FOI & PRIVACY

INFORMATION LAW UPDATE

No. 4 | 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

Proposed amendments to the *Privacy Act 1988* – the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021

On 25 October 2021, the Attorney-General released an exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021. The Bill would enable the creation of a binding Online Privacy code (OP code) for social media services, data brokers and other large online platforms operating in Australia.

The Bill seeks to strengthen privacy protections by:

- introducing a binding code of practice for social media and other online platforms that trade in personal information
- introducing an OP code
- enhancing penalties and enforcement measures available to the Australian Information Commissioner (Commissioner).

The OP code will set out how organisations that provide social media services, data brokerage services or large online platforms will need to meet the obligations under the *Privacy Act 1988* (Privacy Act) in addition to the particular requirements of the OP code.

The Bill will strengthen the Commissioner's enforcement functions by increasing the maximum civil penalty for a serious and/or repeated interference with privacy. For a natural person, the Bill increases the maximum civil penalty for serious and repeated interferences with privacy to 2,400 penalty units ($532,800 on current penalty unit values). For a body corporate, the maximum penalty will increase to an amount:

- not exceeding the greater of $10 million
- 3 times the value of the benefit obtained by the body corporate from the conduct constituting the serious and repeated interference with privacy
- 10% of their domestic annual turnover, if the value cannot be determined.

The Bill creates a new infringement notice provision for failing to give information, answer a question or provide a document or record to the Commissioner when required to do so as part of an investigation (with associated additional civil penalty provisions). The Bill will also create a new criminal penalty for multiple instances of non-compliance. This would enable the Commissioner to refer matters to the Commonwealth Director of Public Prosecutions for more serious, systemic conduct.

The Bill will clarify the extraterritorial application of the Privacy Act. The Bill will remove the condition that an organisation has to collect or hold personal information from sources inside of Australia. This would mean that foreign organisations who carry on a business in Australia must meet the obligations under the Privacy Act, even if they do not collect or hold Australians' information directly from a source in Australia.

Submissions on the exposure draft of the Bill were due on 6 December 2021. A copy of the exposure draft of the Bill is available from the Attorney-General's Department website.

Privacy Act Review – Discussion Paper

A broader review of the Privacy Act is being conducted in parallel with the Bill to build on privacy protections in the Privacy Act. On 12 December 2019, the Attorney-General announced that the Australian Government would conduct a review of the Privacy Act.

Key matters to be considered by the review include if:

- the scope and application of the definition of 'personal information' and if the word 'about' in the definition of personal information should be changed to 'relates to'
- the phrase 'reasonably identifiable' should cover circumstances in which an individual could be identified, directly or indirectly
- the definition of 'collection' should expressly cover information obtained from any source and by any means, including inferred or generated information
- there should be an express requirement in Australian Privacy Principle (APP) 5 that privacy notices must be clear, current and understandable, including legislating factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable
- consent should be defined as voluntary, informed, current, specific, and an unambiguous indication through clear action
- pro-privacy settings should be enabled by default

- an individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information
- APP 6 be amended to expressly require that, at or before using or disclosing personal information for a secondary purpose, APP entities are to determine each of the secondary purposes for which the information is to be used or disclosed and to record those purposes
- countries and certification schemes be prescribed for the purpose of APP 8.2(a)
- there should be a direct right of action available to any individual or group whose privacy has been interfered with by an APP entity
- there should be a statutory tort of privacy for serious invasions of privacy.

A copy of the exposure draft of the Bill and the Discussion Paper are available from the Attorney-General's Department website. Feedback on the Discussion Paper is due by **10 January 2022**.

OAIC releases Privacy Impact Assessment in relation to remote working arrangements

A copy of the Office of the Australian Commissioner's (OAIC) Privacy Impact Assessment (PIA) on remote working arrangements in response to COVID-19 has been published on the agency's FOI disclosure log.

