Welcome to AGS's second Information Law Update for 2020, bringing you the latest developments in FOI and Privacy law.

We are interested to make 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

ACCESS TO INFORMATION DAY 2

FOI UPDATE 2

- FOI Essentials Toolkit 2
- Disclosure of public servants' names position paper 3
- FOI case studies 4

PRIVACY UPDATE 9

- Threshold Privacy Impact Assessments 9
- Notifiable Data Breaches Report – January - June 2020 10
- OAIC and UK Information Commissioner's Office (ICO) Clearview investigation 10
- Privacy case studies 11

ARCHIVES UPDATE 15

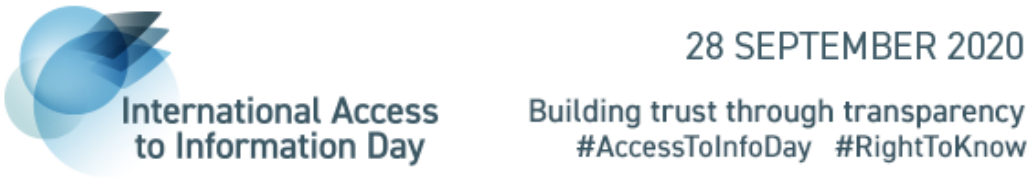
- Archives case studies 16

OTHER MATTERS 17

- Practitioner Forum date 17
- FOI and Privacy courses 17
- Information Law Team 18

ACCESS TO INFORMATION DAY

This update marks International Access to Information Day, better known as 'Right to Know' day. This global event recognises the importance of the community's right to access information held by government, and we recognise the important role our clients play in assisting members of the public to exercise their rights.



The Office of the Australian Information Commissioner (OAIC) has launched a website containing useful resources to mark the day, including a message from the Information Commissioner (the Commissioner).

AGS is the Australian Government's central legal service, with a long history with and depth of specialist expertise in relation to FOI and access to information. We are proud to assist agencies in relation to their obligations to facilitate access to government information.

FOI UPDATE

FOI Essentials Toolkit

The OAIC has launched a new toolkit, FOI Essentials, which repackages the Commissioner's Guidance and FOI resources to make it easier for APS staff and FOI practitioners to identify relevant information, tips and resources. Similar to the Privacy Officer toolkit, this will be a great reference for FOI practitioners.

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

Disclosure of public servants' names position paper

The OAIC has released a position paper, Disclosure of public servants' names and contact details in response to FOI requests. This paper is the outcome of consultation on an earlier discussion paper, and seeks to address the balance between transparency and accountability, and the right of public servants to be safe in the context of a changed online environment. The paper outlines a set of principles that will inform updates to the FOI Guidelines (which will be the subject of consultation). Key points from the paper are:

- the Commissioner remains of the view that generally it will not be unreasonable to disclose the names and contact details of public servants because this information only reveals that they were performing their public duties
- Agencies should take a starting position that full names and contact details of staff should be disclosed in documents in response to FOI requests, unless a work health and safety risk has been identified. Specific concerns about the health, safety and wellbeing of staff are most appropriately addressed under the conditional exemption in section 47E(c) of the FOI Act.
- where such a risk exists (for example, because of the nature of the agency's work or client base), the position paper suggests the agency should consider whether the only way to mitigate these risks is by removing the names and contact details before release, or whether there are other ways to mitigate any risk
- Where a risk exists and it cannot be mitigated, agencies should try to negotiate the scope of the request to exclude names and contact details as irrelevant material (s22 of the FOI Act). If the applicant does not agree, the agency must make a decision based on the particular circumstances and the context of the matter. Factors that may be relevant to assessing the risk include:
  - the nature of the functions discharged by the agency such as law enforcement functions
  - whether the FOI applicant has a history of online abuse or a history of harassing or abusing staff
  - the personal circumstances of the particular public servant, such that they may be vulnerable to, or at greater risk of harm, if their name and contact details are disclosed – for example, circumstances of family violence, mental health issues or other factors
- if redacting names and contact details, agencies should consider whether it is appropriate to impose a charge given the increased time redactions take (noting that the decision to impose a charge is discretionary)
- In general, it will only be appropriate to delete names and contact details as irrelevant material where the applicant gives explicit confirmation. Agencies may ask this question in access request forms and, if adopting such a practice, should be transparent about this on their website.
- agencies must ensure that staff understand that they are accountable for their decisions, their advice, and their actions, and this must be made clear in induction and training.

