FOI & PRIVACY INFORMATION LAW UPDATE

No. 3 | 2021

Welcome to AGS's Information Law Update, bringing you the latest developments in FOI and Privacy law.

We are interested in making sure that these updates are helpful and relevant for APS staff and FOI and Privacy practitioners, and welcome your feedback. Please email the Information Law Team if you have suggestions for the types of content you would like covered in these updates. Information about how to subscribe/unsubscribe can be found below.

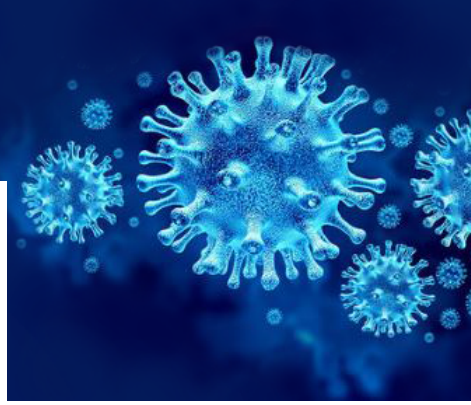
Contents

PRIVACY UPDATE

Privacy Awareness Week

This year Privacy Awareness Week (PAW) will be held from 3– 9 May. The theme is 'Make privacy a priority'. AGS has signed up as a PAW supporter. Signing up as a PAW supporter and distributing PAW materials is one way agencies and Privacy Champions can seek to meet their obligations under s 11(4) of the Australian Government Agencies Code to promote a culture of privacy that values and protects personal information.

To coincide with PAW, AGS is running a full day FOI and Privacy Forum. This forum is held once every 2 years and includes a mix of significant and contemporary topics in information law. For more information see here.



Privacy and COVID-19 vaccinations

The OAIC has released guidance for entities on privacy obligations in relation to COVID-19 vaccination information. The guidance emphasises that:

- the collection of vaccination information should only occur in very limited circumstances
- only the minimum amount of personal information that is reasonably necessary to maintain a safe workplace should be collected
- agencies must only collect vaccination information about employees with consent and where the collection is reasonably necessary for the agency's functions and activities, unless an exception applies.

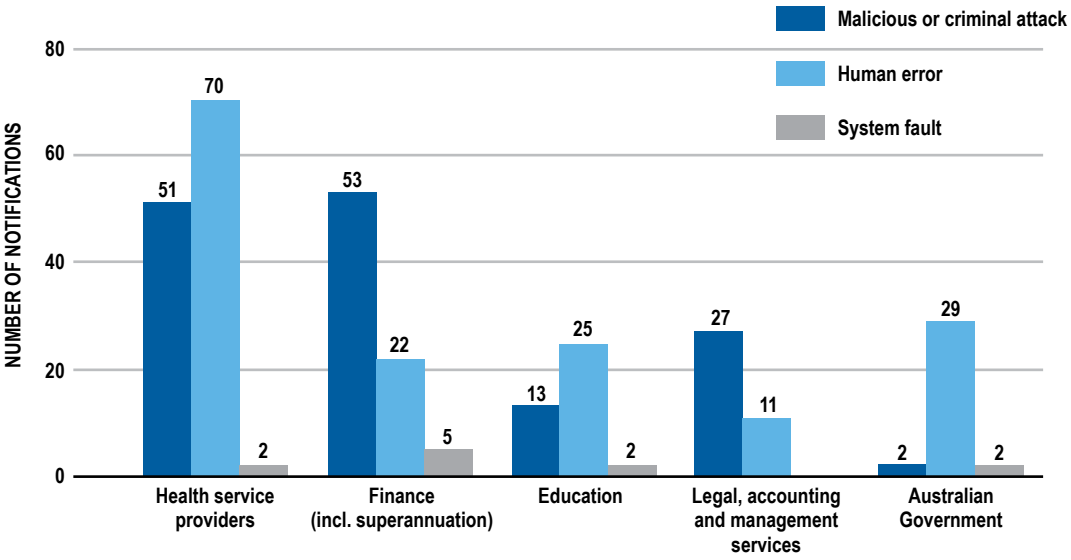
Depending on the circumstances, collection may be authorised under the *Workplace Health and Safety Act 2011* (see *AIT18 v Australian Information Commissioner* (2018) 267 FCR 93, which AGS has summarised here). If your agency does collect vaccination information, you must tell your staff the type of personal information collected and how it will be handled. Consent must be current and informed.

Notifiable Data Breach report

JULY–DECEMBER 2020

Australian government agencies featured in the NDB report for the first time as one of the top 5 industry sectors reporting data breaches to the OAIC, notifying 6% of all breaches (33 in total). Only 58% of notifications from the Australian government were made to the OAIC within 30 days of the entity becoming aware of the incident.

Source of data breaches – Top 5 industry sectors



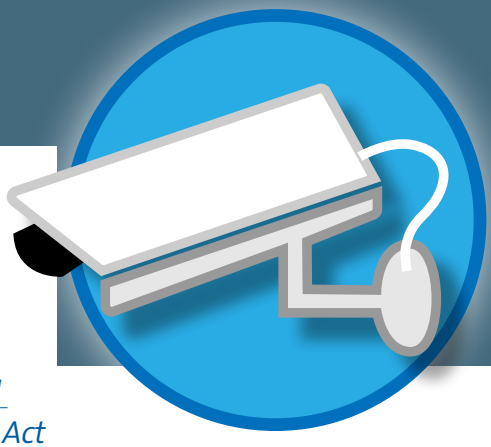
Human error was the cause of 29 out of 33 Australian government entity data breaches. The Commissioner was unable to draw a direct link between the breaches and changed business and information handling practices as a result of the Covid-19 pandemic.