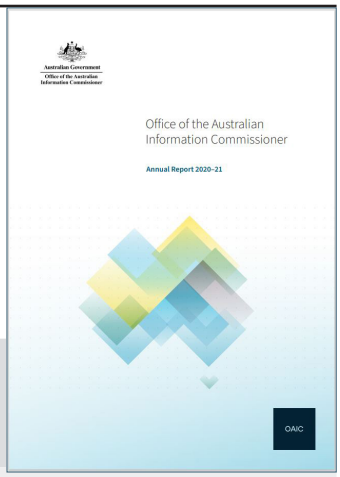
The PIA also contains an action plan allocating responsibility for recommended mitigation strategies.

OAIC conducts a desktop audit of PIA registers

In May 2021, the OAIC commenced a government-wide assessment of compliance with the requirement, under s 15(1) of the Australian Government Agencies Privacy Code (Code), to publish a register of the PIAs the agency conducts on their website.

Full details of the report are published on the OAIC website.

OAIC Annual Report 2020–21



On 21 October 2021, the OAIC released its 2020–21 Annual Report. The Annual Report provides statistical summaries of the privacy and FOI activities of the OAIC and across the Commonwealth.

Privacy

In 2020–21, in relation to the privacy function:

- the largest number of privacy complaints were received against entities within finance (including superannuation), Australian Government, and health service providers
- most privacy complaints received by the OAIC concerned:
  - APP 6 – the use or disclosure of personal information: 29.3%
  - APP 11 – the security of personal information: 28.2%
  - APP 12 – access to personal information: 17.9%.
- of the 71 privacy complaints which were closed by the OAIC in 2020–21 and in which compensation was given, 56 involved amounts of less than $5,000.

The full 2020–21 OAIC Annual Report can be downloaded from the OAIC's website.

Notifiable Data Breaches (NDB) Report

In the latest NDB Report (January–June 2021), Australian Government agencies again feature in the top 5 industry sectors to notify data breaches to OAIC. Australian government entities notified 34 data breaches in total (7% of all data breaches notified to OAIC during the reporting period).

Human error remains the most common cause of data breaches within the Australian Government, accounting for 25 out of 34 data breaches (74%). Sixteen of the human error breaches (64%) resulted from the disclosure of information to the wrong recipient by email, mail or other means. The last reporting period saw an increase in the number of Australian Government data breaches caused by a malicious or criminal attack. This included cyber incidents, the theft of paperwork or data storage devices and social engineering or impersonation.

The Commissioner has emphasised that a ransomware attack constitutes an eligible data breach if there are reasonable grounds to suspect that there *may have been* an eligible data breach, even if there is insufficient information to confirm whether the eligible data breach *has occurred*. Given the prevalence of these kinds of cyber-attacks, the OAIC expects entities to have appropriate internal practices, procedures, and systems in place to allow the entity to undertake a meaningful assessment of whether an eligible data breach may have occurred. By way of example, entities should keep audit and access logs, routinely test backup systems for data integrity, have an incident response plan, and consider engaging a cyber security expert if a ransomware attack occurs.

AGS has experience preparing operating procedures and fact sheets for a range of agencies. We can assist you to develop tailored resources for your agency to help you to prevent and respond to data breaches.

PRIVACY CASE STUDIES

- **Collection of customer biometric information without consent ruled out by Information Commissioner:**
  ***7-Eleven Stores Pty Ltd (Corrigendum dated 12 October 2021) [2021] AICmr 50* (29 September 2021)**

From June 2020–August 2021, 7-Eleven Stores Pty Ltd (7-Eleven) deployed a customer feedback mechanism that used a facial recognition tool supplied by a third-party provider.

Images were stored briefly on the tablet, before being uploaded via a secure connection to a secure server.

7-Eleven's purpose for collecting facial images and generating faceprints was to detect if the same person was leaving multiple responses to the survey, to exclude potentially false results, and to allow 7-Eleven to understand customer demographics. 7-Eleven could access individual survey responses at any time on the Service Provider's portal, and the provider generated and provided the respondent with regular reports. 7-Eleven argued that the facial images and faceprints were not personal information because they were not used to identify, monitor or track any individual.