FOI case studies

'SY' and Services Australia (Freedom of information) [2020] AICmr 39 (12 August 2020)

REQUIREMENT FOR REQUEST – (S 15(2)(B)); PRACTICAL REFUSAL (IDENTIFICATION OF DOCUMENTS) (SS 24, 24AA, 24AB)

Background to the review: The applicant made an FOI request for access to documents relating to their interactions with Services Australia. However, because they had been framed as questions rather than requests for documents, Services Australia considered the request to be 'invalid.'

The applicant complained to the Commonwealth Ombudsman's office, which transferred the applicant's complaint to the OAIC pursuant to s 6C of the *Ombudsman Act 1976*.

The Commissioner treated the complaint as an application for an IC review.

Validity of request – can I ask questions?

The Commissioner considered whether the FOI request was a valid request for the purposes of s 15(2)(b), which requires the applicant to provide information necessary to enable document(s) falling within scope to be identified. However, s 15(3), in combination with the FOI Guidelines, also requires agencies to take reasonable steps to assist applicants with making a valid FOI request. The Commissioner noted that there was no evidence that Services Australia had taken such steps. In particular, Services Australia had not commenced either informal or formal consultation under s 24AB of the *Freedom of Information Act* (FOI Act) in order to clarify aspects of the request.

Request was not invalid

The Commissioner considered Services Australia's submission that the request was invalid because it had been framed as a series of questions. The Commissioner noted that the FOI Guidelines encouraged agencies to take a broad view of what constitutes a request and referred to *Mills and Department of Immigration and Border Protection* [2014] AICmr 54, where the previous Commissioner found that it may be appropriate for an FOI request to identify documents by reference to the information that they would contain.

The Commissioner was satisfied that the applicant had provided sufficient information to enable Services Australia to identify the documents sought by the applicant, notwithstanding that the request consisted of questions rather than requests for documents. The Commissioner set aside Services Australia's decision under s 55K and substituted its decision that the applicant's FOI request was a valid FOI request for the purposes of s 15(2)(b) of the FOI Act and Services Australia was required to process the request.

This decision demonstrates that agencies should be mindful not to interpret requests too narrowly or to assume that a request that may be in the form of questions necessarily means that relevant documents are not able to be identified for the purpose of s 15(2)(b).

'SW' and Australian Criminal Intelligence Commission (Freedom of Information) (No 2) [2020] AICmr 36 (5 August 2020)

REASONABLE SEARCHES S 24A; CREATION OF A NEW DOCUMENT S 17

The request: The applicant in this matter sought access to '[t]he number of convicted child sex offenders from Australia believed to be living abroad.'

The Australian Criminal Intelligence Commission (ACIC) initially identified one document within the scope of the applicant's request and refused access on the basis that it was exempt under s 47B of the FOI Act (damage to Commonwealth-State relations exemption). In the course of deciding the request, the ACIC consulted with 6 State and 2 Territory police agencies under s 26A of the FOI Act, some of which objected to the disclosure of the information.

Internal review decision: In its internal review decision, the ACIC decided instead that no single document fell within the scope of the applicant's request. The ACIC considered whether it could produce a document in accordance with s 17 of the FOI Act and declined to do so on the basis that any document produced would be exempt under s 47B.

Reasonable searches (s 24A of the FOI Act)

The Commissioner was satisfied that reasonable steps had been taken to find the requested document before refusing access to it on the basis that it could not be found or did not exist, in accordance with s 24A of the FOI Act.

During the Information Commissioner review, the ACIC submitted that the information sought was stored in a national policing agency system known as the Australian National Child Offender Register (ANCOR). The Register was housed on the National Child Offender System (NCOS), a system used for police agencies to record, search and access child sex offender data, and to monitor and manage registered offenders. The ACIC submitted that ANCOR is used by all Australian police jurisdictions within a strictly controlled framework for access and use of data under the statutory schemes in the different jurisdictions. Although ACIC was capable of providing the information because it housed and was responsible for the administration and maintenance of ANCOR, it was not authorised to do so and would need permission from all States and Territories to allow it to extract and provide the information.

The limitations on access based on the operation of State and Territory child protection legislation were sufficient for the ACIC to satisfy its onus to establish that all reasonable steps had been taken to find documents within the scope of the request.

Creation of a new document (s 17 of the FOI Act)

The Commissioner was also satisfied that the obligation under s 17 to create a new document did not apply in this case.

Section 17(1) of the FOI Act requires an agency to produce a written document in response to an FOI request and deal with the request for the document under the FOI Act as it would for any document already in its possession.

