider it appropriate to add a copy of the attached determination and a note (or a copy of this email) containing Mr Knowles APP13 request. Alternatively you may decide that no action is required in which case I request you provide reasons for that decision.

Your response is requested by Mon 28 March 2017 to enable a consolidated response to be provide within the 30 day timeframe.

26. That request was the subject of various responses over subsequent weeks, to the substance of which I shall shortly return.
27. On Sunday, 9 April 2017, Mr Knowles sent a follow up email to Messrs Bavington and Heldon. Again, it is convenient to set out the content of that email in full (errors original):

Attn Defence Privacy/Ian Heldon,

On the 2nd March 2017 and, subsequently on the 3rd March 2017 (following the highhanded, malicious, insulting & oppressive conduct of Defence EL2 employee Ian Heldon, who made the same fraudulent defamation that [the Other Department] was criticised by the Information Commissioner for, which he was aware of at the time of making said comments), two seperate but related APP13 Correction applications were made to Defence.

Defence was required to deal with both these APP13 Correction applications within 30 calendar days (so Monday 3 April 2027, given the weekend, for both application), under the Privacy Act and related Guideline requirements.

To date, no formal decision and correction has been made/notified by Defence (it is not acceptable to simply forward the matter to another area of Defence, to be left up to them, without any further confirmation that this has actually been carried out – just as an FOI decision requires a formal response/confirmation, so too does these actions under the Privacy Act).

Given Defence has not formally responded to either APP13 correction application, and this matter is now overdue a number of days, this is legally a deemed refusal by Defence to deal with these applications as required by the legislation and related guidelines.

I now have 30 days in which to seek review of this breach of the Privacy Act by Defence, which I advise you of my intent to do so. It is certainly apparent from the ongoing highhanded, malicious, insulting & oppressive conduct by Defence, who have gone to great lengths to frustrate and prevent lawful access to, and correction of, Defence records relating to my PI, that this will be the only mechanism to force Defence to comply with its legal obligations.

Suffice to say, it is disgusting behaviour by Defence, and the irony of a powerful and deeply unethical cohort in Defence, who act unlawfully in extreme prejudice to the legal rights of others, demanding they be treated with obsequious forelock tugging, when their actions have been anything but respectful (and indeed are breaches of the APS Code of Conduct) is noted (it

is nothing more than a fraudulent manipulation, a poisoning of the well, a shield to the powerful - much like Assad or Putin criticise the West for its hostility to its repeated breaches of international law, respect is not a right, and it is hypocritical to demand respect when you act in such a unethical and unlawful way).

28. Mr Bavington replied the following day, summarising the responses that he had collated from the various areas within the Department whose assistance he had enlisted for the purposes of addressing the 2 March APP 13 Request. Again, it is convenient to set out the text of Mr Bavington's email in full (errors original):

Dear Mr Knowles

I apologise for the delay in resolving your concerns. I asked four areas of Defence to annotate your records by including a copy of the OAIC determination. Those four areas are Air Force (Personnel and Executive records), Joint Health Command (Medical records), the Australian Government Security Vetting Agency (Security records) and Service Police (Policing Records). I have received confirmation that Joint Health Command and the Service Police have annotated your records. The Australian Government Security Vetting Agency has advised me that they have no records relating incident that resulted in the OAIC determination and therefore they have not annotated their records. Air Force is still working through some issues. I am following that up and I will get back to you when that matter is finalised.

Please note I will be the point of contact for any future privacy matters you may wish to raise with Defence.

Your sincerely

Peter

29. Twenty minutes later, Mr Knowles responded in the following terms (errors original):

Peter,

Again, an APP13 decision, required under the legislation, is not some soft serve "we will ask other internal areas of the Department to see if they wish to update" type of response as if this was an optional activity/mere suggestion, as given here, but a requirement to give an actual decision and amend records accordingly.

I also note you did not address at all the second APP13 submission, also overdue, requiring the removal of the defamatory claims of Ian Heldon from the records.

The outcomes requires are no different from that for an FOI decision, a formal letter from an authorised decision maker, granting the APP13 correction sought, or denying it, and giving a statement of reasons.

No such activity has taken place, despite the statutory deadline having passed and this constitute a deemed refusal to deal with the matter and a breach of the Act.

No apology for Ian Heldon's disgraceful behaviour (which insultingly was lifted from the Determination cited, that being making knowingly fraudulent inferences/claims of serious risk to self or others) has been provided either.

It seems rather clear that Defence do not intend to deal ethically with these matters, and won't do so short of being reminded of the law, in a courtroom.

30. Later in 2017, Mr Knowles commenced a proceeding in this court against the Australian Information Commissioner. That proceeding appears to have concerned, amongst other things, the OAIC Complaint. It was ultimately the subject of a successful application for summary dismissal: *Knowles v Australian Information Commissioner* [2018] FCA 1212 (Tracey J). The court’s reasons in support of that outcome contain the following factual summary:
- 19 On 27 June 2017 the Assistant Commissioner gave Mr Knowles a notice stating that he intended to dismiss his APP 12 complaint under s 41(1)(e) and s 41(2)(a) of the Privacy Act (“the proposed s 41 decision”). Mr Knowles was invited to comment by 11 July 2017.
 - 20 Although Mr Knowles indicated that he would comment on the notice he did not, ultimately, do so. Instead, on 30 June 2017, he varied his application to the Court to seek relief in relation to the proposed s 41 decision.
 - 21 The proposed s 41 decision has been put on hold pending the outcome of this proceeding.
31. The reference to the “APP 12 complaint” is a reference to a complaint that Mr Knowles directed to the Office of the Australian Information Commissioner on 30 January 2017 concerning a request that he made of the Department on 25 November 2016 for access to information under APP 12: *Knowles v Australian Information Commissioner* [2018] FCA 1212, [12]-[16] (Tracey J). I infer—and it is plainly the case—that that request was the 25 November APP 12 Request (above, [8]); and that that complaint was the OAIC Complaint (above, [15]).
32. By correspondence sent to Mr Bavington and dated 23 May 2019—after the summary dismissal of Mr Knowles’s earlier proceeding in this court and after the commencement of the present proceeding—the Office of the Australian Information Commissioner gave notice that it had decided to exercise its discretion under s 41(2)(a) of the Privacy Act to not investigate Mr Knowles’s OAIC Complaint.
33. There is no evidence that Mr Knowles has sought to challenge that determination, nor that he has complained to the Australian Information Commissioner in respect of the Department’s response (or failure to respond) to his 2 March APP 13 Request or his 3 March Demand Email.

2. LEGISLATIVE FRAMEWORK

34. The relief that Mr Knowles presently seeks is said to be authorised under various commonwealth enactments. It is prudent to map out in some detail the legislative bases upon which his application rests.

2.1. The Privacy Act

35. The Privacy Act regulates, amongst other things, certain ways in which Commonwealth agencies must handle particular types of information. Sch 1 to that act contains the APPs. By s 15 of the Privacy Act, “APP Entities” are prohibited from conducting themselves in ways that amount to breaches of an APP. Such conduct is the subject of further definition, into which it is not presently necessary to delve: Privacy Act, s 6A. It is not disputed that the respondent qualifies as an “APP Entity” and, more specifically, as an “agency”: Privacy Act, s 6.

36. By s 13 of the Privacy Act, an APP Entity is deemed to have “interfered with the privacy of an individual” if it engages in an act or adopts a practice that, in either case, breaches an APP in relation to personal information about that individual. “Personal information” is defined to mean “...information or an opinion about an identified individual, or an individual who is reasonably identifiable...whether the information or opinion is true or not [and] whether the information or opinion is recorded in material form or not”: Privacy Act, s 6.
37. There are two APPs that are relevant to this proceeding: APP 12 and APP 13. APP 12 is relevantly in the following terms:

12 Australian Privacy Principle 12—access to personal information

Access

- 12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

...

Dealing with requests for access

- 12.4 The APP entity must:
- (a) respond to the request for access to the personal information:
 - (i) if the entity is an agency—within 30 days after the request is made; or
 - (ii) if the entity is an organisation—within a reasonable period after the request is made; and
 - (b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

...

38. APP 13 is relevantly in the following terms:

13 Australian Privacy Principle 13—correction of personal information

Correction

- 13.1 If:
- (a) an APP entity holds personal information about an individual; and
 - (b) either:
 - (i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or
 - (ii) the individual requests the entity to correct the information;
- the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

...

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

- (a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and
- (b) the mechanisms available to complain about the refusal; and
- (c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

- (i) if the entity is an agency—within 30 days after the request is made...

39. Part V of the Privacy Act is headed “Investigations”. Section 36 provides that an individual may complain to the Australian Information Commissioner about an act or practice that he or she feels has resulted in an interference with his or her privacy. By s 40 (and subject to exceptions not presently relevant), the Australian Information Commissioner is required to investigate such complaints. That requirement is subject to the discretions conferred upon the Australian Information Commissioner by s 41 of the Privacy Act, which include a discretion not to investigate a complaint made against an APP entity if satisfied that the entity has adequately dealt with it.

40. Section 52 of the Privacy Act deals with the determination of complaints. Relevantly, it provides as follows:

52 Determination of the Commissioner

(1) After investigating a complaint, the Commissioner may:

(a) make a determination dismissing the complaint; or

(b) find the complaint substantiated and make a determination that includes one or more of the following:

- (i) a declaration:

(A) where the principal executive of an agency is the respondent—that the agency has engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct; or

(B) in any other case—that the respondent has engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct;

(ia) a declaration that the respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued;

(ii) a declaration that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;

(iii) a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint;

(iv) a declaration that it would be inappropriate for any further action to be taken in the matter.

41. Division 3 of Part V of the Privacy Act concerns (amongst other things) the enforcement of determinations made under s 52. A complainant may apply for orders in this court or the Federal Circuit Court to enforce such a determination: Privacy Act, s 55A. A complainant who is unhappy about a determination made under s 52 of the Privacy Act may apply to the Administrative Appeals Tribunal to have it reviewed: Privacy Act, s 96(1)(c).

42. Part VIB of the Privacy Act deals with enforcement of the obligations that the act otherwise imposes. Section 80W concerns enforcement by means of injunctions. It relevantly provides as follows:

80W Injunctions

Enforceable provisions

(1) The provisions of this Act are enforceable under Part 7 of the Regulatory Powers Act.

...

Authorised person

(2) For the purposes of Part 7 of the Regulatory Powers Act, each of the following persons is an authorised person in relation to the provisions mentioned in subsection

(a) the Commissioner;

(b) any other person.

Relevant court

(3) For the purposes of Part 7 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the provisions mentioned in subsection

- (a) the Federal Court;
- (b) the Federal Circuit Court.

2.2. The ADJR Act

43. The *Administrative Decisions (Judicial Review) Act 1977* (hereafter, the “**ADJR Act**”) confers upon this court jurisdiction to review certain administrative decisions.

44. Section 5 of the ADJR Act relevantly provides as follows:

5 Applications for review of decisions

(1) A person who is aggrieved by a decision to which this Act applies that is made after the commencement of this Act may apply to the Federal Court or the Federal Circuit Court for an order of review in respect of the decision on any one or more of the following grounds:

- (a) that a breach of the rules of natural justice occurred in connection with the making of the decision;
- (b) that procedures that were required by law to be observed in connection with the making of the decision were not observed;
- (c) that the person who purported to make the decision did not have jurisdiction to make the decision;
- (d) that the decision was not authorized by the enactment in pursuance of which it was purported to be made;
- (e) that the making of the decision was an improper exercise of the power conferred by the enactment in pursuance of which it was purported to be made;
- (f) that the decision involved an error of law, whether or not the error appears on the record of the decision;
- (g) that the decision was induced or affected by fraud;
- (h) that there was no evidence or other material to justify the making of the decision;
- (j) that the decision was otherwise contrary to law.

(2) The reference in paragraph (1)(e) to an improper exercise of a power shall be construed as including a reference to:

- (a) taking an irrelevant consideration into account in the exercise of a power;
- (b) failing to take a relevant consideration into account in the exercise of a power;
- (c) an exercise of a power for a purpose other than a purpose for which the power is conferred;
- (d) an exercise of a discretionary power in bad faith;
- (e) an exercise of a personal discretionary power at the direction or behest of another person;
- (f) an exercise of a discretionary power in accordance with a rule or

policy without regard to the merits of the particular case;

(g) an exercise of a power that is so unreasonable that no reasonable

person could have so exercised the power;

(h) an exercise of a power in such a way that the result of the exercise of the power is uncertain; and

(j) any other exercise of a power in a way that constitutes abuse of the power.

45. Section 6 is in similar terms, save that it relates to (amongst other things) conduct in which a person has engaged for the purposes of making a decision to which the ADJR Act applies.

46. Section 7 of the ADJR Act relates to failures to make decisions to which the ADJR Act applies. It provides as follows:

7 Applications in respect of failures to make decisions

(1) Where:

(a) a person has a duty to make a decision to which this Act applies;

(b) there is no law that prescribes a period within which the person is required to make that decision; and

(c) the person has failed to make that decision;

a person who is aggrieved by the failure of the first mentioned person to make the decision may apply to the Federal Court or the Federal Circuit Court for an order of review in respect of the failure to make the decision on the ground that there has been unreasonable delay in making the decision.

(2) Where:

(a) a person has a duty to make a decision to which this Act applies;

(b) a law prescribes a period within which the person is required to make that decision; and

(c) the person failed to make that decision before the expiration of that period;

a person who is aggrieved by the failure of the first mentioned person to make the decision within that period may apply to the Federal Court or the Federal Circuit Court for an order of review in respect of the failure to make the decision within that period on the ground that the first mentioned person has a duty to make the decision notwithstanding the expiration of that period.

47. Section 3 of the ADJR Act defines what qualifies as a “decision to which this Act applies”. It is not in dispute that the decisions made (or not made) by or on behalf of the Department in connection with each of the 25 November APP 12 Request and the 2 March APP 13 Request were decisions to which the ADJR Act applied. For reasons that will become apparent, I do not consider that the Department’s response (or failure to respond) to the 3 March Demand Email was conduct that related to, or was otherwise a failure to make, a decision to which the ADJR Act applied.

48. The rights of review conferred by ss 5, 6 and 7 of the ADJR Act are in addition to any other rights that a person has to seek review of a relevant decision, relevant conduct engaged in for the purposes of making a decision, or a relevant failure to make a decision: ADJR Act, s 10(1). This court may, in its discretion, refuse to grant an application under any of those sections in circumstances where another law makes adequate provision for a process or processes by which a person may apply to a tribunal to have the decision, conduct or failure in question reviewed: ADJR Act, s 10(2).

49. Section 16 of the ADJR Act confers upon this court various powers that, in its discretion, it may exercise by way of review of an impugned decision, impugned conduct or an impugned failure to make a decision. It provides as follows:

16 Powers of the Federal Court and the Federal Circuit Court in respect of applications for order of review

(1) On an application for an order of review in respect of a decision, the Federal Court or the Federal Circuit Court may, in its discretion, make all or any of the following orders:

- (a) an order quashing or setting aside the decision, or a part of the decision, with effect from the date of the order or from such earlier or later date as the court specifies;
- (b) an order referring the matter to which the decision relates to the person who made the decision for further consideration, subject to such directions as the court thinks fit;
- (c) an order declaring the rights of the parties in respect of any matter to which the decision relates;
- (d) an order directing any of the parties to do, or to refrain from doing, any act or thing the doing, or the refraining from the doing, of which the court considers necessary to do justice between the parties.

(2) On an application for an order of review in respect of conduct that has been, is being, or is proposed to be, engaged in for the purpose of the making of a decision, the Federal Court or the Federal Circuit Court may, in its discretion, make either or both of the following orders:

- (a) an order declaring the rights of the parties in respect of any matter to which the conduct relates;
- (b) an order directing any of the parties to do, or to refrain from doing, any act or thing the doing, or the refraining from the doing, of which the court considers necessary to do justice between the parties.

(3) On an application for an order of review in respect of a failure to make a decision, or in respect of a failure to make a decision within the period within which the decision was required to be made, the Federal Court or the Federal Circuit Court may, in its discretion, make all or any of the following orders:

- (a) an order directing the making of the decision;
- (b) an order declaring the rights of the parties in relation to the making of the decision;

(c) an order directing any of the parties to do, or to refrain from doing, any act or thing the doing, or the refraining from the doing, of which the court considers necessary to do justice between the parties.

(4) The Federal Court or the Federal Circuit Court may at any time, of its own motion or on the application of any party, revoke, vary, or suspend the operation of, any order made by it under this section.

2.3. The Regulatory Powers Act

50. The *Regulatory Powers (Standard Provisions) Act 2014* (Cth) establishes (amongst other things) a framework for the enforcement of certain legislative provisions by means of injunctive relief. Part 7 of that act (hereafter, the “**RP Act**”) is headed “Injunctions”. Section 121 of the RP Act provides as follows:

121 Grant of injunctions

Restraining injunctions

(1) If a person has engaged, is engaging or is proposing to engage, in conduct in contravention of a provision enforceable under this Part, a relevant court may, on application by an authorised person, grant an injunction:

- (a) restraining the person from engaging in the conduct; and
- (b) if, in the court’s opinion, it is desirable to do so—requiring the person to do a thing.