The Australian Information Commissioner found:

Faceprints are personal information: The Commissioner found that faceprints were created by automatically converting facial images into an encrypted algorithmic representation of a customer's face. The Commissioner considered that as digital representations of a particular individual's facial features, the faceprints were information 'about' an individual, as the process by which faceprints were generated allowed the person to be distinguished from other individuals whose faceprints were held on the Server, making them 'reasonably identifiable'. The faceprints were also found to be biometric information that is 'sensitive information' (s 6 Privacy Act).

Collection via third party: The Commissioner found that 7-Eleven collected the facial images when the data was temporarily stored on the tablets, and because 7-Eleven had contractual control and a right of access over the data held by the service provider on the secure server.

The Commissioner was satisfied that the facial images and faceprints were 'biometric information' and 'sensitive information' under the Privacy Act. This means that 7-Eleven was required, under APP 3.3, to obtain consent from the individual for collection, and that the collection must be reasonably necessary for one or more of 7-Eleven's functions or activities (unless an exception applies).

Consent was not given: The Commissioner found no evidence that individuals expressly consented to the collection of their facial images or faceprints. Although notices were displayed and information was included in 7-Eleven's privacy policy on its website, the Commissioner found that consent could not be implied as the notices were deficient. The Commissioner was not satisfied that the use of the tablet unambiguously indicated an individual's agreement to the collection where no information was provided on or in the vicinity of the tablet. The notices were unclear and the privacy policy did not link the collection of photographic or biometric information to the use of in-store 'feedback kiosks'.

Consent cannot be inferred from the privacy policy: The Commissioner held that even if a privacy policy were comprehensive, consent could not be inferred from the existence of a privacy policy, as it was not current and specific to the circumstances of collection. The Commissioner held that where an entity intends to collect sensitive information from its customers, a request for consent should:

- clearly identify the kind of information to be collected, the recipient entities, and the purpose of the collection
- be sought expressly and separately from a privacy policy at a current point in time
- be fully informed and freely given.

Collection was not reasonably necessary for the functions or activities: While the Commissioner accepted that implementing systems to understand and improve customers' in-store experience is a legitimate function or activity, the Commissioner was not satisfied that 7-Eleven had justified that collecting its customers' sensitive biometric information was reasonably necessary.

The Commissioner found the risks associated with the collection of such information were not proportional to the function or activity of understanding and improving customers' in-store experience, finding that at most the collection was helpful or convenient.

Inadequate notice was given: The Commissioner found that 7-Eleven did not inform individuals about the fact and circumstances of collection of facial images and faceprints, as required by APP 5.2(b). The Commissioner held that 7-Eleven should have provided a more detailed collection notice specifying the purposes of collection of the images, and outlining that analysis would be undertaken using facial recognition technology to collect faceprints. This notice should have been on or in the vicinity of the tablet screen, and should have been provided before the first facial image was captured.

Remedy: The Commissioner made a declaration requiring the respondent not to repeat or continue the conduct, and to destroy, or cause to be destroyed, all faceprints it collected through the customer feedback mechanism. The Commissioner also required the respondent to provide written confirmation to the OAIC when it had complied with this declaration.

Lessons: This determination is a good reminder of the dangers of trying to infer consent from a privacy policy or privacy notice, and the need for the personal information collected to be proportionate to the purpose for which it is collected.

▶ Scraping biometric information from the internet ruled to be breach of privacy: *Commissioner-initiated investigation into Clearview AI, Inc. [2021] AICmr 54*

Following a joint investigation by the OAIC and the UK Information Commissioner's Office, the Commissioner found that Clearview AI, Inc. breached the Privacy Act by scraping biometric information from the internet (social media platforms and other publicly available websites) and disclosing it through a facial recognition tool.

Collection was without consent: The Commissioner found Clearview AI had breached APP 3.3 because, by scraping biometric information from the internet, it was collecting sensitive information without consent.

Collection was by unfair means: Clearview AI had breached APP 3.5 because it collected personal information by unfair means. In reaching this conclusion, the Commissioner had regard to the kind of information collected by Clearview AI and Clearview AI's commercial purposes. The Commissioner also considered the fact that collection was covert, meaning that the vast majority of individuals would not have been aware or had any reasonable expectation that their scraped images had been collected. In the circumstances, the Commissioner did not accept that the impact on individuals' privacy was necessary, legitimate and proportionate, having regard to any public interest benefit of the facial recognition tool (i.e. for potential law enforcement objectives).