This obligation applies if these conditions are met:

- it appears from the request that the desire of the applicant is for information that is not available in discrete form in written documents of the agency (s 17(1)(b))
- it does not appear from the request that the applicant wishes to be provided with a computer tape or computer disk on which the information is recorded (s 17(1)(ba))
- the agency could produce a written document containing the information by using a 'computer or other equipment that is ordinarily available' to the agency for retrieving or collating stored information (s 17(1)(c)(i)), or making a transcript from a sound recording (s 17(1)(c)(ii)).

However, an agency is not required to comply with the obligation to produce a document if it would substantially and unreasonably divert the resources of the agency from its other operations (s 17(2)).

The Commissioner again had regard to the limitations imposed upon the ACIC by State and Territory legislation authorising child protection registers and enabling the establishment of the NCOS. The absence of authorisation by State and Territory police agencies for the purposes of providing access to the information under the FOI Act meant that the ACIC could not produce a written document containing the information requested by the applicant in discrete form by the use of a computer or other equipment that was ordinarily available to it.

Rex Patrick and Commonwealth Scientific and Industrial Research Organisation (Freedom of Information) [2020] AICmr 34 (5 August 2020)

RELEVANT MATERIAL S 22(1)(A)(iii); DELIBERATIVE MATERIAL AND PUBLIC INTEREST S 47C

The request: Senator Patrick applied to the CSIRO for access to 'any reports, investigations or documents' that were produced by the CSIRO as a result of the findings in the Murray-Darling Basin Royal Commission report.

Reviewable decision: The CSIRO refused access to one of the 5 documents, relying on the deliberative processes exemption (s 47C). CSIRO granted access to four documents with deletions on the grounds that the information was irrelevant to the request (s 22(1)(a)(iii)).

Whole documents were relevant

The Commissioner was not satisfied the information was irrelevant, finding that as the request was for 'reports' and 'documents' produced in response to the Royal Commission report, the entirety of any document that the CSIRO had identified as within the scope of the request would be covered by the request.

Material was deliberative but public interest favoured disclosure

The Commissioner accepted that the material comprised an assessment and evaluation of the Royal Commissioner's report, which included commentary made about the CSIRO and its research. The Commissioner found that a vital part of the CSIRO's function is to facilitate the application of the CSIRO's scientific research, including ensuring that the public perception of the research is not misleading. As the document related to the functions of the CSIRO, it was deliberative matter and was conditionally-exempt under section 47C of the Act.

In addressing public interest factors weighing against disclosure, the CSIRO had submitted that the detriment to the ability of the CSIRO to engage internally in critical discussions regarding scientific integrity outweighed arguments for disclosure of the document for the public benefit, raising a 'frankness and candour' argument. The Commissioner affirmed that frankness and candour claims may be contemplated when considering deliberative material and weighing public interest, but should be approached cautiously and in accordance with sections 3 and 11B of the FOI Act. The Commissioner noted that the circumstances in which these claims arise should be special and specific.

In making her decision, the Commissioner referred to her approach in *'PM' and Department of Industry, Innovation and Science (Freedom of information)* [2018] AICmr 70, and was not persuaded that 'special and specific circumstances' were made out, as sufficient particulars were not given to explain how disclosing the material would impact the CSIRO's abilities to implement its functions and engage internally in critical discussions.

Farrell; Chief Executive Officer, Services Australia and (Freedom of Information) [2020] AATA 2390 (21 July 2020)

PRACTICAL REFUSAL – SUBSTANTIAL AND UNREASONABLE DIVERSION OF RESOURCES SS 24, 24AA

The request: The FOI applicant, Mr Farrell, requested access to the 'final decision notices to all applicants for Australian Victims of Terrorism overseas payments since January 2014.'

The initial decision: Services Australia found that a practical refusal reason existed because processing the request would take 195 hours, and 'substantially and unreasonably' divert the agency's resources from its 'other operations' (s 24AA FOI Act).

IC Review: The FOI applicant applied to the Commissioner for review and the Commissioner set aside the decision, on the basis that it was estimated that it would take 61.25 hours to process the request, which was a substantial but not unreasonable burden for Services Australia.

61.25 hours was substantial but not unreasonable

Services Australia applied to the Administrative Appeals Tribunal (Tribunal) for review of the Commissioner's decision.

In the Tribunal proceeding, it was agreed it would take 61.25 hours to process the request and involve not only employees from the FOI team but also the Emergency Management Team.