Performance injunctions

(2) If:

- (a) a person has refused or failed, or is refusing or failing, or is proposing to refuse or fail, to do a thing; and
- (b) the refusal or failure was, is or would be a contravention of a provision enforceable under this Part;

the court may, on application by an authorised person, grant an injunction requiring the person to do that thing.

51. Other provisions of the RP Act define what is contemplated by provisions that are “enforceable” under Part 7 (RP Act, s 118), who qualifies as an “authorised person” (RP Act, s 119) and what is an “authorised court” (RP Act, s 120). It suffices presently to note that the provisions of the Privacy Act are provisions that are enforceable under Part 7 of the RP Act, and that, for that purpose, Mr Knowles is an “authorised person” and this court is an “authorised court”: Privacy Act, s 80W (above, [42]).

2.4. The Judiciary Act 1903

52. The *Judiciary Act 1903* (Cth) (hereafter, the “**Judiciary Act**”) confers upon this court jurisdiction to determine matters in which injunctive relief, or writs of mandamus or prohibition are sought against an officer or officers of the commonwealth, or which otherwise arise under commonwealth laws: *Judiciary Act 1903* (Cth), s 39B(1) and (1A)(c).

3. MR KNOWLES'S CASE

53. There are three distinct aspects to the case that Mr Knowles prosecutes. They align with the three requests that he made (or purported to make) under the Privacy Act, namely: the 25 November APP 12 Request, the 2 March APP 13 Request and the 3 March Demand Email. It is convenient to deal separately with each of those three aspects of Mr Knowles's case.

3.1. The 25 November APP 12 Request

3.1.1. Summary of the contentions advanced

54. As the factual summary above sets out, the 25 November APP 12 Request concerned an attempt by Mr Knowles to access certain personal information that the Department held about him. Although the information that he sought was provided to him, Mr Knowles was and remains unhappy about the manner in which the Department handled that request.
55. There are two dimensions to his discontent. First, he says that the Department failed to afford him access to the information that he sought within 30 days of his request, which, he says, was required under APP 12. Second, he maintains that the Department's conduct in handling his request was attended by bad faith on the part of Mr Heldon. That alleged bad faith is itself comprised of multiple parts, in that it is said that Mr Heldon:

(1) did not take steps to address the 25 November APP 12 Request until nearly 30 days from the time that he received it;

(2) indicated to Mr Knowles that he (Mr Heldon) was awaiting responses from within the Department when, in truth, he had not initiated any process to elicit the information that Mr Knowles had sought; and

(3) provided to Mr Knowles, in partial satisfaction of the request, documents that he (Mr Heldon) knew had already been provided pursuant to another request that Mr Knowles had earlier made.

56. Mr Knowles seeks declaratory relief to record that the Department contravened APP 12 by not providing him with access to his personal information within 30 days of his request, and that Mr Heldon acted in bad faith in attending to that request in the manner that he did.

3.1.2. Appropriateness of declaratory relief

57. The court's power to grant declaratory relief in matters that it has jurisdiction to determine is not in question. For present purposes, it exists at least by dint of s 16(c) of the ADJR Act and s 21 of the *Federal Court of Australia Act 1976* (Cth), if not inherently by reason of this court's status as a superior court of record: *Ainsworth v Criminal Justice Commission* (1992) 175 CLR 564 ("*Ainsworth*"), 581 (Mason CJ, Dawson, Toohey and Gaudron JJ).
58. Mr Knowles did not identify the terms in which he hoped that the court might grant declaratory relief. Respectfully, the submissions that he advanced—which I pause to note were otherwise cogent and well-structured—did not clearly articulate the right or rights whose existence he sought to make the subject of declarations. He contended that he had a right to have his 25

November APP 12 Request addressed within 30 days and in a manner unpolluted by bad faith. Those rights were, he says, infringed by the manner in which the Department addressed his request. Logically, declaratory relief could assume one or both of two forms: it could state that Mr Knowles possessed the rights that he has identified and/or that the Department infringed them by addressing his request in the manner that it did.

59. Either way, what Mr Knowles seeks in respect of his 25 November APP 12 Request is not an appropriate exercise of the court's power to grant declaratory relief. In *Ainsworth* (at 582), the majority made the following observations about declaratory relief (references omitted):

“[D]eclaratory relief must be directed to the determination of legal controversies and not to answering abstract or hypothetical questions. The person seeking relief must have “a real interest” and relief will not be granted if the question “is purely hypothetical”, if relief is “claimed in relation to circumstances that [have] not occurred and might never happen” or it “the Court’s declaration will produce no foreseeable consequences for the parties”.

60. Although I have had occasion to express some doubt about the point (see, for example, *Construction, Forestry, Maritime, Mining and Energy Union v Milin Builders Pty Ltd* [2019] FCA 1070, [80]-[85] (Snaden JJ)), it seems to be accepted in this court that declaratory relief *may* be granted simply to record the basis upon which a proceeding resolves: *Cruse v Multiplex Ltd & Ors* (2008) 172 FCR 279, 298 [53] (Goldberg and Jessup JJ, Gray J dissenting). Unhelpfully, there is other full court authority to the contrary effect: *Warramunda Village v Pryde* (2001) 105 FCR 437, 440 [8] (Gray, Branson and North JJ); *Australian Competition and Consumer Commission v MSY Technology Pty Ltd & Ors* (2012) 201 FCR 378, 388 [35] (Greenwood, Logan and Yates JJ).
61. Assuming, momentarily, that the Department's conduct in respect of the 25 November APP 12 Request was engaged in in contravention of the law (in that the request was not addressed within 30 days and/or that the manner in which it *was* addressed was tainted by bad faith), and that the court might properly “record” as much by making a declaration or declarations to that effect (or otherwise so as to record what Mr Knowles's rights are or were), the court's attention naturally turns to whether there is any utility in doing so.
62. I am not persuaded that there is any utility in granting declaratory relief in respect of the 25 November APP 12 Request (supposing, as I do for the sake of argument, that the Department's relevant conduct was unlawful in either or both of the ways that Mr Knowles alleged). The 25 November APP 12 Request was addressed. Mr Knowles received what he was entitled to receive and, for obvious reasons, he does not challenge his successful prosecution of the request. He simply seeks to validate his view that it was not handled as it ought to have been. Even assuming that he is right about that, it is difficult to see how declaratory relief from this court might benefit him in any legal sense.
63. It is unfair to describe Mr Knowles's prosecution of this aspect of his present claim as a personal vanity project; but, equally, it is difficult to see how declaratory relief might vindicate any presently existing legal right to which he lays claim. On that front, Mr Knowles noted that he intends to lodge further requests for information under APP 12 and that the relief sought presently would (or might) serve to inform the manner in which the Department responds to them. Respectfully, those are hypothetical propositions into which this court cannot properly be drawn. Declaratory relief is granted to resolve justiciable controversies; not as a means of

providing advice to future or potential litigants : *Porter v OAMPS Ltd* (2005) 215 ALR 327, 337 [34] (Goldberg J).

64. Even assuming that Mr Knowles is right to draw the criticisms that he draws about the Department's responses to his 25 November APP 12 Request, I am not satisfied that the circumstances that here present warrant an exercise of the court's discretion to grant declaratory relief (under any of the various sources of the court's power to grant it). However much it might vindicate Mr Knowles's criticisms of the Department, declaratory relief would be legally pointless.

3.1.3. Validity of Mr Knowles's complaints

65. In any event, I am not persuaded that Mr Knowles's criticisms of the Department's conduct—namely that it contravened the Privacy Act by failing to address his 25 November APP 12 Request within 30 days and that its handling of the request was tainted by bad faith—are well-founded. I address each contention in turn.

The 30-day timeframe

66. The requirement in APP 12 is not that access to requested personal information must be granted within 30 days; it is that the request must be responded to within that timeframe. It is not in dispute that the Department did that. Mr Heldon acknowledged the request not long after Mr Knowles made it; and provided documents in partial satisfaction of it within 30 days (above, [9], [11]).
67. The terms of APP 12 reinforce that bifurcation. Paragraph 12.4 (above, [37]) is headed "Dealing with requests for access". It mandates two measures by which an APP Entity must *deal with* requests for access to information under APP 12: first, by the provision of a response to the request; and, second, by the provision of access to the information as requested (subject to notions of reasonableness and practicality that are not presently relevant). The instrument draws a distinction between "dealing with" a request by responding to it and "dealing with" a request by granting access to what is requested. The 30-day deadline applies only in respect of the former.
68. Even had I taken a different view about the appropriateness of declaratory relief to address this aspect of Mr Knowles's complaint, I would not have been persuaded that the Department (or the respondent on its behalf) contravened APP 12 (or any other part of the Privacy Act) by failing to provide to Mr Knowles access within 30 days to the information that was the subject of his 25 November APP 12 Request.

Bad faith

69. Similarly, I would not have been persuaded that the Department's response to the 25 November APP 12 Request was attended by bad faith. To stigmatise its conduct in that way, Mr Knowles would need to show that Mr Heldon (through whom the Department's—and the respondent's—response was actioned) did not honestly or genuinely set out to discharge the obligations that the Privacy Act imposed: *SCAS v Minister for Immigration and Multicultural and Indigenous Affairs* [2002] FCAFC 397, [19] (Heerey, Moore and Kiefel JJ).

70. I do not accept that Mr Heldon’s failure prior to 23 December 2016 to make the internal inquiries necessary to address the 25 November APP 12 Request sinks to the depths of bad faith. There may be any number of innocent explanations for such a failure (for example, the need to attend to other matters). Indeed, the evidence does not safely permit the court to infer that such a failure even occurred: the fact that Mr Heldon sent the Assistance Request Emails on 23 December (above, [13]) is not proof that no other steps had been taken prior to that point to compile the information that Mr Knowles had requested. The evidence simply does not disclose what, if anything, Mr Heldon did between 25 November 2016 and 23 December 2016. It is possible that he didn’t do anything, which would be consistent with the tone of the Assistance Request Emails. But that consistency alone is not a sufficient basis upon which to infer that that, in fact, was what occurred.
71. Mr Heldon’s knowing provision of documents of which Mr Knowles was already in possession (above, [11] and [55]) is not sufficient to constitute bad faith either. It is difficult to see what else Mr Heldon was meant to do with those documents. There is no suggestion that they were outside the scope of the 25 November APP 12 Request. Had he not provided them, he would have contravened the Department’s obligation to do so. That he provided them already knowing that Mr Knowles possessed them (if, indeed, he had such knowledge) is neither here nor there. The suggestion (if it was made) that he did so as some kind of ruse to disguise a degree of inactivity to that point in time (assuming that there *was* some degree of inactivity) is also insufficient to ground a finding of bad faith. It is not disputed that the documents answered the description of what Mr Knowles had requested. Mr Heldon was right to provide them.
72. In any event, this aspect of Mr Knowles’s bad faith allegation does not find clear expression within his further amended originating application of 30 September 2019 (nor any prior variant of that document). It was raised for the first time at the hearing. Although I would have dismissed it on its merits, it would have been dismissed in any event on the basis that it was not part of the case of which Mr Knowles gave prior notice.
73. Mr Knowles also attributes to Mr Heldon bad faith manifest in his indication of 22 December 2016 that he had “...asked other areas in Defence...to review their records [etc but had] not yet received responses” (above, [11]). Mr Knowles contends that that representation was untrue: that, in reality, Mr Heldon had not made any internal inquiries to that point in time and that he lied about having done so. I reject that contention. As has already been explored, there is simply insufficient evidence to conclude that Mr Heldon had not made any internal inquiries prior to 23 December 2016.
74. Again, even had I taken a different view about the appropriateness of declaratory relief to address this aspect of Mr Knowles’s complaint, I would not have been persuaded that the Department (or the respondent on its behalf) had acted unlawfully (or had otherwise done something that engaged either of ss 5(1)(e) or 6(1)(e) of the ADJR Act) by responding to the 25 November APP 12 Request in a manner that bespoke bad faith.

3.1.4. Conclusion in respect of the 25 November APP 12 Request

75. Insofar as it pertains to his 25 November APP 12 Request, Mr Knowles’s further amended originating application of 30 September 2019 should (and will) be dismissed. The relief that is sought—namely, declaratory relief—should (and will) be declined in the court’s discretion on the

basis that there is no utility in granting it. Even were that otherwise, it would be declined on the basis that the respondent's (or the Department's) conduct, insofar as it pertained to that request, was not engaged in in contravention of the Privacy Act and did not otherwise amount to an improper exercise (or improper exercises) of statutory power.

3.2. The 2 March APP 13 Request

3.2.1. *Summary of the contentions advanced*

76. In 2014, the Australian Information Commissioner ruled on a complaint that Mr Knowles had made against the Other Department. It held that the Other Department had interfered with Mr Knowles's privacy by disclosing personal information about him to the Department. That information contained (or assumed the form of) statements of opinion about Mr Knowles, including about his mental health and the level of threat that he posed to the physical safety of himself and others. Those opinions appear to have stemmed at least partly from what were considered aggressive or obnoxious communications that Mr Knowles had directed toward an officer or officers of the Other Department. The particulars of those communications and the opinions that were formed (and, ultimately, disclosed to the Department) in consequence of them need not here be recited. It suffices to note that the Other Department made certain disclosures to the Department at least in part on the strength of the opinions that had been formed about Mr Knowles. The Australian Information Commissioner determined that those opinions neither warranted nor authorised the disclosures that were made (that determination is referred to, hereafter, as the "**OAIC Determination**").
77. By his 2 March APP 13 Request, Mr Knowles sought the correction of Departmental records insofar as they chronicled statements of opinion that were inconsistent with the OAIC Determination. It is in respect of the Department's conduct in response to that request that he now seeks various remedies.
78. The OAIC Determination has since been the subject of an application for review before the Administrative Appeals Tribunal. That review resulted in the determination being set aside; and a subsequent appeal of that decision to this court was dismissed. In both of those proceedings, Mr Knowles was referred to by a pseudonym. It is for that reason that the Other Department has not been identified in these reasons. In order to preserve Mr Knowles's anonymity in those other proceedings, neither of the decisions that they generated will be cited.
79. The conduct engaged in by the Department in response to Mr Knowles's 2 March APP 13 Request is not in contest: certain Departmental records were annotated by having attached to them a copy of the OAIC Determination. Mr Knowles maintains that that course (hereafter, the "**Annotation Decision**") was not one that was open to the Department. Instead, he maintains that the Department ought first to have made a decision one way or the other whether or not it would correct the personal information that it retained about him. In the event that it determined not to correct that information, Mr Knowles maintains that the Department was obliged to tell him as much and to provide him with reasons justifying that course. Then and only then, so Mr Knowles maintains, was it open to him to request that the Department associate a copy of the OAIC Determination with the relevant records in which his personal information was contained.
80. By way of relief, Mr Knowles seeks:

- (1) under the ADJR Act:
 - (a) an order under s 16(1)(a) setting aside the Annotation Decision; and
 - (b) an order under s 16(1)(b) referring the 2 March APP 13 Request back to the Department for further consideration; or, alternatively,
- (2) under the Judiciary Act, that there issue:
 - (a) a writ of certiorari that removes into this court and quashes the Annotation Decision; and
 - (b) a writ of mandamus that requires the Department to reconsider the 2 March APP 13 Request; or, further in the alternative,
- (3) injunctions under s 121 of the RP Act requiring that the Department refrain from relying upon or giving effect to the Annotation Decision, and that it otherwise reconsider its response to the 2 March APP 13 Request.

81. Mr Knowles also complains that the Department did not respond to his 2 March APP 13 Request within 30 days, as APP 13 required. In respect of that failure, he seeks declaratory relief to record the existence of his right to such a response within that timeframe and the Department's breach of that right.

3.2.2. Appropriateness of declaratory relief

82. I will deal, first, with Mr Knowles's request for declaratory relief. It is not necessary that I should replicate what has already been said about the appropriateness of that species of relief, nor about the circumstances in which it might be withheld on discretionary grounds. For reasons equivalent to those outlined in section 3.1.2 of these reasons, I do not consider that the circumstances here warrant an exercise of the court's discretion to grant declaratory relief. There is no utility in granting what is sought. Declaratory relief is granted to record the existence or otherwise of a particular state of affairs and, thereby, to resolve a justiciable controversy. Here, Mr Knowles seeks little (if anything) more than an advisory opinion from the court. That is not an appropriate exercise of the remedy.
83. That notwithstanding, I confess some sympathy for the submission that Mr Knowles advanced. APP 13 required that the Department respond to the 2 March APP 13 Request within 30 days. Although the statutory requirement could be clearer, there is force in Mr Knowles's submission that that required, within that timeframe, some indication from the Department as to whether it would or would not correct what Mr Knowles had asked it to correct. That does not appear to have happened. Had the Department indicated to Mr Knowles within the 30-day timeframe the intention to which it subsequently gave effect, the complexion of the present matter might well have been different.
84. Even assuming that Mr Knowles's criticisms of the Department's response (or non-response) to his 2 March APP 13 Request are well- founded, I am not satisfied that that suffices to warrant an exercise of the court's discretion to grant declaratory relief. Although doing so would undoubtedly validate those criticisms, it would nonetheless be legally inutile.

85. The analyses that follow concern the remaining claims for relief (that is to say, claims for relief other than declaratory relief) that arise in respect of the 2 March APP 13 Request.