Failure to notify of the collection: Clearview AI had breached APP 5 by failing to take reasonable steps to notify individuals of the collection of personal information. In making this determination, the Commissioner had regard to Clearview AI's Data Policy and Privacy Policies, but considered that these documents were deficient as they contained only limited information about the circumstances of collection and did not explain the method of collection (i.e. automated scraping).

Failure to ensure the accuracy of the information: The Commissioner found that Clearview AI had also breached APP 10 by not taking reasonable steps to ensure that the personal information it disclosed was accurate. In making this determination, the Commissioner had regard to public claims made by Clearview AI, its use for law enforcement purposes and limitations on accuracy testing conducted by Clearview AI.

Failure to take reasonable steps to ensure compliance with the APPs: Lastly, the Commissioner also found that Clearview AI had breached APP 1.2 by not taking reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs. In reaching this view, the Commissioner had regard to a range of matters, including:

- the fact that there was no evidence to suggest that Clearview AI took proactive steps to identify when information it previously collected was no longer public
- there was no evidence Clearview AI conducted a systematic assessment of the measures and controls that should be implemented to identify and mitigate the risks associated with its facial recognition tool.

Remedy: The determination ordered Clearview AI to cease collecting facial images and biometric templates from individuals in Australia, and to destroy existing images and templates collected from Australia.

Lessons: This determination is a timely reminder of the fact that the obligations in the APPs can apply even in circumstances where personal information may have been obtained from publicly available sources. Clearview AI has sought review of the Commissioner's decision in the Administrative Appeals Tribunal.

▶ Information Commissioner rules Amazon disclosure of self-publisher personal information unauthorised: *'XU' and Amazon Australia Services Inc [2021] AICmr 42* (30 August 2021)

The complainant published a book on Amazon Australia Services Inc. (Amazon) via self-publishing services which Amazon provided. A third party complained to Amazon and Amazon suspended the sale of the book.

The Information Commissioner found that Amazon breached APP 6 by disclosing the complainant's personal information to the third party. Amazon could not show that the disclosure was permitted under APP 6.2(a) as it was disclosed for an unrelated secondary purpose (to provide the third party with the complainant's contact

information so they could contact the complainant directly to resolve the dispute), or that disclosure could be reasonably expected. The Commissioner also found the disclosure was not permitted under APP 6.2(c) because while Amazon had reason to suspect unlawful activity, it had not substantiated a reasonable basis for the belief that disclosure was *necessary* for appropriate action to be taken.

Similarly, Amazon could not show that disclosure to the third party was reasonably necessary for the third party to establish or exercise a legal claim to defamation. Significantly, the third party had not raised the possibility of commencing legal proceedings, and had not requested the complainant's personal information in their complaint to Amazon.

Remedy: The Commissioner declared that Amazon interfered with the complainant's privacy, and must not repeat or continue such conduct. The Commissioner also awarded the complainant damages of $3,000 for stress, humiliation and feelings of anxiety with attendance at counselling.

Lessons: This decision is a good illustration of the matters an APP entity will need to satisfy itself of, and the thresholds it will need to meet, in order to establish that a permitted general situation exists and the exception in APP 6.2(c) of the Privacy Act applies.

▶ Disclosure of CCTV footage to investigate theft not breach of privacy: *'XO' and 'XP', 'XQ' [2021] AICmr 37* (9 July 2021)

The complainant was an employee of a retail store. The complainant's manager approached Priceline Pharmacy Camden (Priceline) and asked to check its CCTV to see whether an individual wearing their store's uniform had stolen an item. The manager attended Priceline to review the CCTV footage and took a recording of it on their phone. Later, the complainant's manager showed the complainant the CCTV footage and terminated their employment.

The complainant claimed Priceline breached APP 6 and APP 11 by disclosing their personal information to their employer and by allowing their employer to record the CCTV footage.