In making its decision, the Tribunal found that Services Australia constitutes a 'substantial agency,' having regard to its responsibility for payments totalling $184 billion (2018-2019), its 28,000 employees and the fact it had processed 6,210 FOI requests in 2018-2019.

The Tribunal rejected the FOI applicant's contention that the FOI team's work should not be included in the 'other operations' that would be diverted from by the FOI applicant's request.

The Tribunal adopted a definition of 'substantially' that included 'real or of substance,' rather than merely large and found that a request taking 61.25 hours to process would result in substantial diversion of resources.

The Tribunal considered that processing the request was well within the agency's capacity and that the bulk of work would be done by the FOI team. Despite the FOI applicant's refusal to narrow the request, the Tribunal considered the information could not have been obtained with a less burdensome request, taking into account Services Australia's concession that previously unpublished information about the program would be released if the request were processed. The Tribunal briefly addressed the public interest in the requested documents and found it was satisfied simply by additional information about a government spending program coming to light. Finally, despite the quantity of information already publicly available about the program, once it was conceded that more information would be available to the public as a result of processing the request, the Tribunal considered it would be a rare case that the disclosure of other information about the same program would aid in establishing that the consequent diversion of resources was unreasonable.

The Tribunal found that although the request would substantially divert the resources of the agency, it was not an unreasonable diversion for a 'substantial agency' such as Services Australia and affirmed the decision under review.

Jackson Gothe-Snape and Services Australia (Freedom of Information) [2020] AICmr 19 (1 June 2020)

CABINET DOCUMENTS – DOMINANT PURPOSE; WHETHER DISCLOSURE WOULD REVEAL A CABINET DELIBERATION OR DECISION

DELIBERATIVE PROCESSES – WHETHER DELIBERATIVE MATTER AND PURPOSE; PUBLIC INTEREST

The request: the applicant made a request to Services Australia for access to 'the successful policy proposal from the department for Taskforce Integrity and any emails or meeting notes concerning the drafting of that proposal.' Pursuant to s 24AB of the FOI Act, the applicant revised the scope of the request to 'the document that was first approved by the Minister that proposes the policy of establishing or implementing Taskforce Integrity.' Services Australia identified one document within the scope of the request and refused access to the document in full, relying on the Cabinet documents exemption (s 34).

Document contained deliberative matter but public interest favoured disclosure

The Commissioner was not satisfied that at the time of creation the document was brought into existence for the dominant purpose of briefing a minister on a submission, or proposed submission, to Cabinet. Therefore, the Commissioner found that the final New Policy Proposal (NPP) was not an exempt document under s 34(1)(a). The Commissioner noted that insufficient particulars had been provided about the context and timing of the creation of the document. The Commissioner examined the document in issue and noted that Services Australia had provided insufficient particulars as to the material in the document that it contended was subject to Cabinet's deliberations. The Commissioner also had regard to the material relating to Taskforce Integrity in Services Australia's 2015-2016 Annual Report, and found that the existence of the Cabinet deliberation or decision in relation to the establishment or implementation of Taskforce Integrity had been officially disclosed in the 2015-16 Budget Paper statements and Services Australia's annual report. Therefore, the document was not exempt under s 34(4).

The Commissioner found the material was conditionally exempt under s 47C as it comprised opinions or advice that had been prepared for the purpose of briefing the Minister for his deliberation. However, the Commissioner found that providing the applicant with access to the relevant material would not be contrary to the public interest. The Commissioner had regard to '*PM' and Department of Industry, Innovation and Science (Freedom of information)* [2018] AICmr 70 and was not satisfied that the disclosure of the material in this case would 'have an adverse impact on the trusting and effective working relationship between Services Australia and the Minister' or that it would 'diminish the value, quality and relevance of future briefs if they were to be written in anticipation of possible public disclosure' as Services Australia claimed.

PRIVACY UPDATE

The OAIC has released the 2020 Australian Community Attitudes to Privacy Survey. This survey informs business and government about public expectations when it comes to safeguarding personal information.

The Survey highlights the increase in public awareness of digital privacy risks, and community concern about privacy and digital services, including digital tracking, ID theft, fraud and data breaches. It also highlights the importance of good communication, with 84% of people believing it is a misuse of personal information when information is supplied for one specific purpose and used for another purpose.

This is a salient reminder of the importance of providing clear privacy notices and having comprehensive and up-to-date privacy policies available.

More information is available on the OAIC's website.