3.2.3. Existence of alternative remedies

86. As is outlined above, the Privacy Act establishes mechanisms by which a complainant might seek to review conduct engaged in by an APP Entity. At first instance, it provides for the making, investigation and determination of complaints about acts or practices that amount to an interference or interferences with an individual's privacy: Privacy Act, Part V (above, [39]-[40]). Determinations so made may themselves be reviewed by the Administrative Appeals Tribunal: Privacy Act, s 96(1)(c) (above, [41]).
87. Despite his apparent familiarity with those provisions, Mr Knowles has not availed himself of them insofar as concerns his 2 March APP 13 Request. The mechanisms established by the Privacy Act afford Mr Knowles adequate rights of review in respect of Departmental conduct that he considers constitutes an interference or interferences with his privacy. Insofar as concerns the 2 March APP 13 Request, the existence of those mechanisms warrants the court's refusing to grant relief under the ADJR Act as a matter of discretion: ADJR Act, s 10(2)(b).
88. The existence of those mechanisms also informs the court's discretion to grant relief under the alternative sources of power that Mr Knowles seeks to invoke, namely s 39B(1) of the Judiciary Act and s 121(1) of the RP Act. A court may, in its discretion, withhold prerogative relief in the nature of certiorari and mandamus on the basis that a party has chosen not to avail him or herself of convenient alternative remedies: see *Dranichnikov v Minister for Immigration and Multicultural Affairs* (2003) 197 ALR 389, 395-396 [33] (Gummow and Callinan JJ); *CSL Australia Pty Ltd v Minister for Infrastructure and Transport* (2014) 221 FCR 165, 212-213 [219] (Allsop CJ, with whom Mansfield J agreed). Doing so has been described as the "general rule": *Tooth & Co Ltd v Council of the City of Parramatta* (1955) 97 CLR 492, 498 (Dixon CJ, with whom McTiernan, Webb, Fullagar and Kitto JJ agreed). Where relevant, equivalent considerations guide the exercise of the court's power to grant injunctive relief under s 121 of the RP Act and, indeed, all discretionary relief, whatever be the court's power to grant it: *Saitta Pty Ltd v Commonwealth* (2000) 106 FCR 554, 575 [104] (Weinberg J).
89. Insofar as concerns his 2 March APP 13 Request, there is no evidence that Mr Knowles has availed himself of the processes for which Part V of the Privacy Act provides. If the Department's conduct in connection with that request involved improper exercises (or nonexercises) of statutory power under the Privacy Act, then the review mechanisms to which Part V and s 96(1) of the Privacy Act gives effect offer adequate and convenient means of correction. That alone is basis enough to decline to grant the relief that Mr Knowles seeks under s 39B(1) of the Judiciary Act and s 121(1) of the RP Act.

3.2.4. Annotation of records is not unlawful

90. In any event, I do not accept Mr Knowles's submission that the Department's Annotation Decision was beyond what the Privacy Act sanctioned. Upon receiving the 2 March APP 13 Request, the Department was compelled to take reasonable steps to correct personal information that it retained about Mr Knowles. "Correction", in that sense, required the taking of steps to ensure that that information was "accurate, up-to-date, complete, relevant and not misleading": APP 13.1.

91. Here, Mr Knowles’s request was aimed at the opinions that the Other Department formed about him and, more precisely, the Departmental records in which the expression of those opinions was chronicled. Even in the face of the OAIC Determination, it is difficult to see how records that contained (or otherwise referred to) expressions of those opinions might be thought to have been inaccurate, out of date, incomplete or irrelevant. Mr Knowles’s complaint, of course, was that the opinions were unsubstantiated: a view that the OAIC Determination validated (at least until it was set aside). But to observe as much is not to demonstrate that the Department’s records inaccurately recorded the opinions that were communicated to it, or that those opinions had since been altered or qualified such that the records in question were no longer up-to-date or were otherwise incomplete, or were irrelevant in some way. Mr Knowles did not allege as much (either by his 2 March APP 13 Request or by his submissions before this court). He simply wished (and wishes) for it to be known—that is, for the Department’s records to reflect—that the opinions that had been communicated to it were unsubstantiated in light of the OAIC Determination. He sought to ensure that the Department’s records were not misleading (in the sense that a person having occasion to review them might be drawn to conclude that opinions expressed about him were well-founded).
92. APP 13 does not require that an APP entity take any particular steps by way of correction of information. There is, in my view, no reason why a record that is misleading because it records an opinion that has subsequently been the subject of judicial or quasi-judicial criticism or repudiation might not be “corrected”—that is to say, rendered not misleading—by annexing to it a record of that criticism or repudiation.
93. Mr Knowles does not here submit that there were other steps that the Department ought reasonably to have taken in order to correct the personal information that it held about him. He says, instead, that the association of the OAIC Determination to existing records was something that could only be done at his request, and only following (first) a determination by the Department that it would not take steps to correct its records and (second) the provision of written reasons explaining that determination. Mr Knowles contends that, by acting as it did, the Department misunderstood—and failed properly to discharge—its statutory obligation. That, in turn, is said to warrant relief under s 16(1) of the ADJR Act, prerogative relief under s 39B(1) of the Judiciary Act and/or injunctive relief under s 121(1) of the RP Act.
94. I do not accept that the Department misunderstood its obligations or otherwise acted inconsistently with them vis-à-vis the 2 March APP 13 Request. It is apparent that the Department resolved to correct the records that Mr Knowles asked it to correct. That it did so is hardly surprising given the existence at the time of the OAIC Determination, which rendered the opinions about Mr Knowles (or at least some of them) unsustainable. The Department did not communicate its resolution to Mr Knowles and it probably should have. But, regardless, it was entitled to see to that correction by the means that it adopted (namely, by annexing the OAIC Determination to the relevant, existing records). Indeed, doing so was at least superficially consistent with what Mr Knowles had requested. Having opted to take that course, the Department was not obliged to provide Mr Knowles with a notice under paragraph 13.3 of APP 13, and Mr Knowles was not entitled to initiate the process for which paragraph 13.4 of APP 13 provides.

3.2.5. Utility of relief

95. There is another basis upon which the court should, in its discretion, decline to grant the relief that Mr Knowles has sought in respect of his 2 March APP 13 Request. As is set out above, the OAIC Determination is no longer extant: it was set aside by the Administrative Appeals Tribunal and an appeal from that decision was dismissed by a full court of this court. Both of those events occurred after the 2 March APP 13 Request was made.
96. That the 2 March APP 13 Request was premised upon the existence of the OAIC Determination is not readily in doubt. It was by the OAIC Determination that the opinions communicated to the Department by the Other Department were held not to be substantiated. Mr Knowles's demand was that the Department annotate the records in which the Other Department's opinions were expressed to "...specifically advise that these defamatory and false claims by [that Other Department] were not only unlawful but also found to be unsubstantiated" and to "explicitly note that a Determination found these claims by [the Other Department] a breach of the Privacy Act and therefore unlawful". In context, Mr Knowles's reference to what had been "found" or determined can only be understood as a reference to the OAIC Determination.
97. Given that the foundation upon which the 2 March APP 13 Request was erected has since been washed away, it is impossible to see what utility there might be in setting aside the Annotation Decision and requiring that the Department reconsider its response. The court's discretion to grant relief in that nature—whether under the ADJR Act, the Judiciary Act or the RP Act—is properly informed by that want of utility. Even had I come to a different view about the availability of alternative remedies and the propriety of the Department's conduct in answer to the 2 March APP 13 Request, I would, nonetheless and in the exercise of the court's discretion, have declined to grant the relief that Mr Knowles seeks on the basis that granting it would almost certainly be pointless.

3.2.6. Conclusion in respect of the 2 March APP 13 Request

98. Insofar as it pertains to his 2 March APP 13 Request, Mr Knowles's further amended originating application of 30 September 2019 should (and will) be dismissed. The declaratory relief that is sought should (and will) be declined in the court's discretion on the basis that there is no utility in granting it. The other relief that is sought should (and will) be declined:
 - (1) in the court's discretion on the basis that the Privacy Act adequately provides for an alternative, convenient means of review of the Department's conduct; and, alternatively,
 - (2) on the basis that the respondent (or the Department) did not, in any event, misconstrue or fail to comply with the requirements of APP 13, nor otherwise err by conducting itself as it did in response to the 2 March APP 13 Request.

Had I reached different conclusions on those fronts, I would nonetheless have declined to grant that other relief on the basis that there would be no utility in doing so given that the OAIC Determination is no longer extant.

3.3. The 3 March Demand Email

3.3.1. Summary of the contentions advanced

99. Mr Knowles’s contentions relating to his 3 March Demand Email are straightforward. He maintains that, by that communication, he requested under APP 13 that the Department correct personal information about him that was contained in Mr Heldon’s email of that evening (above, [21]). It is not in contest that the Department did not respond to that request and did not make any correction as requested. Mr Knowles contends that those failures were in contravention of APP 13 and, thereby, amount to an interference with his privacy for the purposes of the Privacy Act.
100. Mr Knowles moves the court for the following relief, namely:

(1) under the ADJR Act:

- (a) an order under s 16(3)(a) compelling the Department to consider his 3 March Demand Email; and
- (b) declaratory relief under s 16(3)(b) to record or state his rights and/or the Department’s obligations in respect of that communication; or, alternatively,

(2) under s 39B(1) of the Judiciary Act:

- (a) that there issue a writ of mandamus that requires the Department to consider the 3 March Demand Email; and
- (b) declaratory relief to record or state his rights and/or the Department’s obligations in respect of that communication; or, further and alternatively,

(3) an injunction under s 121(2) of the RP Act to compel that Department to consider his 3 March Demand Email.

3.3.2. Nature of the 3 March Demand Email

101. In order to properly appreciate the character of the 3 March Demand Email, it is appropriate to rehearse the exchange that preceded it. That exchange began the previous day with Mr Knowles’s 2 March APP 12 Request (above, [18]). On any view, that communication—in which, amongst other things, Mr Knowles referred to Mr Heldon as an “unethical fuckhead”—was needlessly petulant and obnoxious.
102. Mr Heldon responded by requesting a copy of the OAIC Determination to which the 2 March APP 12 Request referred. He sensibly did not react to Mr Knowles’s gratuitous disrespect.
103. Later that afternoon, Mr Knowles emailed Mr Heldon an internet link to the OAIC Determination. In that email, he intimated that Mr Heldon ought already to have been aware of the determination, or otherwise ought to have been able to locate it himself. He threatened to “eventually” subpoena Mr Heldon, to subject him to cross-examination and, thereby, to expose Mr Heldon’s “disgraceful behaviour” on a “permanent court record”, which he suggested would “not

go so well if [Mr Heldon] ever want[ed] to do anything else in [his] life". He suggested that Mr Heldon was "lazy or ignorant" and invited him to "[s]top fucking around".

104. It was in response to those bizarre provocations that Mr Heldon sent the response upon which the 3 March Demand Email fixed. By his email of that evening (above, [21]), Mr Heldon began by apologising to Mr Knowles for any appearance of laziness or ignorance, and pointed out that he was, in fact, not a "privacy officer" nor "legally trained in privacy". Instead, he pointed out, his role was one of coordination: it fell to him to coordinate the Department's responses to Mr Knowles's request, requiring, as they inevitably did, input from a range of personnel across the various different parts of the Department. He noted that he did not have any decision-making power and that, in the absence of a request from Mr Knowles that somebody else should coordinate the Department's response, he would continue to do so, including in the face of Mr Knowles's "expletives and threats about taking some action against [him]."
105. Of particular significance was the following passage of Mr Heldon's email:

I understand that I am currently the focal point of your frustrations with Defence and you hold me personally responsible for Defence's responses to date - I assume your expletives and threats are only a reflection of this frustration and do not imply a serious or imminent threat to my health or safety.
106. By his 3 March Demand Email, Mr Knowles described those comments as "defamatory" and demanded that they be "destroy[ed]...from Defence records". He again threatened Mr Heldon with "action against [Mr Heldon] personally" in the event that his demand was not met.
107. This aspect of Mr Knowles's cases turns, in part, upon whether or not Mr Heldon's remark (about Mr Knowles's obnoxious language not reflecting a serious or imminent threat to his [Mr Heldon's] health or safety) constitutes personal information about Mr Knowles. The Department submits that it does not. Before me, Mr Knowles conceded that he didn't "necessarily know...if that falls into the definition of personal information". There is at least some basis for supposing that the remark was more interrogatory than a statement of opinion personal to Mr Knowles.
108. On balance—and not without some hesitation—I accept that Mr Heldon's remark (or the email that contained it) amounted to personal information (as the Privacy Act defines that concept) concerning Mr Knowles. It was a statement of opinion about what Mr Heldon understood was conveyed by the intemperate language of Mr Knowles's earlier emails: specifically, that Mr Knowles was frustrated; but not to the point that he posed a threat to Mr Heldon's health or safety. That conclusion appears very much to align with reality: Mr Knowles was plainly frustrated with the manner in which the Department had responded to his prior requests for information but there is no evidence that that frustration risked expression in the form of physical threats or aggression aimed at Mr Heldon. It is difficult to see how Mr Heldon's opinion was wrong, much less defamatory.
109. That accepted, it is necessary to consider whether the 3 March Demand Email amounted to a request for correction under APP 13. It is plain enough that Mr Knowles clothed his 3 March Demand Email in the language of the Privacy Act. His demand that Mr Heldon "destroy these defamatory claims from Defence records about threatening behaviour" was expressly said to be

required “[u]nder APP13”. Those words alone, however, are not sufficient to constitute the email as a request for correction under APP 13.

110. There are two ways in which an APP entity might be obliged to correct (or consider correcting) personal information held about a person. The first is if it has occasion to consider, of its own volition, that that information is inaccurate, out-of-date, incomplete, irrelevant or misleading. The second is that it receives a request for correction from the person to whom the information pertains. Plainly, the circumstances of this case involve that second trigger. At issue is whether the 3 March Demand Email amounted to a request to correct information.
111. I am not satisfied that it did. The 3 March Demand Email did not request the correction of anything. It was little (if anything) more than a demand that records be “destroyed”, couched in objectionable language that appears to have been calculated only to bully or belittle Mr Heldon. The 3 March Demand Email does not employ the term “correction”, nor any analogue of it (the subject header of the email does but only because it was carried over from the 2 March APP 13 Request, which of course *was* a request for correction of information under APP 13).
112. I am not satisfied that the Department’s failure to respond to the 3 March Demand Email amounts in any way to a contravention of APP 13 (nor to an interference by the Department in Mr Knowles’s privacy).
113. That being the case, the relief that Mr Knowles seeks should (and will) be declined for want of a legal basis for granting it.

3.3.3. Discretionary considerations

114. Even were I to have formed a different view about the nature of the 3 March Demand Email, I would decline to grant the relief that Mr Knowles seeks on discretionary bases.
115. Insofar as he seeks declaratory relief related to that demand, I would decline to grant it for reasons equivalent to those explained in sections 3.1.2 and 3.2.2. The relief that is sought would achieve nothing more than to vindicate Mr Knowles’s opinion that the Department ought to have responded to or acted upon (or was required under APP 13 to respond to or act upon) his 3 March Demand Email, and/or to serve as advice to the Department that that view is correct. For reasons already outlined, that view is not correct; but even if it were, declaratory relief is not a remedy that is appropriately deployed in the service of those ends. Although it would undoubtedly validate Mr Knowles’s criticisms of the Department’s failure to respond to his 3 March Demand Email, declaratory relief in the form sought would be legally pointless (in the sense that it would not serve to vindicate any presently-existing legal rights, nor otherwise resolve any presently-existing justiciable controversy). In light of that want of utility, I am not satisfied that the present circumstances warrant an exercise of the court’s discretion to grant declaratory relief in connection with the 3 March Demand Email.
116. Insofar as Mr Knowles seeks other relief related to that demand, I would decline to grant it for reasons equivalent to those explained in section 3.2.3 above. The Privacy Act— particularly Part V, which provides for the initiation, investigation and determination of complaints concerning alleged interferences with people’s privacy, and s 96(1), which provides for the review of such determinations by the Administrative Appeals Tribunal— affords Mr Knowles adequate and

convenient rights of review in respect of Departmental conduct that he considers was engaged in in contravention of APP 13. The existence of those processes warrants the court's refusing, as a matter of discretion, to grant relief under the ADJR Act in relation to the 3 March Demand Email: ADJR Act, s 10(2)(b). It also warrants the court's refusing, in its discretion, to grant relief in relation to that email under the alternative sources of power that Mr Knowles seeks to invoke, specifically s 39B(1) of the Judiciary Act and s 121(2) of the RP Act (see above, [88]).

3.3.4. Conclusion in respect of the 3 March Demand Email

117. Insofar as it pertains to his 3 March Demand Email, Mr Knowles's further amended originating application of 30 September 2019 should (and will) be dismissed. The respondent (or the Department) did not contravene APP 13—nor otherwise err—by failing to respond to (or otherwise act upon) that communication. Even if he (or it) did, I would, in the exercise of the court's discretion:

(1) decline to grant the declaratory relief that Mr Knowles seeks because there is no (or insufficient) utility in granting it; and

(2) decline to grant the other relief that Mr Knowles seeks because the Privacy Act adequately provides for an alternative, convenient means of review of the Department's conduct.

4. CONCLUSIONS

118. Mr Knowles's further amended originating application of 30 September 2019 should (and will) be dismissed. The respondent seeks an order that Mr Knowles pay his costs. That is appropriate and an order to that effect will also be made.

I certify that the preceding one hundred and eighteen (118) numbered paragraphs are a true copy of the Reasons for Judgment of the Honourable Justice Snaden.