Now that the scheme has been in operation for three years, the Commissioner has indicated raised expectations, including the need to be proactive in preventing data breaches, have systems to detect and respond to data breaches, and have timely responses and appropriate notifications. In one example, an entity was asked to update their notification to clarify that the 'unintended recipient' of personal information was in fact a malicious actor.

AGS has recently developed operating procedures and fact sheets for a number of agencies to assist staff to prevent and respond to some of the most common types of data breaches, drawing on our experience advising agencies as well as guidance prepared by OAIC and ACSC. We can assist you to develop a resource tailored for your agency.

Office of the Australian Information Commissioner website — www.oaic.gov.au

Review of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*



The *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* will amend the *Surveillance Devices Act 2004*, the *Crimes Act 1914* and associated legislation to introduce new law enforcement powers and warrants to enhance the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission's (ACIC's) ability to combat cyber-enabled serious and organised crime, including online child exploitation.

The Bill introduces:

- a data disruption warrant which enables AFP and the ACIC to access data on one or more computers and perform disruption activities for the purpose of frustrating the commission of criminal activity
- a network activity warrant to enable AFP and the ACIC to collect intelligence on criminal networks operating online
- an account takeover warrant to allow AFP and ACIC to take over a person's online account the purposes of gathering evidence of criminal activity
- minor amendments to the controlled operations regime, to ensure controlled operations can be conducted effectively in the online environment.

The Bill gives the Inspector-General of Intelligence and Security (IGIS) oversight of these powers. The Bill amends the *Privacy Act 1988* and the *Australian Information Commissioner Act 2010* to allow the transfer of complaints, and associated information, to the IGIS that are more appropriately dealt with by the IGIS.

The Bill review was referred to the Parliamentary Joint Committee on Intelligence and Security by the Hon Peter Dutton MP, Minister for Home Affairs on 8 December 2020.

Consumer Data Right expansion

The ACCC recently introduced the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* (the Amended Rules), with the consent of the Treasurer. This followed consultation with a broad range of stakeholders.

These changes are intended to expand the Consumer Data Right Rules (the Rules) to allow greater participation in the Consumer Data Right.

The amended rules:

- expand the type of consumers who can use Consumer Data Right (CDR)
- permit accredited data recipients (ADRs), with the consumer's informed consent, to collect CDR data from, and disclose CDR data to, other ADRs who are also providing goods or services to the consumer
- allow ADRs who collect CDR data with consent to also seek the consumer's consent to de-identify some or all of the data to be used for general research purposes (subject to limitations, including de-identification in accordance with rule 1.17 which sets out a specific de-identification process)

From 1 November 2021, the major banks will enable business consumers to share their data with ADRs.

These changes build on the amendments made to the Rules, which commenced on 2 October 2020, to allow accredited intermediaries to collect CDR data on behalf of an ADR.

Consultation regarding proposed Digital Identity legislation

Late last year the Digital Transformation Agency (DTA) sought community views on proposed legislation to support an expanded Digital Identity system in Australia. The current Digital Identity system is underpinned by the Trusted Digital Identity Framework (TDIF), which imposes strict privacy, security and administrative requirements on accredited entities.

In February 2020, the DTA published a summary of the feedback. Key themes included the need for effective governance of the Digital Identity system, an appropriate liability framework and the need for legislation to enshrine key privacy and consumer safeguards.

After considering the feedback, the DTA will engage in a second round of consultation and then commence development of the draft legislation. To find out more, go to www.digitalidentity.gov.au

Privacy Act Review

Over 150 submissions have been made to the Attorney-General's Department review of the Privacy Act. A discussion paper will be released during 2021 for further consultation. Submissions have been made by a broad range of government and non-government entities, and are available here.

OAIC Consultation on updating the Guide to securing personal information

The consultation period to provide submissions on the OAIC's proposed update to the Guide to securing personal information closed on 12 March 2021. Last updated in 2018, we expect that the updated Guide will reflect changing information handling practices, and the OAIC's experience regulating the notifiable data breaches scheme. Watch this space.

PRIVACY CASE STUDIES

▶ 'WP' and Secretary to the Department of Home Affairs (Privacy) [2021] AICmr 2 (11 January 2021) – AIC's first representative complaint determination

IPP 4 – data security failure (breach) – IPP 11 – unauthorised disclosure (breach)

Remedy: *Compensation awarded – manner in which the amount of compensation payable to class members is to be calculated – process for determining dispute regarding the entitlement of a class member to the payment*

On 10 February 2014, the respondent inadvertently published the personal information of 9258 individuals who were in migration detention at that time. The information was contained in a word document that had an excel spreadsheet embedded within it which included the names, gender, citizenship, date of birth, detention location and arrival details of the individuals. The respondent was notified about the data beach by a journalist some 8 days later, and removed the report. The respondent also identified that the report was available on Archive.org and wrote to that website seeking removal, which occurred 16 days after the initial publication.

A representative complaint was submitted to the OAIC. The class members sought a declaration that they were entitled to an apology, as well as compensation for economic and non-economic loss and aggravated damages.

An Own Motion Report dated 12 November 2014 concluded that the respondent failed to put in place reasonable security safeguards to protect the personal information that it held against loss, unauthorised access, use, modification or disclosure and against other misuse. It also found that the publication of the personal information of the listed individuals was an unauthorised disclosure.

Apology given: As an apology was previously given to the class, no determination was made requiring a further apology.

Change of protection visa status not within power: The Commissioner declined to make a declaration that the respondent must reconsider the rejected protection visa applications of class members, noting that protection claims are assessed through a separate administrative decision-making process under the *Migration Act 1958* (Cth), and the Commissioner did not have the power to reconsider decisions made under a separate statutory scheme.