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

Threshold Privacy Impact Assessments

The OAIC has released a new privacy resource, When do agencies need to conduct a privacy impact assessment?

This guidance helps agencies to screen for projects where there are privacy implications by completing a threshold assessment to determine whether a PIA is required under the Privacy (Australian Government Agencies – Governance) APP Code 2017. The OAIC has also developed a template to assist agencies in completing a threshold assessment.

Notifiable Data Breaches Report – January - June 2020

The OAIC has released its six-monthly statistical report about notifications received under the Notifiable Data Breaches Scheme. What was notable about this report was some of the more detailed advice to entities based on observations of notifications made under the scheme, including the following take-aways:

- the capacity to conduct a timely and thorough assessment and investigation of a suspected data breach can be constrained when an entity is unsure of its own information environment and holdings
- entities that did not have audit or activity logging enabled on their network or email servers and accounts, or that could not undertake retrospective traffic analysis of their internet gateway had difficulty determining whether there had been malicious access to their system, or exfiltration of personal information
- not having an effective understanding of what information an agency retains and where it is stored makes it difficult for an agency to respond to a breach, and may also place the entity in breach of APP11
- The OAIC observed a growing risk from Ransomware attacks. The OAIC highlights the importance of entities fully understanding how and where personal information is stored on their network, and notes that entities should consider network segmentation, additional access controls and encryption to reduce the risk of personal or commercial information being exposed by a ransomware attack.
- phishing was still a key cause of data breaches, and the OAIC highlighted steps taken by some entities after experiencing a phishing attack, including:
  - training staff in identifying and responding to phishing emails
  - implementing multi-factor authentication on email accounts
  - resetting credentials on the compromised email accounts and/or the wider network
  - reviewing and upgrading existing security measures to include ongoing monitoring and antivirus and malware detection.

The report highlights the importance of entities learning from the insights of the statistical reports, and taking reasonable steps to protect personal information in line with their obligations under APP 11, rather than waiting for a serious incident to put in place protective measures.

OAIC and UK Information Commissioner's Office (ICO) Clearview investigation

The OAIC and UK ICO have opened a joint investigation into the personal information handling practices of Clearview AI Inc, focusing on the company's use of 'scraped' data and biometric information of individuals.

Clearview's facial recognition application allows face matching between photos of an individual and images collected from the internet, and then links to where the images appeared. Images are alleged to have been 'scraped' from social media platforms and other websites, for inclusion in a database said to include more than three billion images.

This investigation will set an interesting precedent in relation to the collection and use of biometric data and facial recognition technology. Watch this space.

Privacy case studies

Mullen v Aged Care Quality and Safety Commission [2020] FCAFC 78

On 13 May 2020 the Full Court of the Federal Court (McKerracher, Colvin and Jackson JJ) dismissed an appeal from 2 judgments of a single judge of the Federal Court. The matter concerned 2 FOI requests made by the appellant for access to documents regarding a complaint he made in relation to an aged care facility. Some documents within that request had been found to be exempt pursuant to s 38 of the FOI Act, because they contained information the disclosure of which was prohibited under s 86-2(1) of the Aged Care Act 1997 (Aged Care Act), a provision which is listed in Schedule 3 to the FOI Act.

The appellant first argued that the documents were not exempt because the Secretary had a discretion to publicly disclose certain information under s 86-9 of the Aged Care Act and accordingly, documents that contained the types of information specified in s 86-9 could be released to him. The Court rejected this argument, finding that unless and until the power in s 86-9 had been exercised, disclosure of the information described in s 86-9 was prohibited under s 86-2. It followed that it was exempt from disclosure under s 38 of the FOI Act.

The second argument advanced by the appellant was that the power conferred on the Commissioner under s 55K(2) of the FOI Act allowed the Commissioner (and the Tribunal on review) to exercise the power of the Secretary under ss 86-3 and 86-9 of the Aged Care Act to release information to him. The Court found that this had no application in the present case, because the power to disclose information under ss 86-3 and 86-9 was conferred on the Secretary, who was not the decision-maker for the purposes of the FOI Act. The respondent submitted that the power in s 55K(2), which provides that for the purpose of implementing a decision made by the Commissioner on an IC review, the Commissioner may perform the functions and exercise the powers of the person who made the reviewable decision, was confined to the implementation of a decision and the powers of the Secretary could not be exercised for that purpose. The Court declined to express any view on this submission.