Associate:

Dated: 17 September 2020



Australian Government

Office of the Australian Information Commissioner

Privacy complaints – Managing section 36 privacy complaints

Investigator's Guidelines



1 July 2022

OAIC

Contents

Executive summary	2
Part 1: Role of the investigator	2
Part 2: Assessing a case	2
Part 3: Pathways of finalisation	7
Immediate decline	8
Information gathering	14
Part 4: Decision making	21
Part 5: Referring a matter to the Determinations team	27
Part 6: Communicating with the parties	30
Part 7: Appendices	36
Privacy complaint about Tyco Australia Group Pty Ltd t/a ADT Security	36
The complaint	36
Background	37
My view	37
Invitation to provide further information	38
Adequately dealt with	38
Preliminary view regarding next steps	41

Executive summary

The purpose of this guide is to assist investigators to manage a privacy complaint lodged under s 36 of the Privacy Act.

Part 1: Role of the investigator

1.10 The investigator has a number of roles in managing a section 36 privacy complaint:

- **Case officer** - they are the case officer tasked managing the administration of the case, with communicating with the parties, reporting to their supervisor and the Executive on status and anticipated timeframes, and handling all enquiries in relation to the case, including access requests, FOI applications and service complaints.
- **Investigator** - they are the investigator tasked with gathering and assessing information in order to achieve an appropriate outcome for the case.
- **Delegate** – they are the delegate of the Commissioner, exercising all their delegated functions and powers with care, skill and diligence.
- **Administrative decision-maker** – they are the administrative decision-maker for the case, as they make final decisions under the Privacy Act that affect the rights and interests of individuals and which may be scrutinised by review bodies.

Part 2: Assessing a case

Director's instructions

2.10 The goal of the investigator is to bring a privacy complaint to finalisation as quickly and fairly as possible. From the outset, the investigator needs to use their critical analysis skills and their knowledge of the Privacy Act, and related legislation, to find the best pathway to finalisation.

2.11 The investigator receives a complaint from the Director with 'instructions' that set out the following:

- CP reference
- Brief facts and claims
- Relevant APPs
- Remedies sought
- Complexity rating
- Recommended pathway.

2.12 The purpose of the director's instructions is to provide the investigator with a quick overview and suggested direction for the conduct of the case. These are sent to the investigator by email and at the same time, the matter is allocated to the investigator on Resolve.

Example - Director's instructions (sent by email)

Facts: C provides PI to R, a training company for the purposes of requesting an extension for a course task. C's employer mentions details in the medical certificate and has a hard copy of the certificate.

Claims:

- Claim 1 – The respondent has disclosed C's sensitive information for a secondary purpose without consent. This claim raises a breach of APP 6.

APPs: APP 6

Remedies: Compensation and apology

Rating: Simple – R denies disclosure.

Comments: Simple evidentiary fact finding.

Instructions (investigation plan notes): PIs or open an investigation and send a s 44 to third party. Find out whether it received the medical certificate and from whom.

Organising the file

- 2.13 A well-organised file will place the investigator in the best position to efficiently and effectively review the case. Soon after a matter is allocated to the investigator they should tidy up the file in accordance with the Investigations procedures: File management protocols [\[link\]](#)

Investigator's assessment

- 2.14 The investigator's assessment will assist the investigator to become the expert on the facts and issues in the case. It will also help them to plan and strategise a way to bring the case to finalisation.
- 2.15 After receiving the director's instructions, the investigator's first step is to consider whether there is any reason why they cannot take the matter, such as a conflict-of-interest, and respond to the director as soon as possible.
- 2.16 The investigator next considers whether they agree with the director's instructions. It is expected that the investigator will know the details of the case and will be in the best position to bring the case to a quick and fair outcome. The director's instructions are a broad view of the case and are prepared quickly. As such, factual detail may be overlooked and errors may be made.
- 2.17 As soon as they receive the case, the investigator should acquaint themselves with the facts, including by drafting a chronology. The investigator should consider whether they agree with the director's instructions, communicate their views and reach an agreed strategy with the director as soon as possible. The investigator's assessment is to be discussed with the director,

and must be documented, whether in an email to the director filed to Resolve or in the investigation plan.

- 2.18 The components of the investigator's assessment should set out the facts, claims, relevant APPs and remedies. If the matter proceeds to investigation, the information in this assessment will form the basis for the investigation plan.

Facts

- 2.19 The facts are the story of the complainant and includes things like who they are in relation to the respondent, what their dealings with the respondent have been and why they are aggrieved by the respondent's conduct.
- 2.20 Check the facts as set out in the privacy complaint form and as detailed in any subsequent emails sent to ER.

Claims

- 2.21 The claims are much more structured and are essentially acts and practices that may be an interference with privacy. It is important to separate out the claims with precision, as these numbered claims will guide all the decision-making in the case, and a failure to consider a claim will amount to an error of law.

Setting out the claims

- 2.22 An individual has an entitlement under s 36 to make a complaint to the Commissioner about an act or practice that may be an interference with their privacy. Individuals do not have to say which APP is they think the respondent has breached – all they need to do is raise acts and practices about which they are aggrieved.
- 2.23 Where a complaint has been lodged, investigators as the Commissioner's delegate, have an obligation to investigate an act or practice if the act or practice 'may be an interference with the privacy of an individual', subject to exceptions. This means that investigators must determine whether the acts and practices alleged by the complainant raise conduct that may be a breach of one or more of the APPs.
- 2.24 The first step is to set out and number the acts and practices the complainant alleges. While claims may have been discerned through the early resolution process and maybe set out on documents created by early resolution, it is important to ensure that the investigation correctly identifies the claims as put in the complaint. The starting point will be the complaint document.
- 2.25 The steps to setting out the claims are:
1. Separate each act/ or practice
 2. Reformulate the claimed act/practice as a potential privacy breach
 3. Locate the applicable APP.

Example - Complaint

I am making a complaint about a company known as the Database.

Today I did a Google search to check if an individual has been to court. The search hit comes up with the Database in first location of web hits.

I put my name into the "free search" and it revealed 52 court listings in the criminal courts under my name. I attended court on charges where I never entered a plea and all charges and matters were dismissed by the DPP.

I was in an abusive relationship where the perpetrator involved submitted me to intense abuse and engaged in criminal acts to implicate me.

I emailed the Database contact email and asked what the process is to remove records. I had a reply email from them but they did not offer any helpful suggestions. I then rang the contact number today (Sunday 7th June).

I asked the person what the process was to have a record removed from this database and he said that he would not remove any records. He said that the information is freely available but I pointed out that by the public having access to his company's database does not always provide helpful information and asked in my case that he remove my name and records. He refused and I said I would take this further and make a complaint to the Privacy Commissioner.

- 2.26 Sometimes complainants include information that is not relevant to the acts and practices. The investigator's job is to cut through the information provided in the complaint document to determine what are the 'acts and practices' alleged that may be an interference with privacy.
- 2.27 From the example complaint document, the investigator can see that there are two real grievances:
- The fact that the complainant's court attendances have been disclosed on a database and the complainant says that the information does not reflect the outcomes of having attended court
 - The fact that the complainant asked for this to be removed to no avail.
- 2.28 The rest of the information is irrelevant to discerning acts and practices and whether they breached the APPs, though they may be relevant when considering remedies.
- 2.29 Once the investigator has correctly identified the acts and practices, they should ask themselves which APP fits the act or practice. In this case, the complainant's first concern is that the court listings do not reveal additional personal information that provides a complete picture, namely that they never entered a plea and that all charges were dismissed. Essentially, they are aggrieved about the quality of the personal information disclosed. The complainant's second concern is that the respondent did not agree to remove the information. Essentially, this could be taken to be a correction request.

Example of setting out the claims

Claim 1 - The respondent disclosed the complainant's personal information about them having attended court in relation to criminal offences by publishing it on its database. This claim raises a breach of APP X.

Claim 2 - The information was incomplete as it does not show dismissals of charges. This claim raises a breach of APP X.

Claim 3 - The complainant requested that the respondent correct the personal information they contended was incomplete by removing it and the respondent did not take any steps to do so. This claim raises a breach of APP X.

2.30 After having conducted this exercise the investigator will now have the claims of the complainant. They should set these claims out as numbered in the investigation opening letter and stick to these numbers throughout the course of the investigation. They will also have satisfied themselves that these claims raise potential interferences with privacy. Next, they will locate the relevant issues, that is, the relevant APPs that apply.

Relevant APPs

2.31 The next step to assessing the case is to locate the relevant APPs. Complainants do not need to specify the relevant APP they think the respondent has breached. All they need to is set out the acts and practices of which they are aggrieved. It is up to the investigator to locate any and all relevant APPs that apply.

2.32 Locating the relevant APPs to a particular set of facts is a skill that develops with experience and practice. This is a task that requires the investigator to consider whether anything raised by the complainant could be a breach on the part of the respondent. It can help to think of the order of privacy practices from the respondent's perspective as follows:

- The respondent creates a privacy policy, as well as practices, procedures and systems to handle personal information.
- The respondent collects certain personal information from the complainant.
- The respondent discloses personal information of the complainant.
- The respondent holds and maintains the quality of personal information of the complainant.
- The respondent protects personal information from certain risks.
- The respondent owes access rights to the complainant.

2.33 Any acts or practices raised by the complainant fit somewhere along these privacy events.

Example – Locating APPs

Claim 1 - The respondent disclosed the complainant's personal information about them having attended court in relation to criminal offences by publishing it on its database. [This claim raises a breach of APP 6.](#)

As can be seen from this example, the claim involves disclosure. APP 6 should be considered.

Claim 2 - The information was incomplete as it does not show dismissals of charges. [This claim raises a breach of APP 10.](#)

As can be seen from this example, the claim involves reference to a quality factor, in this case, completeness. APP 10 should be considered.

Claim 3 - The complainant requested that the respondent correct the personal information they contended was incomplete by removing it and the respondent did not take any steps to do so. [This claim raises a breach of APP 13.](#)

As can be seen from this example, the claim involves reference to correction. APP 13 should be considered.

Remedies

- 2.34 The next step is to list the remedies. It is important to understand what it is the complainant seeks requested from the beginning. Complainant's may expand their requested remedies. What the complainant originally sought should form the basis of any assessment that is fair and reasonable.
- 2.35 In some circumstances, what is fair and reasonable will be informed by an expanded set of requests, particularly where the respondent has caused delay to the complainant or engages in conduct that exacerbates any loss or damage of the complainant throughout the case.
- 2.36 When providing instructions, the Director will give the case a complexity rating is intended to assist the investigator in planning the matter and uses the following key:

Part 3: Pathways of finalisation

- 3.2 At the forefront of the investigator's mind from allocation of the case, is the pathway by which the case will be finalised. This may change throughout the conduct of the case, but the investigator must always start with a plan to begin with one particular pathway, and a backup plan if they need to switch to another pathway.
- 3.3 Most cases in Investigations are finalised by either decline or referral for determination. Occasionally, cases are finalised by a complainant withdrawing their complaint.
- 3.4 The possible pathways upon allocation by the director are:
 - 1) immediate decline
 - 2) preliminary inquiries, then decline or investigate

- 3) investigate, then decline or refer for determination.

Immediate decline

- 3.5 In some cases it might be possible to immediately finalise a case by way of decline without undertaking any information gathering. This occurs infrequently, as most of the cases referred to Investigations from Early Resolution require some level of information gathering.
- 3.6 The director may recommend immediate decline where the file suggests the following:

Provision	Decline type	When to consider
S 41(1)(a)	No breach ('no breach' decline)	There is enough evidence on the file to show that there has been no breach.
S 41(2)(a)	Adequately dealt with (ADW decline)	There is enough evidence on the file to show that the complainant first complained to the respondent and the respondent has adequately dealt with, or is, adequately dealing with the case.
S 41(1)(da)	Not warranted in all the circumstances (not warranted decline)	While the respondent may have breached the privacy act, the seriousness of the alleged breach is low, the case is unlikely to settle and investigation is unlikely to result in better outcomes.

- 3.7 Most relevant to the Investigations team are the 'no breach' decline, ADW decline and not warranted decline. There are other declines powers with which the investigator needs to be familiar. The **Declines Guide** sets out the decline powers in detail.

'No breach' decline

- 3.8 The 'no breach' decline power can only be exercised where the delegate is satisfied that the act or practice is not an interference with the privacy of a complainant.
- 3.9 This means that the delegate will need to be satisfied on the evidence that either:
- 1) the alleged acts and practices did not occur, or did not occur in the way alleged by the complainant, or
 - 2) assuming the alleged acts and practices occurred, they are not a breach of the privacy act.
- 3.10 In deciding whether the acts practices occurred, the delegate must apply the balance of probabilities. That means that the decision maker needs to be satisfied that it is more likely than not that the fact occurred, with reference to credible evidence, and using an assessment based on logical grounds.
- 3.11 The complainant only needs to provide evidence of matters within their knowledge and control. When it comes to evidence that would reasonably be within the respondent's, or

others, knowledge and control, it is up to the delegate to seek that information from the respondent or other sources, which will usually require inquiries or an investigation.

- 3.12 For that reason, it can be difficult to find from the outset that the alleged practices did or did not occur.
- 3.13 As such it is usually preferable to assume that the acts and practices did occur and determine whether they would amount to an interference with privacy under the APPs.

Example – ‘No breach’ decline

The following is an example of a privacy complaint that can be immediately declined as ‘no breach’ without preliminary inquiries or investigations. The investigator does not need to use any formal information gathering powers to finalise this case. The Investigator’s tools required are:

- 1) a clear understanding of the acts and practices alleged by the complainant
- 2) a working knowledge of which APPs apply to those acts and practices
- 3) an inspection of the file, including responses of the respondent
- 4) desktop research such as the respondent’s website.

Complaint - The complainant (C) complains about the respondent (R) collecting her personal information in the form of her name, address and profession, disclosing it on the R’s website, and inviting individuals to write reviews about the complainant.

Remedy sought - C wants R to delete the personal information.

R’s response - The R is an entity that runs a website allowing individuals to set out reviews on healthcare providers.

‘No breach’ decline recommendation - Assuming that the respondent has in fact collected the complainant’s personal information, there is no breach.

Reasoning:

The relevant APPs are APP 3, APP 6 and APP 11:

- APP 3 - the personal information is not sensitive information and the respondent is an organisation, therefore APP 3.2 applies.
- APP 3.2 - The respondent claims that its functions and activities are providing a review website about health professionals. The respondent’s website confirms this. The personal information was collected for the purpose of carrying out the review website.
- APP 6 - The purpose for which the respondent collected the personal information was to conduct the review website. This is the same purpose for which it was disclosed.
- APP 11 - The Respondent continues to carry out functions and activities of the review website. It therefore continues to need the personal information for a purpose it was collected under APP 6. It is therefore not obliged to take steps to destroy or de-identify.

Adequately dealt with (ADW) decline

- 3.14 The ADW decline power should be considered in cases where the respondent has made an offer to resolve the case.
- 3.15 The ADW power can only be exercised where the delegate is satisfied that:
- 1) The complainant has complained to the respondent and
 - 2) The respondent has dealt or is dealing adequately with the complaint.
- 3.16 The first element is important to check as the OAIC has in the past had to remit matters from the court on the basis that the delegate failed to consider whether the complainant had taken the particular act or practice to the respondent prior to making the decision.
- 3.17 In the event that the delegate considers the case suitable for ADW decline but for the fact that the complainant has not complained to the respondent, the delegate should proceed to consider not warranted decline under s 41(1)(da).
- 3.18 In determining whether the respondent has dealt with or is adequately dealing with the complaint, at the referral to Investigations stage, the question is whether the respondent is providing a remedy to the complainant that is fair and reasonable.
- 3.19 In order to determine this, the delegate should consider the following:
- 1) What remedies has the complainant sought?
 - 2) Has the respondent provided, or offered to provide all or some of the remedies?
 - 3) Are those remedies fair and reasonable?
 - 4) Is there any injustice to the complainant in finding that the remedies are sufficient to show that the responded has adequately dealt with the complaint?
- 3.20 The delegate will be able to find that the respondent has adequately dealt with the complaint where:
- 1) the respondent has provided all the remedies sought by the complainant
 - 2) the respondent has provided some remedies sought by the complainant and:
 - the delegate has assessed these remedies, compared to the alleged breach, to be fair and reasonable in addressing the privacy breach, and
 - in refusing the remaining remedies there is no substantial injustice to the complainant.
 - 3) The respondent has provided remedies not sought by the complainant, however, the delegate has assessed these to be fair and reasonable remedies, including that they logically connect to the privacy breach.
- 3.21 The delegate will be able to find that the respondent is adequately dealing with the complaint where the respondent has undertaken to provide remedies, the delegate has assess those remedies to be consistent with the points set out in the preceding paragraph and the delegate is reasonably satisfied the respondent will follow through with their undertaking.

Examples – ADW decline

The following are examples of how a delegate may assess remedies in a particular case to consider their appropriateness for ADW decline.

Facts: The complainant's (non-sensitive) personal information was collected without notifying the complainant of any of the matters under APP 5.

Example 1 – All remedies provided

The complainant asks for an apology and information about whether their personal information will be disclosed to overseas recipients.

The respondent has provided an apology and the information on likely overseas disclosures.

The delegate can find that the respondent has adequately dealt with the matter as the respondent has provided all the remedies requested by the complainant.