Compensation for economic and non-economic loss: The Commissioner determined that the participating class members are to be paid compensation for economic and non-economic loss, and directed the respondent to assign a quantum of damages for each participating class member, with reference to a Table provided as an addendum to the determination. The Commissioner declared that if, after a preliminary assessment, the respondent and class member are in agreement, compensation is to be paid as resolution of the matter within a reasonable timeframe. The Commissioner set out a process for reassessment, including the

possibility of referring the matter for assessment by an expert, with the respondent to bear the costs for resolving cases where agreement is not reached.

The table at Addendum A to the determination sets out a system of categorising non-economic loss, with Category 1 being 'general anxiousness, trepidation, concern or embarrassment' resulting from the breach, with a quantum range of $500–$4000, up to Category 5 being for 'extreme loss or damage' from the breach, and indicating a quantum of $20,000 or more would be appropriate. The table provides useful guidance to ranges of compensation depending on the degree of non-economic loss.

▶ 'WQ' and Commissioner of Taxation (Privacy) [2021] AICmr 4 (11 February 2021)

APP 6 (no breach) — APP 10 (no breach) — APP 11 (no breach)

Remedy: *None*

The complainant was advised by an ATO officer to apply for a release from his tax debt instead of pursuing a payment plan. Nearly two months later, the ATO provided the complainant's personal information to a Mercantile Agent for debt collection. The complainant then received a letter of demand from the Mercantile Agent, and contacted the ATO regarding that letter on the same day. The ATO advised the complainant that it had not received any release application from him. The ATO processed the complainant's application for a release from his tax debt a day later.

The ATO denied it had interfered with the complainant's privacy and the disclosure to the Mercantile Agent was necessary for its debt collection activities.

While WQ alleged that automation of the referral process was a breach of APPs 6, 10 and 11, the Commissioner found that the requirements of these principles were met.

The Commissioner found that the ATO did not breach APP 6 in providing access to the complainant's entire taxation file, as the data file and general information related to the specific function of debt collection, being the primary purpose under APP 6. The Commissioner found that information used for the secondary purpose fell within exceptions in APP 6.2(a).

The Commissioner found that given the range of duties required of the Mercantile Agent's staff, the ATO took reasonable steps to ensure protection of the complainant's personal information and there was no breach APP 10 or 11.

▶ 'WL' and Secretary to the Department of Defence [2020] AICmr 69 (22 December 2020)

APP 3.1 (breach)

Remedy: *Declaration of interference with privacy – Apology.*

WL posted Australian Defence Force (ADF) equipment for sale on a website. Under the *Defence Force Discipline Act 1982* (DFD), unlawful sale of Commonwealth property is an offence.

Defence obtained details of the user from the website, which it matched with other data to identify WL as a former reservist. As Defence's activities extend only to investigating suspected unlawful activity by serving members and reservists, it referred the matter to Victoria Police.

WL claimed the collection, use and disclosure of their information breached APPs 3 and 6. WL also claimed that the sharing of information internally led to his details being posted on an unauthorised Facebook page in breach of APPs 6 and APP 11.

The Commissioner found that Defence interfered with WL's privacy by over-collecting their personal information. In addition to information that was reasonably necessary to collect, Defence had collected information from the website about WL's website feedback score, password, billing and user ID history. The Commissioner found collection was not reasonably necessary or directly related to the function to investigate service offences and a breach of APP 3.1.

The Commissioner found that the disclosure to Victoria Police, after Defence determined it no longer had jurisdiction to investigation the potential offence, occurred for a secondary purpose that a reasonable person would expect, which was authorised under APP 6.2(a). The Commissioner was not satisfied that the acts of individual members posting on the Facebook page could be attributed to the respondent.

The Commissioner made a declaration that Defence interfered with the privacy of WL and should make an apology. Damages were not considered appropriate as there was no evident connection between the additional information provided in the response and the complainant's emotional distress. The Commissioner found aggravated damages were unwarranted.

▶ 'WG' and AustralianSuper Pty Ltd (Privacy) [2020] AICmr 64 (16 December 2020)

APP 5, APP 6, APP 10, APP 11 (breach)

Remedy: Compensation awarded for non-economic loss — No aggravated damages

During November 2014, the complainant submitted a claim to the respondent for payment under income protection and total and permanent disablement insurance policies with the respondent. At different times during the assessment of the insurance claim, the complainant engaged the services of two different law firms (Law Firm 1 and Law Firm 2) to assist with their claim.

Prior to the date the respondent made a payment to the complainant in respect of the insurance claim, WG terminated the engagement of each of the law firms and notified the respondent that they had revoked authority for the firms to act. Despite the revocations, the respondent made contact with the firms regarding the insurance claim.

The complainant made a range of claims, including that the assessment of their claim was done by the administrator, not the insurer, and that this had not been made clear to them (claim 1), disclosure of their personal information to Law Firm 1 (claim 2) and Law

Firm 2 (claim 3) was unauthorised in circumstances where they had revoked authority, and disclosure to Law Firm 1 that they had received a payment (claim 4) was unauthorised.

The Acting Commissioner found that claims 1 and 4 were not substantiated. However, she was satisfied that claims 2 and 3 were substantiated, finding that:

- the respondent breached APP 6 when it disclosed the personal information of the complainant to the complainant's previous legal representatives after the complainant withdrew their consent for the respondent to do so
- the respondent breached APP 10 by failing to take reasonable steps to ensure that the complainant's previous authorisation to communicate with the law firms, was accurate and up-to-date,
- the information was disclosed in a way that amounted to a breach of APP 11 as there were additional reasonable steps the respondent could have taken in the circumstances to protect the information from an unauthorised disclosure.

The complainant considered the alleged breaches of the Privacy Act by the respondent were willful and caused a deterioration in the complainant's psychological health. The complainant sought compensation of $20,000 by way of damages for this alleged deterioration (damages claim).