The case provides an example of the distinction between the duty to disclose documents under the FOI Act and the discretion to disclose information pursuant to provisions in other Acts, and why these separate and distinct bases for disclosing information should not be conflated.

An application for special leave to appeal the judgment of the Full Court has been dismissed.

Australian Information Commissioner v Facebook Inc (No 2) [2020] FCA 1307

In April of this year, the Federal Court made orders for the service outside jurisdiction on Facebook Inc of the Commissioner's application alleging contravention of civil penalty provisions in the Privacy Act.

On 14 September 2020, the Federal Court dismissed Facebook Inc's application to set aside those orders.

Relevantly, Justice Thawley found that the Commissioner had met the threshold of establishing a prima facie case that Facebook Inc carried on business in Australia, and collected or held personal information in Australia, in the relevant period; and therefore had a prima facie case that the Privacy Act applied extra-territorially to the relevant acts or practices of Facebook Inc: see s 5B(3) of the Privacy Act.

Facebook Inc has applied for leave to appeal from the judgment OR Facebook Inc has not appealed the judgment.

AGS acts for the Commissioner.

'ST' and Chief Executive Officer of Services Australia (Privacy) [2020] AICmr 30 (30 June 2020)

IPP 11 (breach)

Remedy: Non-economic loss: $3,000

Complaint: ST objected to a decision by the former Child Support Agency (CSA) in relation to child support paid by her ex-partner. In conducting a review of its decision, CSA collected ST's bank statement from ST's bank using its statutory collection powers and without notifying ST. The bank statement contained personal information regarding ST's purchases, including the location and frequency of those purchases (locational information). When ST sought review of the CSA's objection review decision with the then Social Security Appeals Tribunal, CSA provided the Tribunal and ST's ex-partner (who was a party to the review) with a bundle of relevant documents which included the bank statement.

ST alleged that the collection from the bank and the disclosure to her ex-partner interfered with her privacy. ST said that she feared harm from her ex-partner, and had attempted to keep her location unknown to him. CSA had some awareness of the need to remove information as ST had made redactions on the bank statements she provided to CSA herself.

Determination of breach: The Commissioner found that collection had been done lawfully as it was for the purpose of processing an objection application, which necessarily involved a high degree of intrusion into ST's financial affairs.

The Commissioner accepted Services Australia's submission that the disclosure of most of the personal information was lawful because s 95(3) of the *Child Support (Registration and Collection) Act 1988* required Services Australia to provide relevant documents to the Tribunal and to parties to the review. However, as s 95(3) (at that time – since amended) permitted documents to be provided *in part*, the Commissioner found that CSA should have redacted the bank statement to remove the locational information, which the Commissioner found was not relevant for the purposes of s 95(3).

Remedies: The Commissioner found that this breach had caused ST distress and awarded an amount of $3,000. ST also claimed economic loss arising from damage to her car allegedly caused by her ex-partner, the subsequent cost of hastily selling her car at a loss because of fear of harm, solicitor's fees and impairment of her regular counselling and psychiatric sessions. The Commissioner found that ST had provided insufficient evidence establishing this damage or establishing that the damage had a causal connection with the disclosure.

As the Commissioner was satisfied that the breach was unlikely to be repeated in the future, she declined to make a declaration requiring Services Australia to take preventative steps.

Agencies should take care when including personal information in Tribunal documents that they are relevant and necessary to the review and consider whether any parts ought to be redacted.

'SF' and 'SG' (Privacy) [2020] AICmr 22 (19 June 2020)

APP 12 (breach)

Remedy: Non-economic loss: $3,000; Aggravated damages: $2,000; declaration that the respondent must provide the complainant with access to her clinical records

Complaint: The complainant, 'SF', was a patient of the respondent's psychological services between February and November 2014. In 2017, she made 2 requests for access to her clinical records. The respondent did not respond to the requests.

In correspondence to the Commissioner, the respondent initially claimed that information would not be provided because of ongoing legal proceedings. The respondent later claimed that he did not hold the personal information at the time of the request, alleging the complainant may have taken them while working for him. Alternatively, the respondent relied on various exceptions to the requirement to provide access under APP 12.1.

Determination of breach: The Commissioner was satisfied that the respondent held the clinical records at the time of the access request, rejecting the belated assertion that the records had been taken by the complainant.