Example 2 – Some remedies provided

The complainant asks for an apology, a statement setting out the purposes for which the respondent collects personal information and \$50,000 for hurt feelings.

The respondent has provided an apology and the requested information, but declines to provide compensation.

The delegate reviews the file and finds no evidence as to any harm suffered by the complainant arising from the privacy breach. The delegate is able to find that the respondent has adequately dealt with the complaint as:

The respondent has adequately remedied the breach by providing the specific information the complainant wanted to obtain.

The respondent has provided a remedy as requested by the complainant, namely, an apology

Those remedies are fair and reasonable having regard to the nature of the breach, as they serve to provide an outcome that connects with the breach, and an acknowledgement of wrongdoing on the part of the respondent.

There is no injustice to the complainant and the respondent not providing compensation, as the complainant has not particularised or evidenced the reason for seeking compensation. Additionally, it is difficult to see how a failure to provide notice of the matters under APP 5 could cause hurt or suffering of an extent warranting compensation.

Example 3 – Some remedies provided

The complainant asks for a statement setting out a full APP 5 statement and \$3,000 for psychological damage. In their application form, they say that they are a refugee applicant, whose personal information was the subject of an unauthorised disclosure by the respondent in the past and that they have seen a counsellor for trauma-related to disclosures of their personal information to their home country. Upon discovering their personal information was collected

without their knowledge, they immediately panicked as they did not know whether the personal information had been sent to their home country.

The respondent has provided the requested information, but declines to provide compensation.

The delegate cannot find that the respondent is adequately dealing with the matter as:

While the provision of the APP five statement goes part way towards addressing the breach, all that remedies is the fact that the complainant was deprived of in a PP five statement at an earlier time. The provision of this information now does not remedy the psychological damage claimed by the complainant. The delegate cannot be satisfied that the remedies are fair and reasonable in all the circumstances. The delegate cannot decline the complaint as ADW and will need to consider another pathway, such as inquiries and potential investigation.

Example 4 – Different remedies provided

The complainant asks for the respondent to give them a visa to stay in Australia.

The respondent declines and instead provides the complainant with an APP 5 notice.

The delegate can find that the respondent has adequately dealt with the matter as:

The respondent has provided a remedy. This remedy is fair and reasonable as it directly connects with the breach.

There is no injustice to the complainant in not providing the requested remedy, as the grant of a visa does not connect with the breach.

Example 5 – Different remedies provided

The complainant asks for \$10,000 compensation and does not provide any particulars.

The respondent offers to give the complainant access to certain services while in immigration detention.

The delegate cannot be satisfied that the remedy connects with the privacy breach and will need consider another pathway.

‘Not warranted’ decline

3.22 The ‘not warranted’ decline power can be exercised where the delegate is satisfied that investigation is not warranted having regard to all the circumstances.

3.23 In deciding whether investigation, or further investigation is not warranted, the Commissioner considers the following circumstances:

- 1) whether investigation would be a productive use of powers
- 2) whether investigation would be an efficient use of powers.

Productive use of power

In considering whether an investigation is warranted, it is relevant to consider whether investigation would be productive. This involves a consideration as to the likelihood of the investigation resulting in a beneficial outcome:

- 1) **Seriousness of the alleged breach** - In considering the level of seriousness the delegate is to consider the factors set out in the OAIC's Guide to Privacy Regulatory Action including:
 - Adverse consequences - Where the alleged breach would have adverse consequences for the complainant, this factor may suggest that the alleged breach is serious. Where the adverse consequences would not be significant, this may suggest that the alleged breach is less serious.
 - Sensitivity of information - Where the alleged breach involves personal information that is 'sensitive information' as defined by the Privacy Act, or involves personal information that is of a sensitive nature, this may suggest that the alleged breach is serious.
 - Complainant's circumstances - The particular circumstances of the complainant may suggest that the breach is serious. For example, where the alleged acts and practices were in relation to a complainant with vulnerabilities or disabilities, this circumstance may suggest that the alleged breach is serious.
 - Respondent's conduct - Where the respondent has engaged in conduct that is deliberate or reckless in relation to the alleged privacy breach, this may suggest that the breach is serious.
- 2) **Merits of the complaint** – This factor does not require a complete assessment as to whether there is breach. If satisfied there is no breach, the pathway should be 'no breach' decline. Rather, if it is not clear whether there has been breach and the respondent has raised an arguable case that the conduct was not a breach of the APPs, this factor may be suggestive that the issues are complex and investigation may not lead to an outcome without significant investment of resources.
- 3) **Likelihood of resolution** - This factor should consider the extent to which it appears settlement between the parties is likely. Past conduct can be predictive of future conduct. It will be relevant to consider whether the parties attended conciliation and the outcomes, and whether there have been settlement attempts on the papers which have been unsuccessful. The delegate also look at whether the parties have disparate views on what would resolve the case.
- 4) **Likelihood of better outcome** - This factor should consider what the respondent has offered and what the complainant seeks by way of remedies and should attempt to determine whether investigation is likely to result in the complainant obtaining the outstanding remedies.

Efficient use of power

In considering whether investigation or further investigation is an efficient use of powers, the delegate should consider the resources invested to date and the resources required to take the matter further.

- 1) The delegate should set out the resources used to date, including the work done by early resolution, and whether matter was conciliated. It should also set out the amount of material provided by the parties.
- 2) The delegate should set out the resources required to investigate the case and what would be required if the matter is referred for determination.

Balancing the factors

The delegate will need to balance the factors by considering the seriousness of the alleged breach, the low likelihood of investigation resulting in a better outcome and these resource considerations, in all the circumstances, and reaching a view as to whether investigation is warranted.

The **ITD template** for Not Warranted declines provides sets out these factors to assist the decision maker.

Decision about whether to immediately decline

- 3.24 The investigator will need to make an early decision about whether to immediately decline. If the matter is not to be immediately declined, it moves to an information gathering pathway, whether by preliminary inquiries or investigation.

Information gathering

Information gathering strategy

- 3.25 Having assessed the case and made a decision it is not suitable for immediate decline, the investigator should have a good idea of the issues. The investigator may have views about whether the respondent has breached and/or whether the respondent is willing to offer remedies. These views will inform the investigator's strategy ahead of the information gathering stage.
- 3.26 The investigator should consider the extent to which it is necessary to obtain information to evidence breach in order to facilitate offers from the respondent. Sometimes in order to access the adequacy of the respondent's offers, it is necessary to determine the extent of the alleged breach. This is a matter for the investigator's judgement which develops with practice and experience.
- 3.27 As champions of the Privacy Act, and as regulators for good privacy practices, the investigators should begin with the presumption that their task is to determine whether the respondent has breached. Most parties have had a sufficient opportunity to attempt to settle the case before it comes to Investigations. It is not the role of the investigator to act as an intermediary, a conciliator or a negotiator between the respondent and complainant in an attempt to facilitate settlement between the two.

3.28 Rather, the investigator's role is to determine whether any offers made by the respondent are fair and reasonable having regard to what is known about the case. That means the offers either address the complainant's requested remedies, or if they don't, they are commensurate with the alleged breach.

3.29 Therefore, an investigator enters information gathering with various strategies towards finalisation:

- They gather evidence that proves the respondent breached. Once this evidence emerges, they can attempt to get the respondent to make additional offers.
- They gather evidence that proves the respondent did not breach. Once this evidence emerges, they can decline as no breach.

3.30 The possibilities the investigator prepares for in their information-gathering stage are:

Likely finding	How to identify	Likely finalisation outcome
No finding of breach – R is willing to provide remedies	R has actively engaged in the OAIC's processes and has been responsive to PIs. R made offers when dealing with the complaint and/or early in the OAIC's process. R's offers addressed C's requested remedies, in whole or in part.	ADW or not warranted decline The investigator's information-gathering may be reasonably simple. It could focus on whether the respondent is willing to make additional offers and whether the complainant is willing to accept the offers made. It may also clarify with the respondent what certain offers involve and place timeframes around compliance. The investigator should prepare for the event that on assessment the offers do not address all the alleged breaches and be ready to investigate to confirm no breach.
Breach – R is willing to provide remedies	An assessment of the case is suggestive of breach or it is not clear on the face of the material that R has complied. R has actively engaged in the OAIC's processes and has been responsive to PIs. R made offers when dealing with the	ADW or not warranted decline The investigator's information-gathering may be reasonably simple. It could focus on whether the respondent is willing to make additional offers and whether the complainant is willing to accept the offers made. It may also clarify with the respondent what certain offers involve and place timeframes around compliance.

complaint and/or early in the OAIC's process.

R's offers addressed C's requested remedies, in whole or in part.

Breach – R refuses to provide remedies	R may have not participated in the OAIC's process and may have been non-responsive to OAIC's PIs.	Determination
---	---	---------------

- 3.31 Complexities arise where there are breaches on some claims, but not others, and the respondent offers remedies that address some breaches but not others. In such cases, if wholistically, the offers appear fair and reasonable, the investigator may prepare for a NW decline.

Information gathering powers

- 3.32 In any information gathering activity, an investigator must know the power that they are using when they are gathering information for this purpose.

- 3.33 In order to manage a complaint under s 36, the delegate of the Commissioner have powers to:

- conduct preliminary inquiries under s 42(1)
- open an investigation under s 40(1)
- obtain information from make obtain information and make enquiries under s 43(1A)
- compel the production of information or documents under s 44.

- 3.34 While certain preconditions must exist before these powers can be exercised the following table sets out, generally, when the investigator should use each power:

Provision	Power	When to use
S 42(1)	Preliminary inquiries	<ul style="list-style-type: none"> - an investigation has not been opened - the case could be immediately finalised if certain information were known and - that information could likely be obtained through one set of questions to the parties.
S 40(1)	Open investigation	-Investigator has discussed the case with the director and:

- it is unlikely that one round of questions will enable the investigator to finalise the case or
- the parties have responded to the investigators preliminary enquiries and the investigator does not have enough information to finalise the case.

S 43(1A)	Request for information	-an investigation has been opened and - a s 44 notice is not being used
S 44	Notice to produce information or documents	- investigator has attempted to obtain information from the respondent or a third party, and they have declined, have been evasive in their responses or have ignored the request - the person has indicated they do not consider themselves capable of responding to the RFI unless they are required to do so by law.

Preliminary inquiries

- 3.35 The power to make preliminary inquiries under s 42(2) is a power to make inquiries of the respondent or a person in order to decide whether to investigate an act or practice or not.
- 3.36 By the time a case has come to investigations, it will have been through early resolution, to likely will have already conducted preliminary inquiries.
- 3.37 While the term ‘preliminary inquiries’ may be thought of as the power, it may also be used to describe a stage of the conduct of the complaint. Namely, a stage that occurs as a precursor to investigation.
- 3.38 At the time of receipt, and at continuing points during the conduct of the case, the investigator will need to consider whether the case is appropriate to continue to be dealt with by way of ‘preliminary inquiries’ or whether it is appropriate to open an investigation.
- 3.39 The director may include in the instructions recommendation about whether to open an investigation immediately or whether to continue with preliminary inquiries. By way of general instruction, preliminary inquiries should only be used by investigators where it looks likely that one round of questions is all that is required to achieve a final pathway for the matter. If it looks like there may need to be multiple rounds, the investigator should open an investigation.

Investigation

- 3.40 The power to open an investigation under s 40(1) is framed as a default power of the Commissioner (Commissioner ‘shall’ investigate) where the act or practice raised by the section 36 complaint ‘may be’ an interference with privacy. As already discussed, this power is subject to the decline powers - if the complaint is to be declined, there is no mandatory requirement open an investigation.
- 3.41 That said, by the time the matter comes to the Investigations team it may have been on foot for quite some time. The issues in the case are likely to be complex as the Early Resolution team will likely have already considered whether the complaint should be declined and concluded that it needs to be referred to the Investigations team.
- 3.42 The benefit of opening an investigation is that it puts the parties on notice that the case has moved to a more formal stage. It is also beneficial insofar as once an investigation is open, the investigator can consider issuing a s 44 notice and can refer for determination.
- 3.43 There are a number of steps required to open an investigation. If the investigator thinks that one round of questions is worth pursuing in order to make one last attempt at an early resolution of the case, they may do so. However, in most cases, the complaints referred to the Investigations team are unlikely to be resolved that simply and the resources required to open an investigation are usually worth undertaking sooner rather than later.
- 3.44 Before opening the investigation, the investigator must obtain director approval. This may be in the form of the director instructions, the investigator’s assessment or by email confirming that the investigator has discussed with the director.
- 3.45 The procedures to open an investigation are as follows:
- 1) Email the respondent under s 43(1) notifying them that the OAIC intends to investigate the complaint – template. This is an important step that must be done separately to the sending of the letter opening the investigation. This email does not need to be cleared by the director.

Example s 43(1) email

Subject: Privacy complaint about [respondent’s name] – CPXX/XXXXX – Investigation to be opened

Dear [name]

I refer to this privacy complaint made on XX/XX/XX. As advised on XX/XX/XX this matter has been referred to the Investigations team for assessment. Pursuant to s 43(1) of the *Privacy Act 1988* (Cth) I advise that the Office of the Australian Information Commissioner (OAIC) intends to open an investigation into this complaint.

Shortly, the OAIC will send you a letter outlining how the investigation will be conducted.

Regards

- 2) In all cases, check whether the respondent is or was contracted service provider to an agency under a Commonwealth contract. If they were, send the relevant Commonwealth agency a notice of investigation under s 43(1A) – template

Example s 43(1A) email

Subject: Privacy complaint about contracted service provider [respondent's name] – CPXX/XXXXX – Investigation to be opened

Attachment: CPXX/XXXXX.S 43(1A).doc

Dear [name]

I refer to this privacy complaint made on XX/XX/XX about [respondent's name]. Under s 43(1A) of the *Privacy Act 1988* (Cth) I am required to notify an agency that a contracted service provider of that agency is to be investigated. I advise that the Office of the Australian Information Commissioner (OAIC) intends to open an investigation into this complaint. Please see attached correspondence.

Regards

- 3) Email each party a letter opening the investigation under s 40(1) – template. This does not need to be cleared by the director unless the letter includes a request for information.

Example s 40(1) email

Subject: Privacy complaint about [respondent's name] – CPXX/XXXXX – Investigation opened

Attachment: CPXX/XXXXX.S 40(1).doc

Dear [name]

I refer to this privacy complaint made on XX/XX/XX. As advised on XX/XX/XX this matter for referred to the Investigations team for assessment. Pursuant to s 40(1) of the *Privacy Act 1988* (Cth) I advise that the Office of the Australian Information Commissioner (OAIC) has opened an investigation into this complaint. Please see attached correspondence, outlining how the investigation will be conducted.

Regards

- 4) Once an investigation is opened, all requests for information and documents, apart from those the subject of a s 44 notice, should refer to s 43(3) as the relevant power under which the information is requested.

Example RFI referring to s 43(3)

Subject: Privacy investigation about [respondent's name] – CPXX/XXXXX – Request for information due XX/XX/XX

Dear [name]

I refer to the investigation of this privacy complaint. Under s 43(3) of the *Privacy Act 1988* (Cth) I am requesting information from you. Please providing the information by XX/XX/XX

Request for information

[set out RFI].

Regards

Compelling the production of evidence

- 3.46 The power to compel the production of information and or documents under s 44 requires the following elements:
- 1) the investigator has reason to believe that the person the subject of the s 44 notice has the particular information or the particular document
 - 2) that document will that information will be relevant to the investigation.
- 3.47 There are formal requirements for a properly issued s 44 which are set out in the s 44 template. In order to complete the template, investigator will need to have clarification on the following:
- 1) the person to whom the s 44 template is addressed does in fact hold the informational document
 - 2) the investigator has already done a thorough investigator's assessment, correctly setting out the claims and correctly identifying the relevant APPs
 - 3) the information or documents clearly link to those claims and a PP's.
- 3.48 The s 44 is to be cleared by the director. In complex or sensitive cases, the director may seek Asst Commissioner clearance.
- 3.49 The benefit of the s 44 is that it can be used to compel an unresponsive respondent to provide information that they were not otherwise provide. It may also be used for third parties that require legal compulsion in order to release information.
- 3.50 The challenges of using a s 44 is that they are resource intensive, and in addition to ensuring all formal requirements are met, they require carefully crafted information in questions to ensure they are legally sound. There are special confidentiality obligations that attached information produced under s 44. All information produced in response to a s 44 is to be clearly marked on resolve.

Information gathering skills

3.51 The **guide to conducting investigations** will assist the investigator in drafting RFIs.

Part 4: Decision making

Types of decisions

4.10 As set out earlier, the finalisation outcomes will either be withdrawn, declined, or determined.

Withdrawal

- 4.11 It is rare for a complainant to withdraw their complaint. Examples where they might do so include where they have negotiated a settlement with the respondent and as part of that settlement, they are required to withdraw.
- 4.12 Where a complainant withdraws their complaint, the OAIC must not investigate. A complainant will need to indicate their intention to withdraw using clear and unambiguous language, and will need to do so in writing.
- 4.13 If there is any doubt the complainant withdraws the complaint, the investigator must request confirmation from the complainant in writing.
- 4.14 Unless the complainant does so confirm, the investigator is to continue progressing the case. Where the complainant is non-responsive, the investigator should consider declining under s 41(1)(db), rather than withdrawing the complaint.