Apology be provided: The Acting Commissioner declared that a written apology be provided by the respondent to the complainant within 7 days of the determination.

Compensation for non-economic loss: The Acting Commissioner was satisfied by evidence from the complainant's psychologist and mother that the complainant had experienced some pain and suffering arising from the privacy breaches of the respondent. The Commissioner considered that an amount of $4,500 was appropriate to compensate the complainant for non-economic loss but aggravated damages were not warranted.

Audit required: The Commissioner decided that an audit was required to ensure the respondent does not repeat the conduct underpinning the breaches of APP 10 and APP 11. Her declaration includes 6 steps and specific timeframes for an audit process for procedures and changes for updating changes to authorities to act.

▶ 'WC' and Chief of Defence Force (Privacy) [2020] AICmr 60 (27 November 2020)

Spent convictions

Remedy: *Declaration ADF engaged in unlawful conduct – non-economic loss: $6,000; reasonably incurred expenses: $4,850.*

This matter was the first determination made by the Commissioner in relation to spent convictions.

WC claimed that the Australian Defence Force (ADF) had breached s 85ZW(b)(ii) of the *Crimes Act 1914* by taking into account convictions that were 'spent' (s 85ZV(2)), or subject to a right of non-disclosure (s 85ZV(3)) in its decision to terminate his appointment.

While the Commissioner was not satisfied the convictions were spent, a right of non-disclosure existed under Queensland law. Although the ADF argued it considered only the conduct underlying the convictions in making its termination decision, the Commissioner found the ADF had taken into account the convictions.

The respondent argued that the exception in s 85ZZH(g) applied as the disclosure was for the purpose of 'assessing appointees or prospective appointees to a designated position'. The Commissioner did not accept the submission as she found no formal determination had been made designating the position for the purposes of the Crimes Act 1914, and the information was used to terminate WC's service, not assess suitability for appointment to, or removal from, the relevant position.

The Commissioner concluded that the ADF had breached s 85ZW(b)(ii).

The Commissioner did not make a declaration requiring the reappointment of WC as she was not satisfied the breach of s 85ZW(b)(ii) caused the termination decision.

The Commissioner made declarations that the ADF pay WC:

- $6,000 for non-economic loss as a result of harm caused by the breach (relevantly feelings of distress, anxiousness and upset)
- $4,850 for reasonable expenses, comprising the full amount of fees incurred to engage a lawyer to review documents and draft a submission in response to the Commissioner's preliminary view.

▶ Flight Centre Travel Group (Privacy) [2020] AICmr 57 (25 November 2020)

APP 1.2 (breach), APP 6.1 (breach), APP 11.1 (breach)

Remedy: *Declarations that the respondent had engaged in conduct interfering with privacy of approximately 6,918 individuals; that the respondent must not repeat that conduct; and that it would be inappropriate for further action to be taken.*

The respondent organised a 'design jam' to create new technologies for travel agents. The respondent provided participants with a dataset that mistakenly included credit card details and passport information of approximately 7,000 customers.

This is the first matter to be determined by the Commissioner arising from an investigation made on the Commissioner's own initiative under s 40(2) of the Privacy Act (with other determinations arising from complaints from affected individuals).

The Commissioner found that the respondent had unlawfully disclosed its customers' personal information to participants, having failed to retain effective control over that information. Notably, participants did not sign non-disclosure agreements and arrangements for the deletion of data post-event were inadequate.

The Commissioner found that the personal information had been disclosed for a purpose other than the primary purpose for which it had been collected (the provision of travel advice and services). The Commissioner did not accept the respondent's submission that it could infer customer consent to the disclosure from the mere provision of a privacy policy.

In any case, consent could not be obtained through the policy because it was insufficiently specific and bundled with other uses and disclosures.

The Commissioner found that the respondent had not taken reasonable steps to protect the information. While the respondent had reviewed samples of the data to check for sensitive information, that review had been insufficient and the dataset inadequately cleansed. Further, she did not accept the respondent's submission that the adequacy of its privacy safeguards was irrelevant as they did not cause the breach. The Commissioner found that the respondent should have implemented better training, compliance checks, assurance processes, and technical controls, and that the privacy protections in place, which should have been 'multi-layered and multi-faceted', fell short of the standard required.

The Commissioner found that the practices/procedures/systems the respondent had adopted to comply with the APPs were not reasonable in the circumstances.

The Commissioner made a declaration acknowledging the breach in view of factors including the seriousness of the incident and the specific and general educational, deterrent or precedential value in making a determination. However, she did not require the respondent to take further steps and noted the respondent's conduct after the breach in voluntarily notifying affected individuals, cooperating with the OAIC investigation, making payment of $68,500 to replace passports, and promptly improving its practices to mitigate against future breaches.

FOI UPDATE

Commissioner-initiated investigation into the Department of Home Affairs

On 29 January 2021, the Australian Information Commissioner published a Commissioner-investigated investigation report into the Department of Home Affairs' compliance with statutory processing requirements under the *Freedom of Information Act 1982* for non-personal information requests.

This is only the third such report by the Commissioner since s 69(2) of the FOI Act was inserted, giving the Information Commissioner the power to investigate an action taken by an

agency in the performance of functions, or exercise of powers under the FOI Act. This is the second investigation report by the Commissioner into the Department's processing of non-personal information requests.

The Commissioner's determination to undertake the investigation followed from her review of statistical evidence about delays in processing FOI requests for non-personal information, previous investigations, and the number and nature of FOI complaints and IC reviews made to the OAIC that highlighted the Department's failure to process FOI requests for non-personal information within the statutory processing period.