Further, the Commissioner found that no exception under APP 12.3 applied:

- giving the complainant access to the records would not impact on the privacy of others as the complainant would presumably already know the content of the materials in them: APP 12.3(b)
- the request was not frivolous or vexatious as the Commissioner accepted the complainant did not take her records: APP 12.3(c)
- the records did not relate to legal proceedings between the parties, and in any event, the proceedings had been finalised: APP 12.3(d)
- no unlawful activity was made out: APP 12.3(h).

The Commissioner concluded that the respondent had breached APP 12.1 by failing to provide access, and APP 12.9 by failing to notify the complainant of the reasons for the refusal and how she could complain about it.

Remedies: The Commissioner awarded the complainant $3,000 for non-economic loss for hurt feelings arising out of the privacy breach but found that no economic loss was made out. The Commissioner also awarded $2,000 in aggravated damages because the respondent's conduct towards the complainant was insulting and unjustified, demonstrating a disregard for the complainant's privacy rights. The Commissioner declared that the respondent must send to an authorised person, nominated by the complainant and notified to the Commissioner, a copy of her clinical records or if not possible, a statutory declaration explaining why.

The Commissioner commented on the respondent's failure to respond to a notice issued pursuant to s 44 of the Privacy Act and that she would consider taking further action to address this non-compliance.

'SD' and 'SE' and Northside Clinic (Vic) Pty Ltd (Privacy) [2020] AICmr 21 (12 June 2020)

APP 6 (breach) – APP 11 (breach)

Remedy: Non-economic loss:$10,000 (first complainant), $3,000 (second complainant); Economic loss: $3,400 (first complainant)

Complaint: The first complainant was a patient of the respondent's clinic who was diagnosed as HIV-positive. He and his husband (second complainant) had previously been part of a global study into particular aspects of HIV transmission facilitated by the respondent and were considering participating in a further study. The first complainant provided his work email address, which included a reference to his place of employment, and the second complainant provided a personal email address, which comprised his first and last name, as well as his middle initial.

During email correspondence with the first complainant, the respondent copied in an incorrect email address for the second claimant, breaching APPs 6 and 11.

Determination of breach: The Commissioner found that the respondent disclosed personal information about the complainants to an unknown third party. The personal information disclosed was sensitive information as defined in the Privacy Act, as it included health information and information about the complainants' sexual orientation. The Commissioner did not accept the respondent's contention that the second claimant was not reasonably identifiable and found that the respondent breached APP 6 in relation to both complainants.

The Commissioner found the respondent breached APP 11 in failing to take reasonable steps to protect personal information given that the disclosure occurred and there was no evidence of steps taken by the respondent prior to the incident to prevent such disclosure.

Remedies: The Commissioner awarded the first complainant $3,400 for economic loss for the cost of psychologist sessions and $10,000 for non-economic loss. In making the latter award, the Commissioner placed significant weight on 2 reports prepared by the first complainant's treating psychologist regarding the distress and psychological damage caused by the privacy breach. It was highly relevant that the psychiatrist had treated the applicant for unrelated matters before the breach and could comment on the first complainant's psychological state at an earlier time and at the time of the disclosure. The Commissioner also awarded the second complainant $3,000 for non-economic loss as a result of the distress caused by the breach. No award of aggravated damages was made.

The Commissioner was satisfied the respondent had subsequently taken steps to improve its compliance with APP 11 and did not consider it necessary to declare that the respondent take further steps.

ARCHIVES UPDATE

Archives case studies

The Palace Letters – *Hocking v Director-General of the National Archives of Australia* [2020] HCA 19

In this case, the High Court of Australia considered the meaning of 'Commonwealth records' as defined in the *Archives Act 1983* (Cth) (the Archives Act). The High Court held that whether a record is the 'property' of the Commonwealth or a Commonwealth institution for the purposes of that definition is a question of the power to control the custody of the record, rather than reference to common law concepts of ownership, or expectations held at the time of the deposit of a record with the National Archives of Australia (the NAA).

This decision concerned a 2016 request to the NAA by academic historian and writer, Professor Jennifer Hocking. Professor Hocking sought a file of correspondence between Her Majesty Queen Elizabeth II and the then Governor-General of Australia, the Right Honourable Sir John Kerr, dating to the period of his dismissal of the Whitlam Government in 1975. The NAA refused the request on the basis that the correspondence was not Commonwealth record. Professor Hocking sought judicial review of NAA's decision in the Federal Court of Australia. The Federal Court dismissed her application and her subsequent appeal to the Full Court of the Federal Court was also dismissed.

A 6:1 majority of the High Court allowed Professor Hocking's appeal, declared the deposited correspondence to be Commonwealth records within the meaning of the Archives Act and ordered that a writ of mandamus issue to compel the Director-General to reconsider Professor Hocking's request for access.