Decline

- 4.15 Decline is the most frequently used finalisation outcome for the investigations team. As set out earlier, the most common decline powers for the investigations team are no-breach decline, ADW decline and not warranted decline.
- 4.16 There are a number of other decline powers which are set out in detail in the declines guide.

Determination

- 4.17 Determination is a finalisation pathway where the case cannot be declined or otherwise finalised. The Determinations Handbook sets out the practices and procedures of the determinations team. The OAIC's guide to regulatory action sets out the factors to consider when deciding whether to refer a case for determination.

Decision-making principles

- 4.18 As administrative decision makers, the investigator needs to ensure that the final decision is legally sound and has been made affording procedural fairness to all parties whose rights may be adversely affected. This means that decision-makers must:
- apply the law correctly
 - make findings of fact based on evidence

- arrive at conclusions that are logical and rational
- only take into account relevant considerations
- do not have regard to irrelevant considerations
- bring an impartial and unbiased mind to the case
- give procedural fairness to individuals whose rights are likely to be adversely affected.

4.19 The **Guide to conducting privacy investigation** goes into detail how these principles apply to making decisions about s 36 privacy complaints.

4.20 The most important one for investigators to be mindful of in managing a s 36 privacy complaint is the procedural fairness principle.

Procedural fairness

4.21 The obligation of the decision-maker is to give procedural fairness to any party whose rights may be adversely affected by a decision. Effectively, this means parties will have an opportunity to comment on information that is credible, relevant, adverse and significant, and would be unknown to the party (**Relevant Information**) and on the critical issues.

4.22 The timing for providing procedural fairness is when it looks like the decision maker may make a decision that will adversely affect the rights of a party. For the complainant, this means when an investigator is considering making a decision to decline. For the respondent, this means when an investigator is considering making a decision to refer to Determinations.

4.23 Procedural fairness is given to a complainant is through a notice of intention to consider declining (**ITD**). Procedural fairness is given to a respondent is through an ‘investigator’s view’ (also known as a short preliminary view – ‘**short PV**’).

4.24 Procedural fairness usually requires the individual to be provided with the Relevant Information. The Relevant Information is to be provided with the ITD or the short PV, as appropriate. It will usually not be known whether information is Relevant Information until the investigator drafts their ITD or their short PV. Providing information as soon as it is received can be problematic as it lacks meaning and context, and may mislead the parties with respect to the relevant issues, which may increase the volume of irrelevant information on file.

4.25 All ITDs and short PVs are to be cleared by the director. Investigators must not advise parties that they intend to provide an ITD or a short PV until the letter is cleared and the investigator is close to sending it.

4.26 A party is not to be advised that an ITD or a short PV has been sent in relation to another party as a general practice. This is because advising one party that an investigator has formed a view as to the merits of the other party, before the other party has had a chance to respond, is premature and does not service to move the case towards finalisation. The other party may provide submissions or information that change the investigator’s views about the case. Advising a respondent of their preliminary view that they intend to decline, or advising a complainant that they intend to find breach, may raise false expectations.

- 4.27 Investigators can use their discretion as to whether they should be advised on a case-by-case basis. It may be appropriate where, for example, a respondent has been non-responsive and the case is likely to be referred to determinations, and the complainant needs assurance that the OAIC is taking appropriate measures.

Drafting and sending the ITD

- 4.28 The purpose of the ITD is to provide procedural fairness to the complainant.
- 4.29 The ITD operates like a draft decision record, insofar as it will form the basis for the draft decision to decline (close letter) once any additional material provided in response to the ITD is considered. The ITD is not a formal administrative decision – the delegate has not yet decided to exercise their discretion to decline, and it remains open to them to decide to not make a decline decision.
- 4.30 The ITD sets out the delegate’s preliminary findings, reasons and the decline power/s they intend to exercise.
- 4.31 The ITD also describes the information the delegate has taken into consideration and annexes any information not previously seen by the complainant. This prompts the complainant to state whether we are missing any documents they have provided. This will provide a level of assurance that the ultimate decline decision considers all relevant material.
- 4.32 There are a number of decline templates on Resolve. Specifically relevant to the Investigations team are the decline templates for ADW declines and NW declines.
- 4.33 The ITD will be cleared by the Director. Once cleared, the ITD is to be sent to the complainant and they will be given 2 weeks to respond.

Drafting and sending the short PV

- 4.34 The purpose of the short PV is to provide procedural fairness to the respondent. Additionally, it may operate as an informal mechanism to alert the respondent to where the case might be headed and to prompt them to take action if they wish to obtain a different outcome.
- 4.35 The short PV should be referred to as the ‘Investigator’s view’ to the parties as this will avoid confusion in the event the matter is referred to determinations and a formal preliminary view is sent.
- 4.36 The short PV is usually email (4-5 paragraphs) which sets out the gist of why the investigator considers they are not satisfied the respondent has complied with a particular aspect of the privacy act.
- 4.37 In some cases, the short PV may need to be produced in letter form, particularly if it is necessary to extract information the respondent has provided and the reasons are lengthy. **Appendix A** sets out an example of a short PV in letter form.
- 4.38 The short PV sets out the complainant’s claims, with a particular focus on the claim in relation to which the investigator thinks the respondent may have breached. The short PV tells the respondent the reason the investigator is dissatisfied, including the gaps in the information that

lead them to this view. In some cases, it may be appropriate to suggest the type of information that the decision-maker is seeking or to include specific RFIs in the short PV.

- 4.39 The short PV sets out the potential benefits for the respondent in providing a response, including the potential for the case to be declined, as well as potential consequences of a failure to provide additional information, namely, referral to the Determinations team.

Example s 40(1) email

- 4.40 An example of a short PV is follows:

Dear [name]

I refer to this privacy complaint. The purpose of my email is to advise you of my view that the respondent may not have complied with APP 6 and to invite your comment on any further information you wish to provide. If you wish to provide information, please do so by XX/XX/XX.

Complaint

As advised previously, the complainant complains that the respondent collected their personal information for the purposes of the respondent managing their health. The information before me (in particular, the respondent's email of xx/xx/xx) leads me to view that it was disclosed to the purposes of direct marketing.

My view

APP 6 provides, in summary, that an APP entity must not disclose personal information for secondary purposes subject to certain exceptions. On my review of the material, none of these exceptions apply. In particular, I note the complainant denies having consented to disclosures of their personal information for secondary purposes.

Invitation to provide information

You are invited to provide information in response to my view. In particular, as you have referred to a consent form you say the complainant completed enabling your disclosure, you may wish to provide this consent form. You may also wish to make any offers you are willing to provide the complainant. As advised previously, the complainant is seeking:

- \$5000 compensation
- a written apology
- changes to your procedures.

Next steps

Please note that the information you provide will inform my next steps. Depending on the information you provide, I may:

- find that the respondent has not breached APP 6 and decline to investigate further
- find that the respondent, may making fair and reasonable offers to resolve the matter, is adequately dealing with the complaint, and decline to investigate further or

- find that the respondent has interfered with the complainant's privacy and refer the matter for consideration of determination.

Determinations are published decisions made by the Commissioner about whether the respondent has interfered with the complainant's privacy and may include declarations requiring the respondent to do certain things. You can find published determinations on our website: [Privacy determinations - Home \(oaic.gov.au\)](https://www.oaic.gov.au/privacy/determinations) and on AustLII: [Australian Information Commissioner \(austlii.edu.au\)](https://www.austlii.edu.au/au/other/oaic/decisions/)

Regards

Response to ITD

- 4.41 The investigator's duty upon receiving a response to an ITD is to give it genuine and careful consideration. The response may appraise the investigator of matters that they have misunderstood or aspects that need to be investigated further.
- 4.42 Even if the response does not change the investigators substantive the case, they may need to incorporate information in the response into the final decision in order to ensure that they are accurately representing facts and submissions. In doing so, the investigator shows that they have complied with the decision-making principle of having regard to all relevant information.

Decision record – 'Close' letter

- 4.43 The decision record - colloquially referred to as the 'close' letter - is the investigator's statement of findings and reasons. It is primarily the vehicle by which the OAIC explains to the complainant why the decision has been made in order to give them transparency, fairness and a sense of closure.
- 4.44 If the complainant seeks review, the OAIC will reproduce the close letter as the primary evidence of the decision, and the reasons for decision. It will be the document that the Court will scrutinise for jurisdictional error.
- 4.45 In all but a few cases, an ITD and the complainant's response to the ITD will precede the close letter. As such, there are two ways to draft the close letter:

Close drafting option	Advantages	Disadvantages	When to use
1. The close letter sets out the response of the complainant, adopts the findings of the ITD and explains why	<ul style="list-style-type: none"> - efficiency for the investigator - increased readability for the complainant, as it will avoid 	<ul style="list-style-type: none"> - clearance processes will take longer as the director will need to check the close against the ITD and may have difficulty assessing the soundness of the investigator's decision. - third parties will lack clarity - the fragmented nature of the 	<ul style="list-style-type: none"> - the complainant has not responded to an ITD - the complainant's response is off topic and does not address the issues in the ITD

the complainant's response does not alter those findings.	length and repetition of information.	<p>decision will mean that anyone reading it in isolation will have difficulty understanding the context of the case.</p> <p>- reasons may come across as cursory and disjointed, and nuanced aspects of the case may be lost. This may create risk that a complainant or a review body may perceive that the decision-maker has not given genuine and careful consideration to the complainant's response.</p>	- the complaint only raises one or two claims and the issues are simple.
2.The close letter replicates the information in the ITD with additional drafting, and changes to the original drafting to reflect the complainant's response.	<p>- faster director clearance the letter, particularly if the investigator tracks their changes to the ITD content.</p> <p>- increased readability for any third party, including review bodies, as it provides one complete decision record</p> <p>- reduced risk that the investigator has misunderstood the response or failed to address all</p>	<p>- additional work for the investigator</p> <p>- may be a lengthy decision for the complainant.</p>	<p>- the complainant has provided extensive responses to the ITD.</p> <p>- the investigator needs to address the submissions of the complainant in their response by referring to what was discussed in the ITD.</p> <p>- the case is likely to be the subject of review.</p>

relevant
issues.

Examples of the two alternate drafting methods are set out at **Appendix X**.

Determinations

- 4.46 Where decline is not appropriate, the investigator will refer the matter to the Determinations team for consideration as to whether to recommend that the Commissioner makes a determination in relation to the complaint.
- 4.47 Decision about whether to make a determination is informed by the matters set out under the **OAIC's Guide to Privacy Regulatory Action** and the **Privacy Regulatory Action Policy**. Broadly, the most frequently referenced principles are:
- it appears there is a prima facie interference with privacy
 - there is evidence to establish an interference with privacy on the balance of probabilities
 - the respondent has not cooperated with the Commissioner's inquiries or investigation, and the Commissioner believes that it is necessary to make formal declarations that the respondent must take certain steps to address the interference with privacy
 - there is a disagreement between the Commissioner and the respondent about whether an interference with privacy has occurred, and the determination would allow that question to be resolved
 - there is a public interest in the Commissioner making a declaration setting out their reasons for finding that an interference with privacy has occurred, and the appropriate response by the respondent
 - there is educative value in determining the matter, including the deterrent or precedential value, or potential to clarify or test the law
 - seriousness of the claimed conduct, including number of persons potentially affected; whether the matter involves sensitive information or other personal information of a sensitive nature; whether disadvantaged or vulnerable groups affected by the conduct; whether the conduct was deliberate or reckless; seniority and experience of person responsible for the conduct.

Part 5: Referring a matter to the Determinations team

- 5.10 In order for the Commissioner to issue a determination under s 52, 3 elements are required:
- the investigation of the complaint, or of the act or practice if the Commissioner initiated the investigation, is complete
 - the Commissioner decides to exercise her discretion to make a determination

- the Commissioner decides upon the content of the determination that she will make.
- 5.11 On handover, the Determinations team needs to check whether the matter is suitable for determination. This will involve checking that:
- the investigation was conducted lawfully
 - there is enough evidence to make findings about whether the respondent has breached or not
 - there is enough evidence to make declarations addressing the requested remedies of the complainant.
- 5.12 As such, the investigator needs to provide the Determinations Team with handover that are sufficient to allow the determinations officers to conduct these tasks.
- 5.13 The handover documents will vary depending on the complexity of the case but generally include:
- summary of findings, evidence, reasons, and recommendations
 - summary of investigation process
 - evidentiary documents prepared in accordance with **Document Naming Conventions - [D2020/000150](#)** and **Index - [D2020/010712](#)**
 - Chronology - [D2020/010713](#).
- 5.14 Where the investigator considers a finding of breach likely, it is generally preferable that the investigator has already sent a short PV to the respondent. If a short PV has been sent, this must be clearly set out in the handover documents.
- 5.15 The handover information may be set out in the Investigation Plan or an email, or a combination. It is up to the Investigator to ensure the right level of detail is provided to the Determinations team. An example handover email is:

Example determinations handover email

Dear [Director Determinations]

I am referring this privacy complaint to the Determinations team for consideration.

Complaint

The complainant (made 1 January 2021) raises the following acts and practices that can be summarised as:

1. Claim 1 – the respondent disclosed their sensitive information (health information) to their employer without their consent. This claim raises a breach of APP 6.
2. Claim 2 - the respondent failed to notify them of the collection of their personal information. This claim raises a breach of APP 5.

3. Claim 3 - the respondent left their file unattended in the waiting room and another patient located it. This claim raises a breach of APP 11.
4. Claim 4 - the respondent's records incorrectly refer to the complainant's diagnosis as 'BPD' in circumstances where they say they did not have 'BPD' but had bipolar. This claim raises a breach of APP 10.

Damages claim:

The complainant claims to have experienced loss and damage as they had a mental health breakdown after they found out the personal information was disclosed to their employer. They have provided statements from their counsellor and treating psychiatrist evidencing their attendance soon after these events and evidencing exacerbation of the pre-existing mental health condition (see *C11-C12). They say that the events left them unable to work, however, have not provided evidence of this, despite being invited to do so.

Remedies:

The complainant seeks compensation in the amount of \$50,000 and an apology from the respondent's CEO.

Investigation plan

An investigation was opened on 2 January 2022. The investigation plan sets out detailed background to the complaint as well as the procedural history of the complaint. The chronology and index of documents are also set out on the investigation plan/ I attach the chronology and index of documents separately to this email.

Short PV sent to respondent

I sent a short PV to on 10 January 2022 (*O3). Essentially, I informed the respondent of my view that I was not satisfied the respondent had complied with APP 11 in respect of Claim 3.

I did not express a view as to whether there was compliance with APP 6, APP 10 or APP 11 in respect of the remaining claims. For the reasons set out on the Investigation plan, I am of the view the respondent has not breached in respect of these claims.

The respondent denied having breached APP 11, however offered an amount of \$500 and an apology from the reception staff who left the file unattended (R8). I have assessed these offers as not commensurate with the established breach and therefore not suitable for decline.

Documents

I confirm all documents are marked on Resolve consistent with the Document Conventions.

There are 15 substantive documents from the complainant (C1-C15), 8 substantive documents from the respondent (R1-R8) and 3 substantive documents of the OAIC (O1-O3).

Regards

- 5.16 The Determinations team is able to conduct simple investigations to fill in the gaps where it would be efficient for it to do so. The Determinations team may need to return a case to the investigator extensive investigations are required to make findings.
- 5.17 The Determinations team may need to consult the investigator if they have questions about the case. In some matters, they may need to seek the investigator's comment on a draft preliminary view or draft determination.
- 5.18 The Determinations team will notify the Investigations team of finalised determinations by circulating the determinations principles table when a new determination is published.

Part 6: Communicating with the parties

General

- 6.10 Once a s 36 privacy complaint has been referred to the Investigations team, the tone of written communications should err on the side of more formality rather than less formality.
- 6.11 Investigators should choose the most appropriate form of communications appropriate to the circumstances. In some cases, it might be more appropriate to telephone rather than write. Investigators must always check Resolve for an individual's preferred form of communication.
- 6.12 Investigators must check Resolve for the correct contact details of the parties and invite updated contact details on a continuing basis.

Introductory email

- 6.13 Investigators should send an introductory email as soon as they are allocated a case and have assessed the case as one they are able to take (that is, they have capacity and there are no conflicts of interest to declare).
- 6.14 This is a good time to check that the OAIC has the most up-to-date contact details for the parties on file.

Example introductory email

Subject: Privacy complaint about [respondent's name] – CPXX/XXXXXX – Referral to Investigations team for assessment

Dear [name]

I refer to this privacy complaint made on XX/XX/XX, which has been referred to the Investigations team. I will be assessing your case over the next few weeks and will be in contact with you soon.

Please be aware that we will continue to use the contact details you have provided the OAIC to communicate with you. If your contact details have changed, please let us know.

Regards

Updates

- 6.15 Investigators should keep parties updated on a regular basis. Investigators should use their discretion with respect to how much detail is appropriate. It is not necessary to tell parties about each and every information request made of the other party.
- 6.16 However, parties have rights to access information. It may be an effective strategy to keep some individuals abreast of the progress of the case than other individuals.

Holding email

- 6.17 Holding emails should be sent where matters may take longer than expected.

Example holding email

Subject: Privacy complaint about [respondent's name] – CPXX/XXXXXX – Update

Dear [name]

Thank you for your patience in awaiting my update in relation to your privacy complaint. I am continuing to assess your case and will be in contact with next steps by XX/XX/XX.

