FOI & PRIVACY INFORMATION LAW UPDATE

FOI & Privacy news for the public sector

Our very first virtual FOI & Privacy Practitioners forum!

As we can't host you at our regular forum, we thought we should deliver the latest developments in Freedom of Information (FOI) and Privacy law (minus the morning tea) straight to your inbox.

We are keen to email our clients a regular Information Law update, along with occasional 'breaking news' updates about significant developments in Information Law.

Email Jo Hodge at agsclientservices@ags.gov.au if you have suggestions for the types of content you would like covered, and how often you would like to hear from us. Information about how to subscribe/unsubscribe can be found below.

We wish all our clients the best during these unprecedented challenging times.

CONTENTS

- **Privacy and FOI in the time of COVID-19** **2**
- **How are you going? Share your experiences and ideas** **3**
- **PRIVACY UPDATE** **3**
  - First ever civil penalty proceedings commenced against Facebook **3**
  - Notifiable data breaches 6 month statistics report 3
  - Health provider Data Breach Action Plan 4
  - Privacy (Australian Bushfires Disaster) Emergency Declaration (No. 1) 2020 4
  - Consumer Data Right – Privacy Safeguard Guidelines released 4
  - Government response to Digital Platforms Inquiry 4
  - ANAO focus on cyber security strategies 5
  - Recent privacy assessments by the OAIC 5
  - APP are not directly actionable in Court 5
  - Privacy Awareness Week 5
- **FREEDOM OF INFORMATION UPDATE** **6**
  - FOI decisions in 2019 – themes and observations 6
  - Key FOI cases in 2019 and 2020 8
- **CONTACT US** **9**

Privacy and FOI in the time of COVID-19

The Office of the Australian Information Commissioner (OAIC) has developed privacy guidance to help Australian Government agencies keep workplaces safe and handle personal information appropriately when responding to the unprecedented challenges presented by COVID-19. This includes:

- using and disclosing individuals' personal information, including sensitive health information, on a 'need-to-know' basis
- only collecting, using or disclosing the minimum amount of personal information reasonably necessary to prevent or manage COVID-19
- advising staff about how their personal information will be handled in responding to any potential or confirmed COVID-19 cases in the workplace
- taking reasonable steps to keep personal information secure, including where employees are working remotely.

The OAIC has also provided useful information about meeting statutory timeframes for FOI requests during this time including:

- encouraging use of self-service or administrative access schemes
- updating your agency's FOI page and/or FOI request form to explain the impact of the COVID-19 pandemic on the agency's ability to process FOI requests, which may require the agency to seek an applicant's agreement to extend the processing timeframe
- seeking agreement from the FOI applicant to an extension of time under s 15AA of the *Freedom of Information Act 1982* (Cth) (FOI Act) as part of the acknowledgment letter
- if the applicant does not agree to an extension of time, applying to the OAIC for an extension of time under ss 15AB, 15AC or 54D of the FOI Act using the OAIC's SmartForm.

The Information Commissioner and State and Territory Privacy Commissioners and Ombudsmen have formed a national COVID-19 Privacy team and recommend that agencies and organisations consider conducting short form Privacy Impact Assessments in respect of COVID-19 matters or projects to ensure proper handling of personal information.

In line with the APSC's Circular 2020/3: COVID-19 Remote working and evolving work arrangements many agencies are transitioning large parts of their workforce to remote working arrangements. This raises privacy challenges as staff engage via new online video conferencing and communication platforms. The ACSC has helpfully published guidance on how to select a secure web conferencing solution.

The Government has introduced a Coronavirus App to communicate with the public about COVID-19 and for members of the public voluntarily to provide information about whether and why they are self-isolating.

AGS is assisting the Government with a range of COVID-19 projects and is available to assist with conducting urgent Privacy Impact Assessments or to advise on how to minimise privacy risks. We can also assist agencies in navigating extensions of time for FOI requests.

How are you going? Share your experiences and ideas

We're interested to hear about the impact on your privacy and FOI teams from the COVID-19 epidemic and measures. We have created a Slido event with 'rooms' for FOI and privacy with a survey about your experiences to date. You can also ask questions and provide information to each other in the Q&A tab in each room.

You don't have to give us your name or agency information to engage on Slido. Unless you choose to add your name or other information, the default is for you to be anonymous. We will review the survey results and report back any meaningful trends with the next news update. We won't identify individuals or agencies in these results. See below for more information about Slido and your privacy.

Use the following links and event codes to get started.