The Commissioner found that Priceline did not breach APP 6 because the purpose of disclosing the CCTV footage to the complainant's manager was to investigate an alleged incident of theft, and this was the also primary purpose of collection.

In considering APP 11, the Commissioner was satisfied that Priceline did not permit the complainant's manager to record the CCTV footage on their phone. The Commissioner acknowledged that it was not reasonable for an APP entity to anticipate and prevent all possible circumstances of unauthorised access and concluded that the complainant's manager recording the CCTV footage was not something that was reasonably foreseeable in the circumstances.

Remedy: In the absence of a breach, the Commissioner assigned no remedy.

Lessons: This decision demonstrates that an APP entity need only take steps to guard personal information against unauthorised access which is reasonably foreseeable.

▶ Information Commissioner requires Uber to address deficiencies in security practices and processes and data breach responses: *Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. [2021] AICmr 34* (30 June 2021)

In 2016, personal information stored by Uber Technologies, Inc. (UTI) in a cloud-based system, Amazon Web Services Simple Storage Service (AWS SSS), was subject to a cyberattack (the Data Breach). The files in the AWS SSS were backup files created and stored outside of UTI's usual processes, and were not encrypted. The attackers had gained access to a private UTI repository on 'Github' and identified an active AWS credential in one of the repositories. The attackers used this credential to access and download files related to approximately 1.2 million Australian accounts.

UTI became aware of the unauthorised access and downloading through an anonymous email from the attackers on 14 November 2016. Uber B.V. (UBV) was not notified of the Data Breach until 4 November 2017.

From 21 November 2017, Uber contacted drivers with driver's licence numbers included in the downloaded files but did not notify any individuals who had been impacted by the Data Breach who used the app solely as riders.

The Commissioner commenced an investigation of whether UTI and UBV (collectively 'Uber') had complied with APP 1.2, APP 11.1 and APP 11.2.

APP 11.1: The Commissioner found there were deficiencies in Uber's security processes and practices that ought to have been addressed by:

- implementing multi-factor authentication
- having written policies requiring employees to rotate access keys on a regular basis and to not make fundamental access keys available in plain text
- adopting and implementing a policy to encrypt backup files
- operationalising these policies through regular employee training.

Ultimately, the Commissioner found that Uber failed to take reasonable steps to protect personal information from unauthorised access, in breach of APP 11.1.

APP 11.2: The Privacy Commissioner also found that the following steps were reasonable under APP 11.2 and should have been taken by Uber to destroy or de-identify the personal information when it was no longer needed for a permissible purpose under the APPs:

- adopting and implementing policies and procedures to:
  - identify whether manually created backup files containing personal information were needed
  - ensure that reasonable steps were taken to delete or de-identify any backup files that we no longer needed
- operationalising the policies and procedures by requiring regular and appropriate training of employees, and implementing processes to monitor compliance.

APP 1.2: The Commissioner accepted that Uber had incident response plans in place to deal with data breaches. However, she found that it would have also been reasonable for Uber to have clear processes for how assessments should occur or for determining whether, when, and how Uber would notify impacted individuals.

The Commissioner found that UBV could have taken steps to ensure that UTI was complying with its obligations under the data processing agreement between the 2 entities on an ongoing basis. For example, UBV could have conducted independent assessments to confirm that UTI was promptly notifying it about any data breaches.

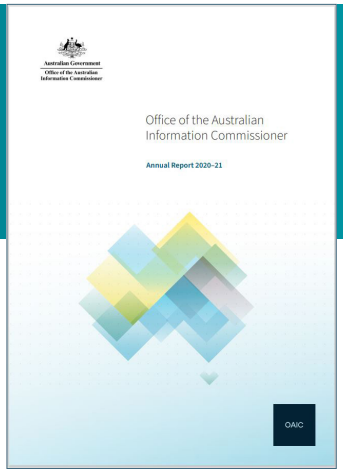
Remedy: The Commissioner made a declaration that Uber must not repeat the acts and practices which caused it to breach the APPs. In particular, Uber was required to take a range of steps to help ensure the conduct would not be repeated, including:

- updating its policies and information security program
- developing an incident response plan
- engaging an independent expert within 3 months of the determination, to prepare a written report to specify whether the necessary policies and procedures had been prepared and implemented
- providing the OAIC with the written reports to confirm that all actions had been completed.