The Commissioner made 4 recommendations for the Department to improve its rate of compliance with the statutory processing period by:

1. appointing an Information Champion
2. preparing and implementing an operational manual for processing FOI requests for non-personal information
3. undertaking and completing FOI training for FOI section staff, FOI decision-makers and support staff, and making online FOI training available to all Departmental staff
4. undertaking an audit of the processing of FOI requests for non-personal information.

The Secretary's response to the Commissioner is published with the report. The Department accepted all recommendations and drew attention to the work already underway in the Department's continuous improvement program for FOI since October 2019 (when the OAIC opened the investigation). Of particular note was that:

- the Department finalised double the number of requests for non-personal information in 2019–20 than it did in 2018–19 (1789 compared to 870)
- the Department finalised double the number of requests for non-personal information between 1 July – 30 November 2020 compared with the same period in 2018–19, and had increased the rate finalised within statutory timeframes to 70% (a 30% increase).

Take away thoughts

The volume of requests for non-personal information the Department is dealing with far exceed those that most other agencies receive (combined with personal information requests the order of magnitude is even greater!). However, other agencies that have also experienced a surge in FOI requests (particularly complex and sensitive requests) may find the recommendations useful to boost their capacity to rise to manage this increased demand.

AGS regularly assists agencies with:

- developing and presenting FOI training materials and sessions, including those targeted for FOI decision-makers and staff providing support with searches and other processing tasks, and
- reviewing FOI processes and guidance material.

Recent updates to FOI Guidelines

On 9 February 2021, the Information Commissioner issued updates to the FOI Guidelines dealing with:

- charges for providing access (Part 4)
- review by the Information Commissioner (Part 10)
- complaints and investigations (Part 11).

Part 4: Charges

The changes to this part are a relatively minor clarification of the more significant revisions in June 2020. However, one aspect that is worth highlighting is described as a '[C]larification of the circumstances in which an applicant may dispute the preliminary assessment of the charge.'

The Guidelines now advise that:

> [4.57] The assessment notice must also inform applicants that they can still contest the preliminary costs assessment even if they have paid (an option that allows processing of the FOI request to continue while the charge is being contested).

Part 10: IC Review

While these are generally minor changes, practitioners may be interested to note that some clarification about the use of s 54W(b).

Section 54W(b) is the power for the Commissioner to decline to undertake a review if satisfied 'that the interests of the administration of the FOI Act make it desirable' that the AAT consider the IC reviewable decision. Agencies have reported an increase in the number of cases in which this discretion has been exercised, leading to more FOI reviews before the AAT.

The list of circumstances in which the Commissioner may decide that it is desirable for the AAT to consider the IC reviewable decision instead of the Commissioner continuing with the IC review has now been expanded to include:

- where there may be a perceived or actual conflict of interest in the Commissioner undertaking review, including where:
  - the FOI request under review was made to, or decided by, the Information Commissioner or their delegate
  - the FOI request or material at issue relates to specific functions exercised by the Information Commissioner under the Privacy Act
  - the applicant has active matters in other forums, including the AAT or Federal Court, and the Information Commissioner is the respondent
- where consideration by the AAT would further the objects of the FOI Act, particularly in relation to the performance and exercise of functions and powers given by the FOI Act to facilitate and promote public access to information, promptly and at the lowest reasonable cost (s 3(4)).

Part 11: Complaints and investigations

There are a number of changes to this part. Of particular note, is the addition of a list of factors the Commissioner will take into account when deciding whether to commence an investigation of an FOI complaint or at the Commissioner's own initiative:

- [11.8] When deciding whether to commence an investigation, the Information Commissioner will take into consideration:
  - the objects of the FOI Act
  - the risks and impact of non-compliance
  - whether the practice complained of is systemic
  - whether significant issues are raised
  - whether there has been non-compliance with statutory timeframes
  - the outcome sought.

FOI CASE STUDIES

▶ *Services Australia and 'WE' (Freedom of information)* [2020] AICmr 62 (14 December 2020)

VEXATIOUS APPLICANT DECLARATION (s 89K)

The Acting Australian Information Commissioner declared 'WE' a vexatious applicant under s 89K of the *Freedom of Information Act 1982* (FOI Act) on the basis that they repeatedly engaged in access actions that involved an abuse of process. The declaration prohibits 'WE' from making requests for access to documents for a period of 12 months to either Services Australia or the Office of the Australian Information Commissioner, or from seeking internal review during that time.

During an approximately two year period, 'WE' made 105 'access actions' to Services Australia. Significantly, 40 access requests were made after Services Australia notified 'WE' that it intended to apply for a declaration if 'WE' did not moderate their behavior and 11 access requests were made after the application for a vexatious applicant declaration was made to the Information Commissioner.

This is the only second vexatious applicant declaration to completely restrain an applicant from making access requests under the FOI Act for a specified period (see *Services Australia and 'RS' (Freedom of information)* [2020] AICmr 6). The decision is a reminder that the Information Commissioner, in finding that the discretion to make a declaration is enlivened by s 89L(1) of the FOI Act, may make a s 89K declaration in terms that are not specifically sought by the agency. In this case, Services Australia sought a declaration that would permit 'WE' to continue to make access applications, provided they obtained the permission of the Information Commissioner to do so. 'WE' had also agreed to the declaration being made in those terms, provided that Services Australia continued to process outstanding requests.

Significantly, the declaration will permit Services Australia not to process access requests and applications for internal review made prior to the declaration.

The Acting Commissioner found that the relevant abuse of process was that the access actions had unreasonably interfered with the operations of an agency (s 89L(4)(b)), including that Services Australia had spent over 418 hours processing the access requests. The Acting Commissioner also took into account that 'WE' had generally sought information falling into four categories and had refused the requests to be dealt with under administrative access. The Acting Commissioner declined to consider whether the access actions also involved harassing or intimidating an individual or an employee of an agency as alleged by Services Australia (s 89L(4)(a)) [62].