Privacy Chats https://app.sli.do/event/zae4kjfu Event code: PrivacyChats

FOI Chats https://app.sli.do/event/qqzlkmd2 Event code: FOIChats

PRIVACY UPDATE

First ever civil penalty proceedings commenced against Facebook

The Australian Information Commissioner has lodged proceedings against Facebook in the Federal Court alleging the social media platform has committed serious and/or repeated interferences with privacy in contravention of Australian privacy law.

This is the first time civil penalty proceedings have been commenced under the *Privacy Act 1988* (Cth) (Privacy Act). The statement of claim (available on the OAIC's website) alleges that, from March 2014 to May 2015, Facebook:

- disclosed the personal information of Australian Facebook users to the *This Is Your Digital Life* app, in breach of Australian Privacy Principle (**APP**) 6
- did not take reasonable steps during this period to protect its users' personal information from unauthorised disclosure, in breach of APP 11.

AGS is acting for the AIC in this matter.

Notifiable data breaches 6 month statistics report

The OAIC recently released its Notifiable Data Breaches Report: July–December 2019. Key statistics include:

- 537 data breaches were reported to the OAIC, up from 460 in the previous 6 months (19% increase)
- malicious or criminal attacks (including cyber incidents) remain the leading cause of data breaches, accounting for 64% of all notifications
- data breaches resulting from human error account for 32% of all breaches, down from 34% in the last reporting period
- the health sector is again the highest reporting sector, notifying 22% of all breaches (with 43% of breaches caused by human error).

The report includes useful information about notifying individuals affected by a breach, the problems caused by using email inboxes for primary storage of information, and how to minimise the risks of email as a communication method.

It is a timely reminder to agencies of the importance of training all staff in privacy and IT security to reduce the likelihood of a breach, and to use and regularly test your data breach response plans!

▶ Health provider Data Breach Action Plan

A four-step Data Breach Action Plan aims to help health service providers contain and manage a data breach involving personal information, including the My Health Record system. The plan has been developed by the OAIC, Australian Digital Health Agency, Australian Cyber Security Centre and Services Australia.

Step 1 – **Contain** — Take action to contain the breach

Step 2 – **Evaluate** — Assess any risks associated with the breach

Step 3 – **Notify —** Contact all relevant parties

Step 4 – **Review** — Minimise the likelihood and effects of future data breaches

▶ Privacy (Australian Bushfires Disaster) Emergency Declaration (No. 1) 2020

The Attorney-General made the *Privacy (Australian Bushfires Disaster) Emergency Declaration (No. 1) 2020* in response to bushfires in Australia resulting in death, injury and property damage occurring from August 2019 into 2020. Under the emergency declaration, Part VIA of the Privacy Act allows agencies and organisations to collect, use and disclose personal information about an individual impacted by the bushfires for several permitted purposes that may not otherwise be allowed under the APP. The OAIC has provided information to assist agencies and organisations to understand their obligations until the emergency declaration expires on 20 January 2021.

▶ Consumer Data Right – Privacy Safeguard Guidelines released

The OAIC released the Consumer Data Right Privacy Safeguard Guidelines, which set out how businesses must protect consumers' data under the new Consumer Data Right (CDR). The CDR allows consumers to access particular data about them in a specified transferable form and to direct a business to securely transfer that data to an accredited data recipient so they can compare services. The CDR will first be implemented in the banking sector from July 2020, followed by the energy and telecommunications sectors.

▶ Government response to Digital Platforms Inquiry

The Government released its response and implementation roadmap to the Australian Competition and Consumer Commission (ACCC) Digital Platforms Inquiry. The Inquiry looked at the impact of digital search engines, social media platforms, and digital content aggregators on the state of competition in media and advertising services markets, and called for significant changes to privacy regulation of digital platforms. The Government's response outlines a roadmap for a program of work, including:

- increasing penalties for breaches of privacy
- introducing a binding online Privacy Code (part of the 2019-2020 budget)
- further strengthening of Privacy Act protections, subject to consultation and design of specific measures, as well as conducting a review of the Privacy Act.

ANAO focus on cyber security strategies

The Australian National Audit Office (ANAO) has announced a performance audit of the cyber security strategies of non-Corporate Commonwealth agencies, due to be tabled in November 2020. The audit will assess:

- the effectiveness of the Top Four cyber security risk mitigation strategies implemented by selected entities to meet mandatory requirements under the Protective Security Policy Framework (PSPF)
- whether the Australian Signals Directorate, the Attorney-General's Department and Department of Home Affairs have worked together to improve those entities' implementation of cyber security requirements under the PSPF.