Lessons: This decision sets out a number of practical steps which APP entities can take to ensure they adequately protect the personal information they hold. It highlights the need for APP entities to have clear, practical and well-documented policies and procedures in place and demonstrates the important role which regular monitoring can have (both in terms of assessing APP compliance but also the practical application of policies and procedures).

FOI UPDATE

Office of the Australian Information Commmissioner (OAIC) Annual Report 2020–21



On 21 October 2021, the OAIC released its 2020–21 Annual Report. The Annual Report provides statistical summaries of the privacy and FOI activities of the OAIC and across the Commonwealth.

The number of FOI requests across the Commonwealth in 2021–21 dropped by 16%. Other interesting statistics from 2020–21 include:

- **Requests received:** There were 34,797 FOI requests received (16% fewer than in 2019–20).
- **Personal information requests:** There were 20% fewer FOI requests for personal information overall compared to 2019–20. The OAIC attributes this to the increased use of administrative access schemes.
- **Transfer and withdrawal of requests:** Fewer FOI requests were transferred between agencies (41% less than in 2019–20). There was also a decrease in the number of FOI requests withdrawn by applicants (32% fewer than in 2019–20).
- **Most used exemption:** Perhaps unsurprisingly, the exemption in s 47F (personal privacy) remained the most commonly claimed exemption, comprising 38% of all exemptions applied in FOI decisions in 2020–21, followed by s 47E (operations of agencies).
- **Practical refusal:** 3,143 notices of intention to refuse a request for a practical refusal reason were issued in 2020–21, 17% fewer than the previous financial year. 48% of the FOI requests subject to an intention to refuse a request were subsequently refused or withdrawn.
- **Timeliness of decision making:** 77% of all FOI requests determined in 2020–21 were processed within the applicable statutory time period.
- **Charges:** Agencies notified a total of $247,572 in charges with respect to 738 FOI requests, but collected only $81,353 (due to the discretion in s 29 of the FOI Act to not impose the whole charge and because applicants sometimes withdraw a request to avoid paying the notified charge).
- **Review:** There were 1,026 applications for internal review received (up 9% from 2019–20), of which 51% affirmed the original decision. 1,224 applications for Information Commissioner review were received (up 15% from 2019–20).
- 54 decisions were made by the Information Commissioner under s 55K of the FOI Act. Of these:
  - 25 affirmed the decision under review (46%)
  - 22 set aside the reviewable decision (41%)
  - 7 decisions were varied (13%).

The full 2020–21 OAIC Annual Report can be downloaded from the OAIC's website.

FOI CASE STUDIES

▶ 'The Administrative Appeals Tribunal (AAT) rules documents of National Cabinet, not within FOI Cabinet exemption, are not expected to cause damage to relationship with States and Territories: *Patrick and Secretary, Department of Prime Minister and Cabinet [2021] AATA 2719* (5 August 2021)

The applicant made 2 FOI requests seeking access to:

- documents that outline/describe the rules that the National Cabinet is bound by
- 'All meeting notes/minutes taken from the meeting of the National Cabinet on 29 May 2020'.

Official records of the Cabinet and a committee of the Cabinet are exempt from release under s 34(1)(b) of the FOI Act.

On 8 and 10 August 2020 Department decision-makers decided to refuse access to a total of 6 minutes of National Cabinet meeting on the basis they were exempt as official records of a Cabinet committee.

The Information Commissioner exercised her discretion under s 54W(b) of the FOI Act to determine that the interests of the administration of the FOI Act made it desirable for the decisions on these FOI requests be considered by the AAT.

On 5 August 2021, Justice White decided:

- The National Cabinet is not a 'committee of the Cabinet' within the meaning of the FOI Act. As a result, National Cabinet minutes were not official records of 'a committee of the Cabinet' and were not exempt from release under s 34(1)(b) of the FOI Act.
- Considering the content and nature of the particular National Cabinet minutes, none of them were documents whose disclosure 'would, or could reasonably be expected to, cause damage to relations between the Commonwealth and a State' under s 47B(a) of the FOI Act.