▶ *Paul Farrell and Department of Defence (Freedom of Information)* [2021] AICmr 3 (3 February 2021)

MANAGEMENT OF PERSONNEL (s 47E(c)) – CERTAIN OPERATIONS OF AGENCIES (s 47E(d)) – PERSONAL PRIVACY (s 47F) – PUBLIC INTEREST TEST (s 11A(5))

The applicant requested access to a report detailing the outcomes of Court Martial and Defence Force Magistrate proceedings (military tribunals) between September 2014 and 18 September 2017.

Disclosure would not have a substantial adverse effect on management of personnel

The Commissioner rejected the department's argument that publication or disclosure of the document would have a substantial adverse effect on discipline, particularly noting that since 31 March 2019, the names of accused in Service Tribunals were published.

The Commissioner found that given the nature of the document and the reasons that the document exists, being the outcome of military tribunals where allegations of misconduct are tested, she was not satisfied that the department established that the names in the document should be exempt under s 47E(c) as disclosure would not have a substantial adverse effect on the department's ability to manage its personnel.

Disclosure would be an unreasonable disclosure of personal information

The Commissioner was satisfied that in circumstances where an accused has not had their matter heard before the Defence Force Discipline Appeal Tribunal, where it was the practice of the department to de-identify outcomes, or where no decision has been published, that it would be an unreasonable to disclose this personal information in response to an FOI request.

The Commissioner was also satisfied that giving access to the names of individuals who have not had their matters heard and decisions published by the Defence Force Discipline Appeal Tribunal, would on balance, be contrary to the public interest.

▶ *Dreyfus and Attorney-General (Commonwealth of Australia) (Freedom of information)* [2021] AATA 249 (17 February 2021)

LEGAL PROFESSIONAL PRIVILEGE – CLAIM OF IMPLIED WAIVER – WHETHER PRIVILEGE WAS IMPLIEDLY WAIVED BY CONDUCT INCONSISTENT WITH THE MAINTENANCE OF LEGAL PROFESSIONAL PRIVILEGE

The applicant requested access to the legal advice provided to the Attorney-General about the operation of the 'Medivac legislation'.

The only issue before the Tribunal was whether the Attorney-General waived privilege in relation to the legal advice and associated documents. Mr Dreyfus argued the Attorney-General waived privilege when he disclosed the substance of the advice in a media release and a series of media interviews. The Attorney-General argued that references to the advice that were made during media interviews were only in relation to two propositions arising from the advice.

Purpose of disclosing advice is highly relevant in discerning whether privilege waived

The Tribunal agreed with the Attorney-General that disclosure was limited to the two propositions. However, it accepted Mr Dreyfus' contention that the disclosure amounted to the disclosure of a conclusion of legal advice and a reason underpinning that conclusion. The Tribunal noted that disclosure of the gist or substance of legal advice may or may not effect a waiver of privilege depending on whether or not the requisite inconsistency of conduct is established.

The Tribunal held that a highly relevant factor in discerning any inconsistency of the conduct with the maintenance of privilege was the purpose of the limited disclosure in the given context. The Tribunal considered that in this particular context, a limited disclosure of legal advice was made partially for the purpose of gaining a political advantage against a political opponent. The focus of the media release was not only to convince the public of a drafting error in the legislation, but also to attribute that error to the Government's political opponents.

The Tribunal found that the limited disclosure for this partial purpose was inconsistent with the maintenance of legal professional privilege and found that the Attorney-General, by his conduct, impliedly waived privilege over the parts of the first advice that addressed the two propositions disclosed in the press release, attached summary of the advice, and his public comments.

The Tribunal held that the Attorney-General's statements that he did not intend to waive privilege were insufficient, in the context of the conduct as a whole, to protect against an implied waiver.

Privilege only waived over parts of the advice

The Tribunal did not consider that the extent of the Attorney-General's disclosure and his purpose in doing so were inconsistent to the extent that waiver had occurred over the entirety of the advice. There had been no relevant disclosure of the other parts of the first advice, which addressed separate and discrete issues.

In relation to the second advice, which was received after the disclosures, the Tribunal noted that even though there was overlap with the first advice, the two documents were separate advices that addressed distinct issues. The Tribunal did not consider that privilege could have been impliedly waived by the Attorney-General's conduct that took place before the documents had been received by him.

▶ *'WN' and Inspector General of Taxation (Freedom of information) [2020] AICmr 71 (22 December 2020)*

SUBSTANTIAL ADVERSE EFFECT ON THE PROPER AND EFFICIENT CONDUCT OF AGENCY OPERATIONS (s 47E(d))

The applicant sought access to documents listing the capabilities and contact details (direct phone numbers and/or email addresses) of the Inspector General of Taxation (IGT) officers.

Release of unrecorded direct telephone numbers would have a substantial adverse effect on the proper and efficient conduct of the operations of the agency

The Commissioner found that the IGT employees' direct telephone numbers and work mobile telephone numbers were conditionally exempt under s 47E(d). Unsolicited calls to those numbers would fall outside the IGT's service platform and be unrecorded, undermining accountability, transparency, quality assurance and employee support.

Public interest did not favour disclosure

The Commissioner was also satisfied that disclosure of those numbers would be contrary to the public interest. She took into account the applicant's submissions that without this contact information he had difficulty making complaints. She gave only limited weight to the IGT's submission that disclosure could prejudice its employees' right to privacy and their health and safety, as that concern was not particularised to individual employees and there was no evidence that the applicant was likely to behave unreasonably. However, she accepted that disclosure could reasonably be expected to prejudice the IGT's performance of its functions, including complaint handling.