Regards

Change of investigator email

- 6.18 Where an investigator has taken carriage of a case from another investigator, they must check the file to see whether the parties have been advised of the change and, as appropriate, send an email to let them know.

Example change of investigator email

Subject: Privacy complaint about [respondent's name] – CPXX/XXXXXX – Change of investigator

Dear [name]

I refer to this privacy complaint. I advise that I have taken carriage of this case.

I will be in contact with next steps but in the meantime, please contact me if you have any queries about your case.

Regards

- 6.19 The **Investigator's Emails Guide** has further examples of how to communicate with the parties.

Extensions of time

- 6.20 Investigations should ideally progress in accordance with the timeframes as planned by the investigator. By the time a matter comes for investigation, the parties will ideally have already actively engaged in the issues, provided at least some information relevant to the complaint, and had a meaningful opportunity to conciliate.
- 6.21 There are circumstances where an investigator will need to consider whether to grant an extension of time (EOT) in investigations matters:
- where the respondent, complainant or a third party seeks an extension to respond to an RFI or a s 44 notice
 - a respondent seeks an extension to respond to a preliminary view (PV)
 - a complainant seeks an extension to respond to a decline.
- 6.22 Any extension of time will have the effect of delaying the finalisation of the case.
- 6.23 If one party fails to provide information within the required timeframe, this will delay the OAIC's consideration of the material and may lead to further requests for EOTs as a flow on effect. This has implications for the OAIC and the parties, and the administration of the case more generally. It makes it difficult for the OAIC, and the other party, to plan their work and allocate resources effectively.
- 6.24 Additionally, there is a broader public interest in ensuring the timely resolution of matters and administrative certainty, particularly where publish determinations provide educational value for the community.
- 6.25 On the other hand, the administration of the case also requires that the parties be treated fairly and equitably in all the circumstances. If the OAIC fails to provide a party with a reasonable time frame within which to comment on credible, relevant, adverse and significant issues that will influence the decision, it likely will be found to have denied procedural fairness. A decision on an EOT is itself an administrative decision capable of review.
- 6.26 In order to balance the obligation to ensure the timely resolution of matters with the obligation to treat parties fairly, it is important that officers turned their mind to relevant considerations in making an EOT decision and ensure that EOT decisions are made consistently.

Timeframes for responses

- 6.27 There are no statutory timeframes by which a s 36 privacy complaint, or an investigation, is to be progressed.
- 6.28 In order to process cases efficiently, the OAIC has decided on a general timeframe of two weeks for each party to respond to an RFI, a s 44 notice, short PV or decline. However, what is a reasonable timeframe to respond (and therefore, what is a fair opportunity to present a case) will vary from case to case, depending on a number of matters, including the complexity of the case and the volume of the documents to be considered.
- 6.29 The OAIC will set out indicative timeframes when sending a s 40(1) letter opening the investigation. The OAIC will also specify the relevant two-week period by which a party is to

respond in the correspondence inviting the response. It is then up to the party to request an EOT.

Principles for deciding EOTs

- 6.30 There is no statutory requirement in the Privacy Act relevant to the making of EOT decisions. An officer is to grant an EOT where it is reasonable in all the circumstances to do so. In deciding whether the grant of an EOT is reasonable in all the circumstances, officers should take into account the non-exhaustive principles from *Hunter Valley Development Pty Ltd v Cohen, Minister for Home Affairs and Environment* (1984) 3 FCR 344 (Hunter Valley Development) as relevant to the case:
- 1) **Explanation for the requested EOT** - where the requesting party has an acceptable reason for requesting the additional time, this will weigh in favour of granting the EOT. The acceptability of an explanation will also depend on whether the explanation connects with the amount of time requested.
 - 2) **Length of the requested EOT** - a short period of additional time requested may weigh in favour of granting an EOT, whereas an excessively lengthy period may weigh against.
 - 3) **Prejudice to the parties** - consider whether granting the additional time would have an adverse effect on the other party, including their ability to organise their case. Consider whether refusing the EOT would have an adverse effect on the requesting party, including the ability to put forward their best case.
 - 4) **Public considerations** - consider the nature of the complaint and the action on which findings of fact are to be made, and whether there is a public interest in granting the EOT, including the desirability in resolving matters expeditiously and use of public resources.
 - 5) **Merits of the substantive case** - where the nature of the case is such that it is unlikely that a response from the requesting party will have a substantive effect on the outcome, this may weigh in favour of refusing the EOT.
 - 6) **Consistency** - consider whether granting the EOT would ensure fairness as between the requesting party and other individuals in a similar position to the requesting party. This is about ensuring consistency across all cases beyond the particular case being considered.
- 6.31 There may be other relevant factors to consider in any given case. For example, where the OAIC has failed to advise parties of its expectations as to timeframes, or where the OAIC itself has delayed processing.
- 6.32 The EOT principles should not be approached as a checklist – some will be relevant, others will not. The principles should be considered holistically to determine whether on balance it is reasonable in all the circumstances to grant the extension of time.
- 6.33 EOTs must not be refused merely because a party has requested EOTs previously. Each EOT must be considered on its own merits. Only if the pattern or tendency revealed by previous EOTs made by the particular individual reasonably affects the factors set out above, should that history be taken into account.

Documenting a decision

- 6.34 As with all administrative decisions, the reasons should be documented. The extent of the documentation should be commensurate with the significance of the decision to be made. In most cases, a short decision setting out dot points as in the example will be sufficient. Examples are set out at the end of this document.

Advising the parties of EOT decisions

- 6.35 An EOT decision should be made in a timely manner and notified to the parties as soon as possible.
- 6.36 Where an EOT is being granted consistent with the request of the party (EOT grantee), it is not legally necessary to send reasons to the EOT grantee, unless these are requested. Short reasons should be provided to the requesting party where a decision is not in accordance with their request, that is, where an EOT is refused or where less time than requested is provided.
- 6.37 Even though it is not necessary to send reasons to an EOT grantee, in some cases, it may be beneficial to communicate with the EOT grantee the basis upon which they are allowed the additional time. This will put the EOT grantee on notice that the grant of an EOT is for a specific purpose, not to enable them to delay engaging in the case.
- 6.38 It is not necessary to provide reasons to the other party. In cases where the investigator has kept the other party updated with respect to request for information, and have an expectation that information will be received by particular date, it will be appropriate to let them know that an extension of time has been granted.

Example EOT grant email to EOT grantee

Subject: Privacy complaint about [respondent's name] – CPXX/XXXXXX – Your request for an extension of time to respond

Dear [name]

I refer to your request for an extension of time to respond to my request for information sent to you on XX/XX/XX. I have decided to grant the extension of time for the following reasons:

- the length of the additional time you request is short – only one week
- the reason for the additional time is acceptable – you have been affected by floods
- there will be no prejudice to the other party - considering the short amount of time you seek, and the nature of the case, I am satisfied that the other party will not be unfairly disadvantaged by granting the additional time.

A look forward to receiving your response by XX/XX/XX.

Regards

Example EOT refusal email EOT requestor

Subject: Privacy complaint about [respondent's name] – CPXX/XXXXXX – Your request for an extension of time to respond

Dear [name]

I refer to your request for an extension of time to respond to my request for information sent to you on XX/XX/XX. I have decided to refuse to extend time for the following reasons:

- the length of the additional time you request is excessive – 3 months
- the reason for the additional time is not acceptable – you state that you ‘have a lot of work on at the moment’ without any particulars.
- prejudice to the other party – the other party has been awaiting access to their medical records for 12 months and there is a strong need to bring this complaint to a conclusion.

It remains open for you to provide the information by XX/XX/XX. After this date, I will progress the case to the next stage.

Regards

Example EOT grant email to other party

Subject: Privacy complaint about [respondent's name] – CPXX/XXXXXX – Time extended

Dear [name]

I refer to this privacy complaint. On XX/XX/XX I updated you that I was expecting information from the respondent by XX/XX/XX. I have decided to grant them an extension of time to provide this information.

I will update you after I receive and consider the information.

Regards

Part 7: Appendices

Appendix A – Example of short PV letter

Our reference: CP XX/XXXXX

[name]

By email: [email]

Privacy complaint about Tyco Australia Group Pty Ltd t/a ADT Security

Dear [name]

I refer to the privacy complaint about [name] (respondent), made under s 36 of the *Privacy Act 1988* (Cth) (the Privacy Act) on 23 September 2020 by [name] (complainant).

On 29 September 2021 the Office of the Australian Information Commissioner (OAIC) opened an investigation under s 40 of the Privacy Act.

I am writing to advise that I have formed a preliminary view that the respondent has breached the Privacy Act, as well as to invite the respondent to provide further information by **17 May 2022**.

After that date I will make a decision about whether to:

- refer the matter for the Commissioner's determination under s 52 of the Privacy Act
- find the respondent has adequately dealt with the complaint and close the case under s 41(2)(a) of the Privacy Act, or
- find the respondent has not breached the Privacy Act and close the case under s 41(1)(a) of the Privacy Act.

Any response you provide will inform my decision.

The complaint

The Australian Privacy Principles (APPs) relevant to this complaint are set out in the attachment.

The complaint raises the following acts and practices of the respondent:

1. Recording a phone call without notification. I consider this to allege a breach of APP 5.
2. Soliciting credit card information from the complainant without verifying their identity. I consider this to allege a breach of APP 3.5 and APP 10.

Background

The complainant alleges that on 24 August 2020 they were telephoned by a staff member of the respondent and asked for their credit card details without verifying the complainant's identity. The complainant was concerned because they were not sure they were dealing with the respondent. The complainant did not provide their credit card details but instead called the respondent themselves and updated the details.

The complainant is concerned that the telephone call was recorded, given that the respondent records inbound telephone calls.

The OAIC invited the respondent to provide information about whether the telephone call on 24 August 2020 was recorded.

On 15 October 2021 the respondent advised:

ADT could not locate any recordings of the telephone call between ADT security and the complainant from 24 August 2020 and as such we are unable to verify that the telephone call was recorded.

The respondent has not suggested that it does not record outbound calls.

The respondent has referred to and relies on its 'standard customer service agreement' to put individuals on notice that calls may be recorded together with its privacy notice that it says was available on its website.

My view

APP 3.5

APP 3.5 requires that an APP entity collects personal information only by fair means. Under the APP Guidelines, this means that collection must not be 'unreasonably intrusive'.

In the absence of information from the respondent to the effect that the caller established the legitimacy of the telephone call to the complainant, including by identifying themselves and identifying the complainant, I am not satisfied that the respondent has complied with APP 3.5.

APP 10.1

APP 10.1 requires that an APP entity takes reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. In this case, I have concerns that the respondent, in failing to identify the individual receiving the call, may have placed the complainant's personal information at risk of inaccurate collection. It would seem a reasonable and simple step for a caller to ensure that they have used the correct contact details for an individual by checking and confirming their identity with recipient of the call.

Based on information before me, I am not satisfied that the respondent took reasonable steps to ensure the accuracy of the personal information it attempted to collect in the phone call of 24 August 2020.

APP 5

APP 5 requires the respondent to take reasonable steps to notify an individual of certain matters (APP 5 matters), or otherwise ensure that the individual is aware of APP 5 matters, at or before the time of collecting personal information about the individual. If it is not reasonably practicable to do so at or before the time of collection, the APP entity must do so as soon as practicable after collection.

The APP 5 matters which an APP entity must notify, or ensure awareness about, include the fact that the entity collects or has collected the information and the circumstances of that collection, if the individual may not be aware that the entity has collected the personal information.

In the circumstances of this case, it would seem reasonable for the respondent to have notified the complainant, or otherwise made the complainant aware, that the outbound call was being recorded and to direct them to a privacy notice setting out the remaining APP 5 matters. As such, I am not satisfied that the respondent has notified or otherwise ensured awareness of the fact that the call was being recorded, or of the other relevant APP 5 matters.

Without having seen the customer service agreement and without information as to the time at which it was provided to the complainant, I am not satisfied that the respondent has discharged its obligations under APP 5. Without having seen a copy of the privacy notice that was visible on its website at the time of the call, and without information to the effect that the individual was directed to this notice, I am not satisfied that the respondent has taken reasonable steps as required by APP 5.

Conclusion

For the above reasons, I have formed a preliminary view that the respondent has interfered with the complainant's privacy.

Invitation to provide further information

Before I make any decision in relation to breaches of the Privacy Act, the respondent is invited to provide further information by **17 May 2022**, including by:

- explaining how the circumstances of the attempted collection were not unreasonably intrusive
- providing a copy of the customer service agreement provided to the complainant
- explaining when the customer service agreement was provided to the complainant
- providing a copy of the privacy notice that was available on the respondent's website at the time of its call with the complainant and now the complainant was advised of this privacy notice.

Any information provided by the respondent will be taken into account in determining how to deal with the matter.

Adequately dealt with

Under s 41(2)(a) of the Privacy Act the Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made under s 36 of the Privacy Act, if the Commissioner is satisfied that the complainant has complained to the respondent about the act or practice and the respondent has dealt, or is dealing, adequately with the complaint.

Throughout the processing of this complaint, I have considered whether the respondent has or is adequately dealing with the complaint.

In the respondent's response of 15 October 2021 the respondent offered to provide a formal apology to the complainant and 'tailored data privacy training to all employees working with customer data ...'.

By emails sent to the respondent on 10 November 2021, 24 November 2021, 10 December 2021 and 21 January 2022, the OAIC attempted to make contact and follow-up with respect to the outcomes the respondent had offered. This included a request for information about the proposed training as follows:

Could you please confirm for me that this training will cover the specific grievance raised by the complainant. Namely, that your customer facing staff who make calls to individuals, where the calls are recorded, must:

- *ensure they advise individuals that the call is being recorded from the outset and seek the individual's consent to recording, before proceeding*
- *take reasonable steps to verify their identity as a genuine ADT employee prior to collecting sensitive information such as credit card details.*

On 24 January 2022, the respondent confirmed it had received the OAIC's correspondence. However, the respondent did not respond to the request for information at that time.

On 2 February 2022, the OAIC again requested a response as follows:

In order for me to find that ADT is adequately dealing with the complaint, it is relevant for me to consider whether ADT will follow through with any undertakings to provide remedial action to the complainant and whether those actions will address the complainant's grievance. To this end, I am seeking information from you about whether ADT is willing to:

1. *Provide a written apology from an appropriate person at ADT. If you are minded to provide this outcome, please advise by whom the apology will be made and the timeframe for its provision to the complainant.*
2. *Agree to provide training to ADT's officers to communicate with clients by phone. This training is to cover the specific grievance raised by the complainant. Namely, that your customer facing staff who make calls to individuals, where the calls are recorded, must:*
 - *ensure they advise individuals that the call is being recorded from the outset and seek the individual's consent to recording, before proceeding*
 - *take reasonable steps to verify their identity as a genuine ADT employee prior to collecting sensitive information such as credit card details.*

The respondent responded on 8 February 2022 as follows:

I am writing to confirm the below:

1. *Provide a written apology from an appropriate person at ADT. If you are minded to provide this outcome, please advise by whom the apology will be made and the timeframe for its provision to the complainant.*

- . *Please advise if the written apology is to be to the customer directly or via yourself.*
- 2.
- 3. *Agree to provide training to ADT's officers to communicate with clients by phone. This training is to cover the specific grievance raised by the complainant. Namely, that your customer facing staff who make calls to individuals, where the calls are recorded, must:*
 - . *ensure they advise individuals that the call is being recorded from the outset and seek the individual's consent to recording, before proceeding*
 - *I can confirm the customer service team has been made aware of this requirement,*
 - *we have also added instructions for the customer service representatives accessing the account to inform the customer their call will be recorded and to seek permission from the customer before proceeding with the call, this is to ensure there is no oversight.*
 - b. take reasonable steps to verify their identity as a genuine ADT employee prior to collecting sensitive information such as credit card details.*
- *the customer services team has been made aware of this requirement,*
- *as an added security measure; the account in question has been updated with instructions for the customer services team to announce to their name, department and reason for the call before proceeding with the call.*

On 9 February 2020 the OAIC confirmed by email to the respondent that the apology was to be sent by the respondent, by registered post, to an address specified in the email.

On 9 February 2022 the respondent advised it would send the apology within two working day and that the respondent would confirm when it had done so.

On 15 February 2022 the OAIC asked the respondent whether the apology had been posted. On 15 February the respondent advised the apology was posted on 11 February 2022.

On 15 February 2022 the complainant advised the OAIC that they had not received the apology letter. They also advised:

doesn't seem like training has been implemented yet as I contacted ADT to fix a payment issue and they didn't confirm any points of ID when I contacted them, once again this was with the credit control department, same department as the original issue.

On 29 March 2022 the OAIC emailed the respondent asking it to confirm the address to which the apology was sent and to provide a registered post tracking number.

The respondent has not responded.

Based on the above information, my preliminary view is that the respondent has not adequately dealt with the privacy complaint, including because I am not satisfied that the respondent has sent the apology letter and I am not satisfied that the respondent has conducted privacy training to address the particular grievances raised by the complainant.

Preliminary view regarding next steps

For the above reasons, my preliminary view is that I should refer this privacy complaint to the OAIC's Determinations team to consider making a determination under s 52 of the Privacy Act.

The respondent is also invited to provide information in response to my preliminary view regarding referral to the OAIC's Determinations team by **[date]**.