Agencies who receive a request which captures documents relating to National Cabinet should consult with the Department of the Prime Minister and Cabinet's FOI team before making any decisions in response to the request.

▶ The Administrative Appeals Tribunal (AAT) sets aside 2 Information Commissioner practical refusal reason decisions

In 2 recent decisions involving Services Australia – *Chief Executive Officer, Services Australia and Cambridge [2021] AATA 1142* (5 May 2021) and *Chief Executive Officer, Services Australia and Urquhart [2021] AATA 1407* (19 May 2021) – the AAT set aside 2 decisions of the Information Commissioner that a practical refusal reason did not exist:

- In *Cambridge*, the AAT set aside the Information Commissioner's decision and found that a practical refusal reason under s 24AA(1)(a) of the FOI Act existed. The AAT was satisfied that the work involved in processing the request – estimated at 88.5 hours to provide documents that had already been provided under administrative access – was not reasonable and would substantially and unreasonably divert the resources of Services Australia from its other operations. Other operations, in this case, included the processing of other requests for access under the FOI Act.
- In *Urquhart*, the question was whether a practical refusal reason existed to refuse access to the requested documents pursuant to section 24(1)(b) of the FOI Act and whether Services Australia undertook a request consultation process as per section 24AB of the FOI Act. The AAT set aside the Information Commissioner's decision and found that the request, estimated to involve 118.51 hours processing time, would involve a substantial and unreasonable diversion of resources, such that a practical refusal reason existed under s 24AA(1)(a) of the FOI Act. The AAT also found that Services Australia had complied with the consultation requirements of s 24AB(2). The decision contains a succinct summary of the factors the AAT considered in reaching this conclusion.

▶ Private legal documents stored on Department system found to be exempt under s 42:
'YE' and Department of Defence [2021] AICmr 58 (19 October 2021)

The Acting FOI Commissioner found that documents concerning a private legal matter between a departmental officer and the applicant were exempt under s 42 of the FOI Act. The Commissioner found the documents were in the possession of the Department of Defence (the Department) and within scope of the FOI request because the officer stored the documents on the Department's email system. However, storing the documents on the Department's email system did not constitute waiver of privilege, nor did the fact the documents were identified by the Department in response to the FOI request.

The Commissioner's determination is a useful reminder that private documents stored on Commonwealth departments' and agencies' IT systems can fall within the scope of FOI requests.

▶ Agency access grant decision upheld following third party review:
'XY' and Torres Strait Regional Authority [2021] AICmr 46 (10 September 2021)

The FOI applicant requested access to copies of all communication (emails, letters and SMS) sent to and from a third party and the chair of the agency. The third party was consulted under ss 27 and 27A of the FOI Act. Over the third party's objections, TSRA decided to grant access in full to 62 documents, exempt 145 documents in part and exempt 62 documents in full.

Disclosure of publicly known association would not be an unreasonable disclosure of personal information

The Acting FOI Commissioner did not accept the third party's submission that disclosing their name and general information relating to their activities in association with the agency would be an unreasonable disclosure of that personal information. This was because the third party's employment associations were well known and in the public domain.

Disclosure of publicly known business information would not have an unreasonable adverse effect

The Acting FOI Commissioner considered that the information in the documents would only reveal the third party's publicly known associations with the agency, the disclosure of which would not unreasonably affect their business or professional affairs.

▶ Security classifications applied to documents relevant but not determinative:
Rex Patrick and Department of Defence [2021] AICmr 39 (17 August 2021)

The applicant sought access to a document relating to the docking of the Collins Class Submarines. The Acting FOI Commissioner affirmed the Department of Defence's s 33(a)(i) claims, having regard to evidence given by the Inspector-General of Intelligence and Security (IGIS).