This follows on from the ANAO's audit of the cyber resilience of Government Business Enterprises (GBEs) and Corporate Commonwealth Entities (CCEs), which assessed the effectiveness of the management of cyber security risks by 3 entities.

Recent privacy assessments by the OAIC

The OAIC conducts privacy assessments of APP entities, including Australian Government agencies. An assessment is essentially a 'privacy audit' of how well an agency complies with its privacy obligations. In the past 6 months, the OAIC published findings in relation to 15 privacy assessments (representing a significant increase in assessments by the OAIC), and included:

- an assessment of the information security practices of 4 major telecommunication service providers (Telstra, Vodafone, Optus, TPG) in relation to their handling of personal information under the *Telecommunications (Interception and Access) Act 2015* (Cth)
- an assessment of the Department of Home Affairs' handling of personal information under the Privacy Act. The OAIC's detailed report included recommendations to address the medium level privacy risks identified by the assessment.

APP are not directly actionable in Court

The Federal Court in *Pathmanathan v Healthscope Operations Pty Ltd* [2020] FCA 65 (6 February 2020) confirmed that a breach of the APP is not directly actionable in Court. The Privacy Act provides for complaints about breaches to be made to the Privacy Commissioner who can make a non-binding determination. Determinations can be enforced by the Federal Court or Federal Circuit Court (s 55A Privacy Act).

Privacy Awareness Week

PRIVACY AWARENESS WEEK

Privacy Awareness Week (PAW) is celebrated from **Monday 4 May — Sunday 10 May**. This annual event highlights the importance of protecting personal information. While face-to-face events may not take place this year, agencies can still sign up with the OAIC to be a PAW supporter. PAW is an important event for agencies, and an opportunity to highlight good privacy practice, refresh training for staff, and to consider whether your Privacy Management Plans are up-to-date in line with agency obligations under the Australian Government Agencies Privacy Code.