Other particulars of employees did not fall within s 47E(d)

The Commissioner found that the other information in the directory, including APS classifications and position titles of staff, was not conditionally exempt under s 47E(d). With respect to the direct complaints lines, the Commissioner considered it significant that IGT employees routinely disclosed those numbers to complainants.

▶ *'WM' and Department of Home Affairs (Freedom of information) [2020] AICmr 70 (22 December 2020)*

PREJUDICE LAWFUL METHODS OR PROCEDURES (s 37(2)(b)) – SUBSTANTIAL ADVERSE EFFECT ON THE PROPER AND EFFICIENT CONDUCT OF THE OPERATIONS OF AN AGENCY (s 47E(d))

The applicant made a request to the Department for access to documents relating to the Department's consideration, assessment or finding in relation to the applicant's identity, nationality or citizenship. The Department exempted the Identity Integrity Assessment form and Identity Integrity Assessment report under ss 37(2)(b), 47C and 47E(d).

Details of methods and procedures for conducting forensic document examination would prejudice lawful methods or procedures for identity verification investigation (s 37(2)(b))

The Acting Commissioner had regard to previous IC review decisions dealing with a document examination report and document examiner investigation. Having regard to the contested material and the Department's evidence, she was satisfied that the

disclosure of the relevant material would reveal lawful methods and procedures used by the Department in conducting forensic document examination and investigating the identity of individuals that is not generally known to the public, and that disclosure would prejudice the effectiveness of those methods and procedures. She affirmed the decision that the document was exempt under s 37(2)(b) of the FOI Act.

Remaining material would have a substantial, adverse effect on Department's identity investigations operations (s 47E(d))

The Acting Commissioner agreed with the Department that disclosing the processes and measures to make identity determinations could have the effect of revealing various aspects of the Department's identity investigations and thereby have a substantial and adverse effect on the efficient operations of the Department when conducting similar investigative actions in the future.

Public interest is against disclosure

In finding that disclosure would be contrary to the public interest, the Acting Commissioner found that disclosure could reasonably be expected to prejudice the ability of the Department to maintain and enforce the integrity of Australia's visa and citizenship processes by revealing covert operating procedures, in the context of a broader national migration framework.

As she was satisfied that the remaining contested material was exempt under s 47E(d), she did not consider the application of s 47C of the FOI Act.

▶ *'WD' and Department of the Prime Minister and Cabinet (Freedom of information) [2020] AICmr 61 (14 December 2020)*

DELIBERATIVE MATERIAL (s 47C) – PUBLIC INTEREST TEST (s 11A(5))

The applicant requested access to the redacted content in a Department of Prime Minister and Cabinet (Department) brief to the Parliamentary Secretary to the Prime Minister regarding the *Humanitarian Overseas Medal (Iraq) Declaration 2004* dated 26 September 2013. The applicant had obtained the redacted brief under the FOI Act as a result of an earlier request.

Deliberative material

The Acting Commissioner examined the document and found that it was created for the dominant purpose of providing advice and recommendations from the Assistant Secretary Honours, Symbols and Territories, Mr Peter Rush, to the then Parliamentary Secretary to the Prime Minister, The Hon. Josh Frydenberg in relation to the award of the Humanitarian Overseas Service Medal to a commercial contractor. The Acting Commissioner was satisfied that the advice and recommendations were deliberative matter for the purposes of s 47C.

Disclosure was not against the public interest

The Acting Commissioner found disclosure would not be contrary to the public interest noting that the Department had failed to particularise its contentions that disclosure would inhibit frankness and candour and there were no special or specific circumstances on the information before her such that a frankness and candour claim should weigh heavily against disclosure.

▶ *Patrick and Secretary, Department of Prime Minister and Cabinet (Freedom of information) [2020] AATA 4964 (9 December 2020)*

DAMAGE TO DEFENCE OF THE COMMONWEALTH (s 33(a)(ii)); DELIBERATIVE PROCESSES (s 47C); EFFECT ON FINANCIAL INTERESTS OF THE COMMONWEALTH (s 47D); EFFECT ON LAWFUL BUSINESS, COMMERCIAL OR FINANCIAL AFFAIRS (s 47G(1)(a))

Senator Patrick applied to the Department of the Prime Minister and Cabinet (Department) for access to an audit report completed by the Auditor-General on 6 September 2018 with respect to the acquisition by the Department of Defence from Thales Australia Ltd of the fleet of vehicles described as 'protected mobility vehicles – light' and known as the Hawkei.

Damage to defence of the Commonwealth: s 33(a)(ii)

The Department contended that disclosure of the exempt parts of the report (Disputed Material) would harm the prospects of Thales and the Australian Army exporting the Hawkei, which would have a negative flow on consequence for the sustainment of the capability of the Hawkei for use by the Australian Army.

The Deputy President took the view that the Disputed Material effectively restates what is contained in publicly available parts of the report, and that some information in the Disputed Material had been sourced from the public domain. On that basis, the Deputy President was not satisfied that the Disputed Material would, or could reasonably be expected to, cause damage to the export prospects of the Hawkei.

Deliberative processes: s 47C

The Deputy President found the report did not involve a deliberative process of the Auditor-General. He found that the Auditor-General's act of assessing the conduct of the Department of Defence with respect to the relevant procurement project did not involve a weighing up or evaluation of competing arguments. Nor did it involve the exercise of a judgment in developing and making a selection from different options. Rather, the report was prepared for the purposes of the Auditor-General performing the function of conducting a performance audit and preparing an audit report. The Deputy President's characterisation of the report and the Auditor-General's function led him to conclude that s 47C does not apply. The findings on s 47C are particular to the circumstances of this case and take a narrow view of the scope of the 'deliberative processes' exemption.