This is a useful reminder that the IGIS must be asked to give evidence before the Commissioner can determine that a document is not an exempt document under s 33: see s 55ZB of the FOI Act. The decision also reinforces the notion that while a protective marking or security classification applied to a document may be relevant, it will not be determinative of whether a document is exempt. Instead, regard should be had to the potential damage that may flow from the release of the document

---

Commissioner addresses approach to agency consultation about edited copies of documents:

'XE' and Australian Electoral Commission [2021] AICmr 20 (4 June 2021)

The applicant sought access to documents relating to the membership of the 'Stop Selling Australia' party.

In making its decision, the Australian Electoral Commission (AEC) had made an 'offer' to the applicant regarding giving access to edited copies of documents. The AEC imposed a time limit within which the applicant could 'accept' the offer, and the notice of decision indicated that rejecting the 'offer' would lead to access being refused. The Commissioner noted that in making this 'offer' to the applicant, the notice of decision sought to confirm whether the applicant would decline access to edited copies for the purpose of s 22(1)(d) of the FOI Act. Expressing the provision in this way (i.e. as an 'offer' which the applicant was required to either accept or reject) resulted in confusion and did not accord with the purpose of s 22 of the FOI Act.

This decision serves as a useful reminder of the importance of ensuring all communications to FOI applicants are clear and explain provisions of the FOI Act in a manner which is consistent with their purpose.

Section 37(2)(b) – Commissioner considers lawful methods and procedures in 2 recent decisions

The Information Commissioner and Acting FOI Commissioner have affirmed s 37(2)(b) exemption claims (lawful methods and procedures) in 2 recent review decisions: *'XD' and Australian Securities and Investments Commission [2021] AICmr 19* (4 June 2021) and *'XR' and Department of Home Affairs [2021] AICmr 38* (17 August 2021). This continues a line of cases upholding the exemption of material that would disclose an investigating agency's methods and procedures for initial assessment processes as to whether to proceed to investigate or intervene.

In both cases, the Commissioners were satisfied that:

- the requested documents would disclose the factors considered in assessing whether to take regulatory action, which were not merely routine methods and not generally known to the public
- disclosure could reasonably be expected to enable individuals to tailor their activities to evade scrutiny, which would be reasonably likely to prejudice the effectiveness of those methods and procedures.

The Commissioners explained that the lawful methods and procedures exemption requires the satisfaction of 2 factors:

- first, a reasonable expectation that a document will disclose a method or procedure
- second, a reasonable expectation, or a real risk of, prejudice to the effectiveness of that investigative method or procedure.

OTHER MATTERS

AGS Legal training

FOI and Privacy courses – 2022

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

MARCH				
Online	Tuesday 8	10:30 am – 2:30 pm	Introduction to privacy – Sessions 1 & 2	Register here
Online	Wednesday 9	10:30 am – 2:30 pm	Introduction to privacy – Sessions 3 & 4	
Canberra	Monday 21	9 am – 4:30 pm	Introduction to FOI	Register here
APRIL				
Online	Thursday 7	10:30 am – 2:30 pm	Practical privacy – Sessions 1 & 2	Register here
Online	Friday 8	10:30 am – 2:30 pm	Practical privacy – Sessions 3 & 4	
Canberra	Wednesday 27	9 am – 4:30 pm	FOI next steps	Register here
MAY				
Online	Tuesday 3	10:30 am – 12:30 pm	Managing Privacy risks	Register here
Canberra	Wednesday 4	9 am – 4:30 pm	FOI exemptions	Register here
JUNE				
Online	Wednesday 8	9 – 11 am	FOI exemptions and Decision-making – Session 1	Register here
Online	Thursday 9	9 – 11 am	FOI exemptions and Decision-making – Session 2	

To view the course outline, visit AGS website, Training courses.

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

CONTACTS FOR

Information Law

Information Law Team Leader

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

Specialist FOI advisers 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

Ned Jackson
Lawyer
T 03 9242 1245
ned.jackson@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

Felicia Nevins
Senior Lawyer
T 02 6253 7123
felicia.nevins@ags.gov.au

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

Madhav Fisher
Lawyer
T 02 6253 7225
madhav.fisher@ags.gov.au

Lauren Lai*
Lawyer
T 02 6253 7407
lauren.lai@ags.gov.au
*currently doing Royal Commission work

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
*on long leave