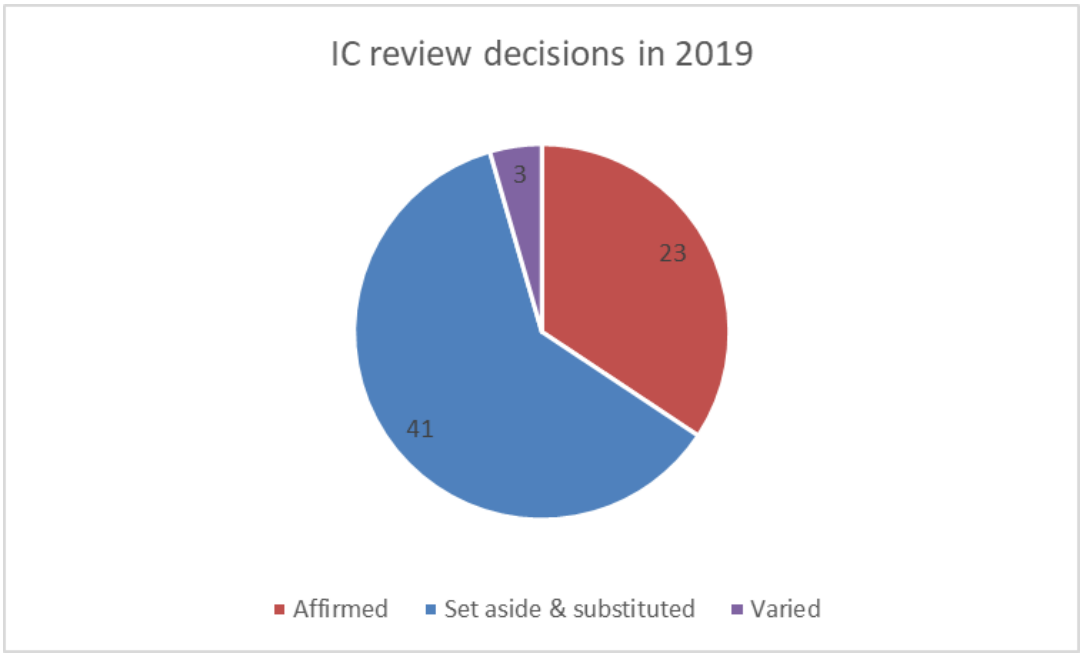
FREEDOM OF INFORMATION UPDATE

FOI decisions in 2019 – themes and observations

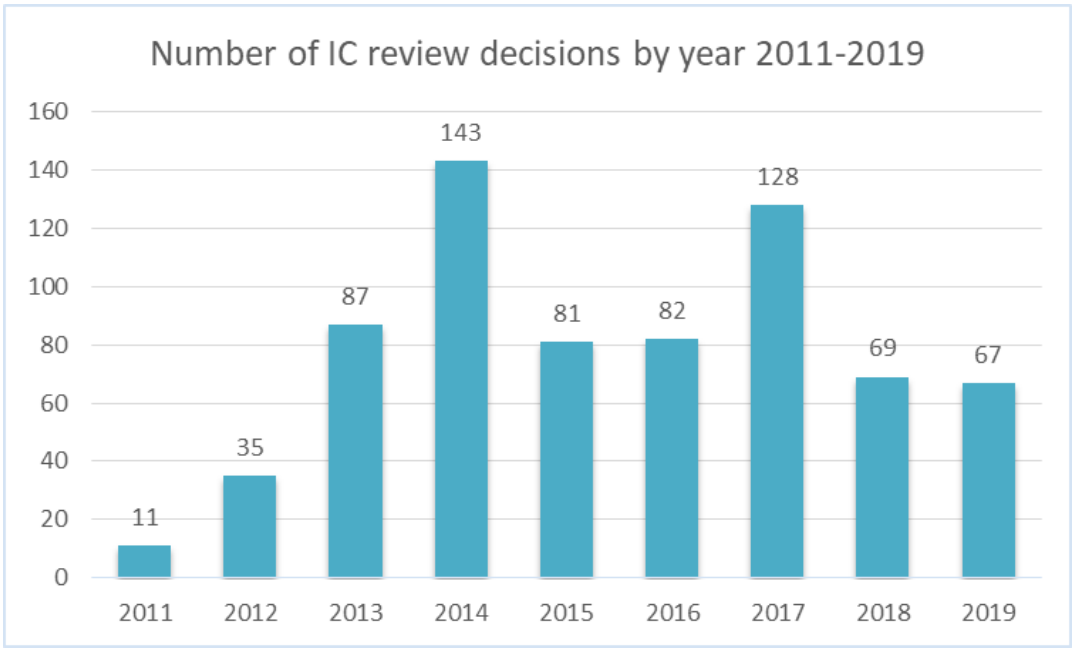
Information Commissioner (IC) review decisions in 2019

In 2019, the IC made 67 review decisions, of which 64 were reviews of access refusal decisions. The other 3 were reviews of access grant decisions. Each of these three involved s 47G business affairs claims, and in each case the agency's decision was affirmed.

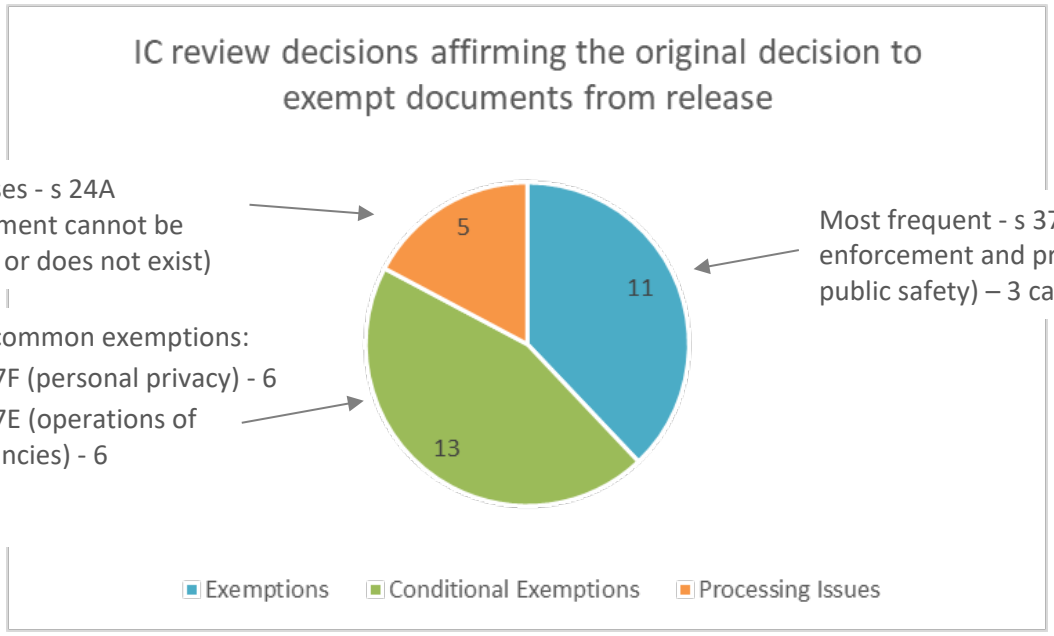
The first chart below shows the breakdown of the decisions affirmed, set aside and substituted, and varied.