▶ *Plowman and Australian Securities and Investments Commission (Freedom of information) [2020] AATA 4729 (24 November 2020)*

MANAGEMENT OR ASSESSMENT OF PERSONNEL (s 47E(c)); PERSONAL PRIVACY (s 47F)

Ms Plowman requested documents related to a workplace complaint made against her.

Reasonableness of searches

Hard copy searches were conducted by ASIC; however, no electronic searches were conducted of ASIC's files. The ASIC employee responsible for processing the request did not consider it necessary because she did not reasonably expect any electronic documents to exist in the particular circumstance of the documents relevant to the request. The Deputy President was satisfied in these circumstances that 'reasonable efforts were made' to search for documents.

Management or assessment of personnel: 47E(c)

ASIC contended that the exempt material contained personal information and opinions of ASIC employees related to workplace issues and if it were released, employee engagement and cooperation could decrease and there was a risk that employees would not feel safe to raise concerns confidentially and have workplace issues addressed. Additionally, ASIC contended that because no investigation was undertaken and no adverse findings were made that there was no need to provide particulars of the complaints to the applicant.

The Deputy President considered that had ASIC taken the view that the complaint deserved to be investigated, the applicant would have been informed of the details and accorded procedural fairness, but that because no investigation was undertaken, it was not necessary to do so. He accepted ASIC's contention that disclosure of documents going to complaints raised with management would tend to discourage employees from raising matters with management.

Public interest test

The Deputy President commented that the public interest question did not relate to whether Ms Plowman was afforded procedural fairness; rather, it related to whether it was in the public interest to disclose the documents which were conditionally exempt. The Deputy President accepted the evidence of the ASIC witness as to the damage to the public interest.

ARCHIVES UPDATE

New policy for management of information and data

The National Archives of Australia's (NAA) Building trust in the public record: managing information and data for government and community policy came into effect on 1 January 2021. The policy will apply until 31 December 2025 (unless extended).

The aim of the policy is to further improve how Australian Government agencies create and manage records, information and data. The policy does this by identifying key requirements and actions for Australian Government agencies (and other Commonwealth bodies) to build capacity and address areas of lower performance.

The policy recognises that good information management has significant benefits to Government, including facilitating delivery on government objectives and building community trust in the creation, collection and use of Australian Government information. Good information management ensures information assets can be found, used and shared to meet government and community needs, which are available for use now and in the future, including as technologies change.

The three key requirements are for agencies to:

1. manage information assets strategically with appropriate governance and reporting
2. implement fit-for-purpose information management processes, practices and systems
3. reduce areas of information management inefficiency and risk (with a focus on transitioning to digital information assets and processes).

The policy gives several examples of what success could look like for each of the above, as well as posing relevant case studies. Appendix A to the policy lists specific actions for agencies to implement under each of the requirements, with actions 1, 9 and 14 being mandatory, and provides implementation advice. The NAA has updated existing advice and will release additional supporting products and advice throughout the operation of the policy.

Appendix B to the policy lists key Australian Government agencies with policy responsibility for information management.

It is important that everyone who works for, or on behalf of, the Australian Government understands their responsibilities in relation to managing information, and we encourage you to familiarise yourself with the new requirements and mandatory actions under the policy.

OTHER MATTERS

SAVE THE DATE

FOI and Privacy Forum

Friday 7 May 2021 | 9 am – 4 pm

Please save the date for our upcoming FOI and Privacy Forum. This forum is held once every 2 years and includes a mix of significant and contemporary topics in information law.

You will have an opportunity to hear from a range of FOI and Privacy experts, including AGS lawyers and esteemed guests, and to network with fellow practitioners.

We will traverse:

- significant cases
- legal developments
- emerging policy reviews
- practical guidance for agencies

So we can meet with as many of you in person as possible, we will be hosting sessions from our AGS offices across Australia and joining together via video link. We will also have a livestream option available.

Further details to come including agenda and cost. www.ags.gov.au

---

FOI and Privacy courses

(face-to-face or online via GovTeams/Microsoft Teams)

Courses	*Outlines*
Introduction to FOI	View
FOI next steps	View
FOI exemptions	View
FOI exemptions and decision-making	View
Introduction to privacy	View
Practical privacy	View
APP intensive	View
ACT FOI key concept, exemptions and decision-making	View

If you require any further information on the above courses, please email trainingservices@ags.gov.au or call 02 6253 7464/02 6253 7145.

Information Law Team

Information Law Team Leader

Elena Arduca
Senior Executive Lawyer
T 03 9242 1473
elena.arduca@ags.gov.au

Specialist FOI advisors and counsel

Justin Hyland
Senior Executive Lawyer
T 02 6253 7417
justin.hyland@ags.gov.au

Justin Davidson
Senior Executive Lawyer
T 02 6253 7240
justin.davidson@ags.gov.au

Information Law Team

Melbourne

Melissa Gangemi
Senior Executive Lawyer (A/g)
T 03 9242 1329
melissa.gangemi@ags.gov.au

Laura Butler
Senior Lawyer
T 03 9242 1320
laura.butler@ags.gov.au

Canberra

Charine Bennett
Senior Lawyer
T 02 6253 7639
charine.bennett@ags.gov.au

Louise Futol
Senior Lawyer
T 02 6253 7073
louise.futol@ags.gov.au

Erin McGachey
Lawyer
T 02 6253 7162
erin.mcgachey@ags.gov.au

Lauren Lai
Lawyer
T 02 6253 7407
lauren.lai@ags.gov.au

Sydney

Amie Grierson
Senior Lawyer
T 02 9581 7521
amie.grierson@ags.gov.au

Caitlin Emery
Senior Lawyer
T 02 9581 7784
caitlin.emery@ags.gov.au