Yours sincerely

[signature]

[name]

Investigator

10 May 2022

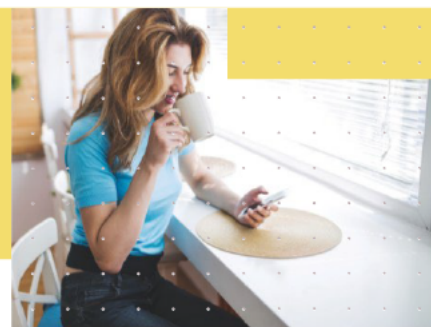


ER Team – Initial contact with parties

Phone call checklist

First contact with Complainant	
Introduction	Confirm allocation of matter Brief description of the OAIC's role (e.g. regulate Privacy Act & resolve complaints quickly)
Clarify understanding of complaint	Note summary of complaint info already provided Ask questions to clarify details of complaint Confirm what complainant is seeking to resolve
Provide info and manage expectations	Relevant legislation, including any threshold/jurisdiction issues How similar matters are usually resolved/finalised
Discuss complaint handling process	<p><i>Decline process:</i></p> <ol style="list-style-type: none">1. Is C satisfied with closing complaint as OAIC is not able to investigate? Confirm closure and whether C wants a quick email confirming this2. Does C want an opportunity to provide further information? Explain ITD process. <p><i>Early Resolution PI process:</i></p> <ul style="list-style-type: none">• Explain that we want to assist the parties in reaching an early resolution of their complaint. We have 21 days to achieve this with the parties.• 21 Days — If we're not able to reach resolution after 21 days, we will assess whether the matter is appropriate for allocation to an investigations officer. If this is the case, allocation may take up to 6-12 weeks before the matter can be reviewed for further inquiries and/or investigation.• Direct contact from R — While the matter awaits allocation, R may contact C directly to attempt resolution.• Info shared with R — <u>We will share C's information with R, this includes providing R with a copy of the complaint. Confirm that this may include C's contact details, so that R can contact C directly.</u>• Teleconferences (if appropriate) — We often use teleconferences as a tool to bring parties together and progress matters quickly. Would C be agreeable to this? If yes, please confirm suitable dates/times.• Correspondence — The ER process works by making phone contact with the parties. We will not be able to respond to correspondence or lengthy submissions. If anything is to be sent it should be emailed to early.resolution@oaic.gov.au
Confirm next steps with complainant	At the end of the 21 days, confirm the process is ending, and discuss next steps for the parties while the matter awaits allocation.

First contact with Respondent	
Introduction	<p>Advise receipt of a complaint</p> <p>Brief description of the OAIC's role (e.g. regulate Privacy Act & resolve complaints quickly)</p>
Clarify understanding of complaint	<p>Note summary of complaint info already provided</p> <p>Ask questions to clarify whether R is familiar with the complaint and obtain any relevant details</p>
Provide info and manage expectations	<p>Relevant legislation, including any threshold/jurisdiction issues</p> <p>How similar matters are usually resolved/finalised</p>
Discuss complaint handling process	<p>Referral to R:</p> <ol style="list-style-type: none"> 1. If we are making phone contact as part of the referral, please try to give a summary of what we think the issues are, and how the matter might be resolved. Encourage direct contact with C if appropriate. Highlight any issues of safety/harm or immediate impact. <p>Early Resolution PI process:</p> <ul style="list-style-type: none"> • Explain that we want to assist the parties in reaching an early resolution of their complaint. We have 21 days to achieve this with the parties. • 21 Days — If we're not able to reach resolution after 21 days, we will assess whether the matter is appropriate for allocation to an investigations officer. If this is the case, allocation may take up to 6-12 weeks before the matter can be reviewed for further inquiries and/or investigation. • Direct contact from R — While the matter awaits allocation, we will ask R to continue to attempt to resolve/respond if appropriate. • Info shared with C — <u>We will share R's information with C, this includes providing C with a copy of any written responses. Confirm whether this may include R's contact details, so that C can contact with R directly.</u> • Teleconferences (if appropriate) — We often use teleconferences as a tool to bring parties together and progress matters quickly. Would R be agreeable to this? If yes, please confirm suitable dates/times. <p>Correspondence — The ER process works by making phone contact with the parties. We will not be able to respond to correspondence or lengthy submissions. If anything is to be sent it should be emailed to early.resolution@oaic.gov.au</p>
Confirm next steps with respondent	<p>At the end of the 21 days, confirm the process is ending, and discuss next steps for the parties while the matter awaits allocation.</p>



30 November 2019

Privacy complaint assessment checklist

Risks to be raised immediately

When first reading the complaint, consider:

- ☐ Does the complaint identify or suggest safety issues, for example does the complainant indicate or threaten self-harm, make threats to another individual or party, or suggest they are in danger? If so **immediately** alert a Director.
- ☐ Does the complaint notify the OAIC of an act or practice that may cause serious harm or affects multiple individuals? If so **immediately** alert a Director.

Parties to the complaint

- ☐ Is the complainant properly identified, and are there any issues with the information on their client profile, for example multiple entries with the same information?
- ☐ Are there any related cases for the complainant? If so consider whether the matters need to be cross-referenced, if the new complaint raises the same/similar issues previously considered, and if correspondence on the new complaint should also be kept on the previous complaint/s.
- ☐ Is the complainant also complaining about the handling of someone else's personal information?
- ☐ Ensure any representatives are clearly identified and have authority to act. Be mindful of complaints made on behalf of children. Authority forms are available on our website: <https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us/>
- ☐ Is the respondent properly identified in relation to what the complainant has described (for example is the complaint really about a credit provider not the credit reporting body), and if the industry sector in the respondent client entry has been properly identified. If relevant, check that the proper respondent contact is identified.
- ☐ Consider if a second complaint needs to be created, for example as the complainant is also complaining about another individual such as a family member's information, or are they making complaints about additional respondents? If yes send an email to the Enquiries Team to register a new case (see Attachment A)

Jurisdiction, threshold and exemptions

Do we have jurisdiction?	Threshold Issues	Exemptions
<input type="checkbox"/> Australian Privacy Principles (APPs)	<input type="checkbox"/> Complaint to the OAIC?	<input type="checkbox"/> Employee records exemption
<input type="checkbox"/> Part IIIA (credit reporting)	<input type="checkbox"/> Complainant's personal information?	<input type="checkbox"/> Small business organisation (SBO) - Check whether R has opted in to coverage under the Act (within client record)
<input type="checkbox"/> Failure to notify under NDB Scheme	<input type="checkbox"/> Personal information in a record?	
<input type="checkbox"/> National Privacy Principles (NPPs)	<input type="checkbox"/> Complainant aware for less than 12 months?	<input type="checkbox"/> Political act or practice of a member of parliament
<input type="checkbox"/> Information Privacy Principles (IPPs)	<input type="checkbox"/> Complained to the respondent?	<input type="checkbox"/> In the course of journalism
<input type="checkbox"/> ACT Territory Privacy Principles (TPPs)	<input type="checkbox"/> Respondent had an adequate opportunity to respond?	<input type="checkbox"/> Royal Commissions
<input type="checkbox"/> My Health Records (formerly PCEHR)	<input type="checkbox"/> Rogue employee?	<input type="checkbox"/> Judicial decisions
<input type="checkbox"/> Tax File Numbers (TFNs)	<input type="checkbox"/> Spam Act? DNCR Act?	<input type="checkbox"/> AHPRA
<input type="checkbox"/> Spent Convictions	<input type="checkbox"/> Related body corporate?	<input type="checkbox"/> Intelligence agency such as ASIO
<input type="checkbox"/> Contracted service providers (CSP) to a Cth agency	<input type="checkbox"/> Health service provider?	<input type="checkbox"/> State or Territory authority, or Contracted Service Provider to one
<input type="checkbox"/> Individual Healthcare Identifiers (IHIs)	<input type="checkbox"/> Extra-territorial application of Privacy Act?	<input type="checkbox"/> Exempt from FOI 7(1)(a)(i)
<input type="checkbox"/> Data-matching	<input type="checkbox"/> Consumer credit or commercial credit?	
<input type="checkbox"/> Personal Property Securities register	<input type="checkbox"/> Trading in personal information?	
<input type="checkbox"/> Approved codes such as the APS Privacy Code	<input type="checkbox"/> Complaint about an individual?	
<input type="checkbox"/> Unique Student Identifiers (USIs)	<input type="checkbox"/> In a record?	

Related matters

- ☐ Does this relate to a current/previous DBN or CII? If so reference in the assessment, and consider whether we need to notify the Directors of the DBN or CII Team and seek their advice.
- ☐ Does this relate to matters that have had media coverage? If so alert a Director who will consider whether the Executive need to be made aware of the matter.
- ☐ Do we need to consult with another team, as the matter raises issues they may be considering? For example, if the matter involves biometric information the Assessments Team in R&S should be notified.
- ☐ Does the matter relate to broader policy issues the OAIC is currently considering, and has commented publicly about?
- ☐ Does the matter relate to the *Freedom of Information Act 1982* (Cth) (FOI Act), for example to an agency's disclosure of personal information under APP 6.2(b) on the basis the disclosure is permitted by the FOI Act, or its decision to refuse access under APP 12.2 on the basis it is required or authorised to refuse access under the FOI Act? If so, discuss with the Director of FOI Early Resolution as to how the matter will be managed – it may be more appropriate for the FOI Team to manage if the application of the FOI Act is to be considered.

Identification of significant or systemic issues

- ☐ Is the Respondent a Minister?
- ☐ Does the complaint include allegations about an agency head, or the equivalent for a large multinational organisation?
- ☐ Does the matter relate to ongoing public debate or highly publicised investigations, or has it attracted media interest?
- ☐ Whether novel issues raised or whether it can be a lead case to address systemic issues?
- ☐ Does it appear there is a pattern of recurring complaints?
- ☐ Does the matter raise concerns about the OAIC's approach to an issue?
- ☐ Are there concerns about an EDR's analysis of privacy issues?

These types of considerations should be noted in the assessment action on resolve, and the Director should discuss with the Assistant Commissioner DR in the first instance. The Director and AC DR may notify the Executive of these issues.

Case fields to be completed

- ☐ EDR used, if yes which one?
- ☐ MOU field, does one apply?
- ☐ Referral source, has the complaint been referred to us from somewhere else?
- ☐ Code flag, does a Code apply?
- ☐ Summary field, ensure you are using key words to capture the issues. Eg, data matching, porting issue, health records, identity theft, fraud, payment default etc.

Writing the assessment

Please be aware of the tone of assessments, and how they set matters on a particular path.

Ensure the assessment:

- articulates the privacy issue
- provides relevant background on what the complainant says occurred

- identifies the outcome the complainant has said they are seeking if this is something that needs discussion
- outlines the OAIC's view on the particular privacy issue (or if appropriate, that there does not appear to be a privacy issue), what approach we intend to take
- clearly outlines the next steps for the case officer that is allocated the complaint
- highlights any risks or issues the officer needs to be aware of, and refers the case officer to relevant cross-references/related files
- clarifies whether the assessment has been confirmed with the Assistant Commissioner and whether the case officer needs to keep the Director informed of the progression of the matter.

See the following example of an assessment where the OAIC will make inquiries with the respondent:

C alleges R has inappropriately disclosed her personal information to a third party. C advises that R disclosed her PI when it....C has raised with R and it has advised...

To resolve her complaint, C is seeking...

Be mindful of the sensitive circumstances C has raised. Discuss with C that APP 6 permits the disclosure of PI in certain circumstances, and discuss Cs outcome and outcomes generally possible through OAIC complaint process. Explain ER process and aim to resolve within 4 weeks. Advise if not resolved or finalised at the end of 4 weeks, has to be referred to Investigations Team and we cannot provide a timeframe but can be several months.

See the following example of an assessment where the OAIC will decline the complaint up front:

C alleges R has inappropriately disclosed her personal information to a third party. C advises that R disclosed her PI when it....C has raised with R and it has advised...

To resolve her complaint, C is seeking...

R appears to have disclosed Cs for the primary purpose it collected the information, as per APP 6.1. 14 day decline under 41(1)(a) on this basis.

Decline powers

Please set out the reasons for the decline with reference to the relevant decline power, and if possible, the relevant APP or provision of the Act.

If a matter falls pre-March 2014 only use the decline powers available at the time of the alleged breach.

Note that if you decide to accept matters out of time (excepting basic credit matters) this should be approved by The Director before finalising the assessment.

Section 36

When it is clear from the outset that we do not have jurisdiction (eg. state government agency, not personal information in a record, etc) the matter is to be assessed as not meeting the requirements of a complaint under **section 36**.

You can use s 41(1)(a), but this is more appropriate for cases out of jurisdiction when we have conducted preliminary inquiries first (because we have already accepted the matter as a complaint). If in doubt, revert to use s 41(1)(a).

Has complainant complained to respondent?

Section 40(1A)

When the complainant has not complained to the respondent, we have discretion to decline under s 40(1A). The acknowledgement letter the Enquiries Team sends states that generally individuals need to complain to the respondent before the OAIC can investigate.

Considerations we may take into account are whether the individual has not complained to the respondent directly due to safety concerns. We should also be mindful of whether there has been a significant delay in the OAIC actioning the matter before exercising this decline power.

Section 41(2)(b)

Where less than 30 days have passed since the complainant complained to the respondent, or in circumstances where it is unclear whether the complainant has lodged an official complaint with the respondent, then it is open to us to decline under section 41(2)(b) on the basis that the respondent has not had an adequate opportunity to deal with the complaint.

This power may also be used when the respondent organisation is clearly dealing with the complaint through something like an internal inquiry and we are satisfied that this is necessary before we can investigate. If this scenario arises discuss with The Director.

Decline powers under section 41- how to apply at assessment stage

Most matters assessed for decline under section 41(1)(a) should allow the complainant 14 days to respond to our intention to decline their complaint, unless the complainant indicates that they do not need us to give them further time to consider the reasons for decline.

Section 41(1)(a) – not an interference with privacy

Broad decline power – there will be some matters where it is clear there is no breach on the papers. If there is any doubt, refer for PIs or if more appropriate, an investigation.

Section 41(1)(c) – complainant complained after 12 months has passed

As a rule we do not accept a complaint after 12 months has passed, unless the complainant was clearly actively pursuing the matter with the respondent or via an EDR, or there are exceptional circumstances. If you are inclined to allow a complaint, please have this checked by the Director or another manager prior to finalising the assessment.

We receive a range of credit matters relating to events that occurred over 12 months ago. Usually, the complainant will only have been recently notified, or we will be unable to discern when they became aware. As credit histories continue to impact on individuals, we tend to generally allow for initial PIs on credit complaints, rather than decline them as out of time at the assessment stage.

An individual's right to access is ongoing, however, the individual should have made a request for access within the last twelve months.

Section 41(1)(d) – lacking in substance

Primarily used when the details of the complaint cannot be made out, or where the allegations seem unsubstantiated. Consider whether more appropriate to make PIs with the complainant first to see if they are able to substantiate the complaint before declining.

Section 41(1)(da) investigation not warranted

This will depend on the circumstances of the matter and may refer to another decline power. For example, it may appear from the information provided that there is no interference with privacy, but we also consider an investigation is not warranted because the act or practice occurred over 12 months ago and the respondent appeared to have taken steps to try and resolve the matter with the individual at the time.

Section 41(1)(db) not responded to a request for information from the OAIC

Not to be used at assessment stage.

Section 41(1)(dc) being dealt with by a recognised EDR scheme

This should be used if an individual confirms they have lodged a complaint with an EDR scheme about the same issue. If it is not clear if the individual has lodged a complaint, the assessment can recommend questions about this as a basis for a possible decline.

Section 41(1)(dd) more effectively or appropriately dealt with by an EDR scheme

Where it is clear that complainant has not been to an EDR and the issues are squarely issues we can deal with, our usual process is to accept the complaint and do PIs. This decline may be more appropriate where the privacy issue is part of a broader issue the EDR can consider and the OAIC cannot, for example if a complainant considers the respondent has failed to ensure the accuracy of their personal information on their bills and utility account and they are also disputing the billing of their account.

Section 41(1)(e) – adequately dealt with under another law

This is to be used where a matter is being considered or a decision has been made under another piece of legislation that deals with the substance of the complaint to us. (eg. an access request where an FOI request is being considered, or a decision has been made under the *FOI Act*.)

Section 41(1)(f) – more appropriate remedy available under another law

For example, where the substance of the complaint is about a range of issues (where privacy is a small component of broader set of issues) and would be better dealt with under other legislation (eg a complaint about telecommunications issues better dealt with by the TIO under the Telecommunications Act, or contractual issues better dealt with under state Fair Trading legislation).

Section 41(2)(a) – respondent has adequately dealt with, or is adequately dealing with complaint

Primarily used where we have information about the steps a respondent has already taken that are consistent with the steps we would consider reasonable to resolve the matter

through our complaint process.

Attachment A

Dear Enquiries

Could you please register the below as a privacy complaint. The details are as follows:

- Complainant name:
- Respondent name:
- Date of receipt:
- How received:
- X-reference to case:
- Please **do/don't** send standard acknowledgement
- After registration, matter can be assigned to **Me/Intake** for assessment.

For further information

GPO Box 5218 Sydney NSW 2001 | **P** 1300 363 992 | **E** enquiries@oaic.gov.au

Or visit our website www.oaic.gov.au

The information provided in this resource is of a general nature. It is not a substitute for legal advice.