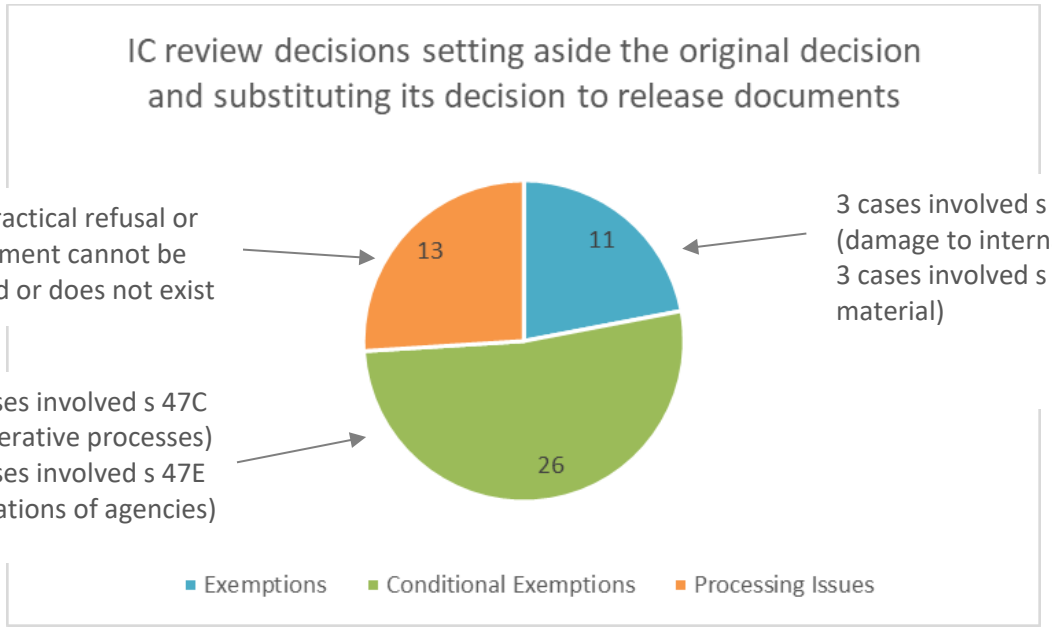
The second chart shows the number of IC review decisions by year from 2011 – 2019. The IC continues to resolve the overwhelming majority of IC review applications by agreement or other means and this might be expected to continue on current numbers (there have been 9 decisions in the first quarter of 2020).



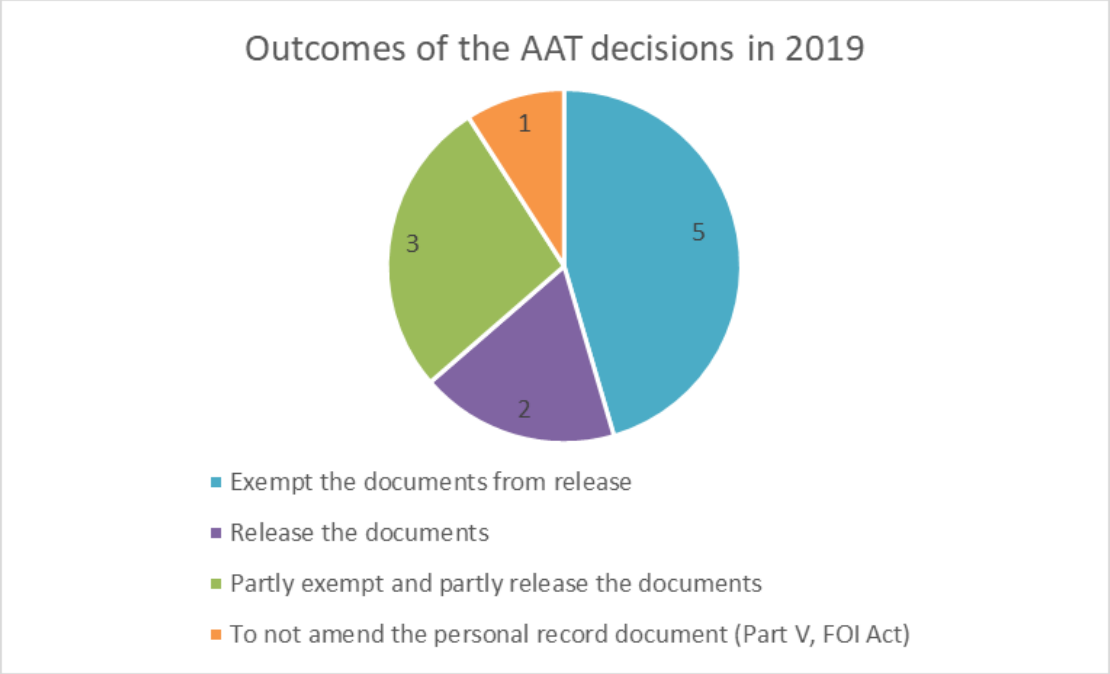
The third chart shows the IC review decisions affirming the decision to exempt documents from release and the breakdown of issues involved. Note that there is some overlap, as some cases involved multiple categories. The information on the side identifies the most common issue in each category.