The central question for the High Court was whether the correspondence fell within the definition of 'Commonwealth records' and was therefore subject to Part V, Division 3 of the Archives Act. With possible exceptions, this would mean that it would be required to be made available for public access because it had entered the 'open access period.' If the correspondence was not a Commonwealth record, it would be covered by arrangements that allowed for public access only after 8 December 2027, subject to approval of the Queen's Private Secretary and the Official Secretary to the Governor-General.

The Archives Act defines a Commonwealth record as 'a record that is the property of the Commonwealth or of a Commonwealth institution.' In turn, 'Commonwealth institution' is defined to include 'the official establishment of the Governor-General.' The High Court found the term 'property' connoted the existence of a relationship in which the Commonwealth or a Commonwealth institution had a legally-endorsed concentration of power to control the custody of a record. Such a power could arise from the capacity to exercise a common law or statutory right from either ownership or possession, but these are not essential. At [96:]

> … the concentration of power can arise from a capacity to control the physical custody of the record that is conferred and is exercisable as a matter of management or administration rather than as a matter of the recognition and vindication of rights of ownership or possession at common law. The Archives Act is not concerned to vindicate the incidents of ownership or possession at common law such as the right to destroy or the right to alienate the property. A record which is kept in the control of a Department in the course of the management and administration of the affairs of the Commonwealth is sensibly described as property of the Commonwealth for the purposes of the Archives Act whether or not another person – such as the author of the record – may have a claim to ownership or possession of the record under the general law.

In reaching its decision that the correspondence was the property of the official establishment of the Governor-General at the time of the deposit, the High Court considered its creation, keeping and deposit. After Sir John Kerr retired from the office of Governor-General in 1977, the correspondence had been left with the Official Secretary to the Governor-General, David Smith. In 1978, Mr Smith copied the correspondence, sent a copy to Sir John Kerr and deposited the original correspondence with the Australian Archives in his capacity as Official Secretary to the Governor-General. The High Court found that the actions of Mr Smith in making the arrangements and fulfilling the deposit demonstrated that the lawful power to control the physical custody of the correspondence lay with him in his capacity as Official Secretary.

Following this decision, the NAA has decided to release the letters in full. The letters are available on its website.

This decision has consequences for the way agencies view the definition of 'property' in the Archives Act and the Privacy Act. The decision means the question now is whether an entity has a capacity to control physical custody of a record rather than the previously understood definition that property required rights of ownership as at common law.

***McGrath and Director-General, National Archives of Australia* [2020] AATA 1790 (9 June 2020)**

This matter involved 24 applications to the Tribunal for review of decisions of the respondent (the Director-General of the National Archives of Australia) to refuse the applicant access to records held by Archives. The applicant (Ms McGrath) sought access to material relating to the negotiations between Australia and Indonesia in the 1970s regarding maritime boundaries in the seabed commonly known as the Timor Gap.

The material in issue comprised a large number of documents including DFAT files, cabinet submissions, advice, correspondence regarding negotiation strategies correspondence regarding negotiation strategies and a transcript of evidence given before the Parliamentary Joint Committee on Foreign Affairs and Defence.

The Director-General claimed that the transcript of evidence given before the Parliamentary Joint Committee on Foreign Affairs and Defence was subject to Parliamentary Privilege and therefore could not be disclosed under s 31 of the Archives Act. The Tribunal agreed and affirmed this decision.

In relation to the remaining material to which the applicant was refused access, the Director-General claimed a number of exemptions listed in s 33 of the Archives Act applied, namely:

(1) Section 33(1)(a): its disclosure could be reasonably expected to cause damage to the security, defence or international relations of the Commonwealth

(2) Section 33(1)(d): its disclosure could constitute a breach of confidence

(3) Section 33(2): it would be privileged from production in legal proceedings on the grounds of legal professional privilege and disclosure of the record would be contrary to the public interest.

In its consideration of the relevant exemptions, the Tribunal referenced the 'mosaic theory,' which describes the idea that even where an individual piece of information alone may not be sensitive, when viewed with other information it may become sensitive. The Tribunal ultimately found that the exemptions did apply and affirmed the decisions to refuse access.

OTHER MATTERS

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 Lawyer
T 03 9242 1329
melissa.gangemi@ags.gov.au

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

Thomas Creedon
Lawyer
T 03 9242 1297
thomas.creedon@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

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