The fourth chart is the same as the third chart, but for the IC review decisions setting aside the original decision and substituting its decision to release the documents.



AAT review decisions in 2019



▶ Key FOI cases in 2019 and 2020

International relations of the Commonwealth: maintaining an exemption claim under s 33(a)(iii) of the *Freedom of Information Act 1982*

The Tribunal's recent decisions in *Secretary, Department of Prime Minister and Cabinet and Summers (Freedom of information)* [2019] AATA 5537 (20 December 2019) (**Summers**) and *Xenophon and Secretary, Department of Defence (Freedom of information)* [2019] AATA 3667 (20 September 2019) (**Xenophon**) provide useful guidance on the scope of the exemption under s 33(a)(iii) of the FOI Act for documents affecting national security, defence or international relations.

Section 33(a)(iii) of the FOI Act provides that a document is an exempt document if disclosure under the FOI Act would, or could reasonably be expected to, cause damage, to the international relations of the Commonwealth.

Factual background

Summers

Mr Summers sought access to 'all letters sent from the Prime Minister(s) of Australia to Queen Elizabeth II (or her representatives) since 1 January 2013.'

The Department of the Prime Minister and Cabinet (PM&C) refused access to the documents on the grounds that they were documents affecting the international relations of the Commonwealth (s 33(a)(iii)), and that all but 1 of the documents contained information that was deliberative in nature (s 47C).

Xenophon

The Australian Government undertook a Competitive Evaluation Process to select an international partner to design and build the next generation of Australian submarines. As part of the process certain documentation was released to a small number of potential suppliers for them to provide a response. The Government of Japan was a potential supplier, but was ultimately not selected.

Mr Xenophon requested the documents that were provided to the potential suppliers as part of the Competitive Evaluation Process (CEP) documentation suite.

The Department of Defence refused access to the documents on the grounds that they were exempt under s 33(a)(iii).

Tribunal Decisions

In both matters, the Tribunal decided that the documents were exempt in full under s 33(a)(iii). The following key themes emerge from the decisions.

Expectation of confidentiality

In each case the Tribunal determined that the foreign governments in issue had an expectation that relevant information would be kept confidential. The expected damage to international relations flowed, in significant respects, from the predicted negative reactions of foreign governments to a disclosure of information contrary to that expectation of confidence.

In Summers, the Tribunal concluded that communications between the Prime Minister and the Queen are recognised as confidential by long tradition, underpinned by constitutional convention. It relied on the evidence of the Official Secretary to the Governor-General for this point. The Tribunal found that this understanding of confidentiality is so deeply entrenched that releasing the documents would not only damage Australia's relationship with the Queen, but also all 16 Commonwealth realms. This is because the confidentiality is mutually important to all and disclosure would raise concerns that Australia cannot protect confidential documents. Evidence from a senior official of the Department of Foreign Affairs and Trade (DFAT) supported this finding.

In Xenophon, Australia had advised Japan during the CEP process that the documents would be kept confidential. The Tribunal relied on subject matter experts from Defence and from DFAT to confirm that understanding. The Tribunal took into account the evidently sensitive nature of the subject area for the Government of Japan in satisfying itself that it was reasonable to expect damage to flow from disclosure.

In both cases, the finding of an expectation of confidentiality was supported by evidence of consultation undertaken with the foreign authority.

Reasonableness of expectation

The Tribunal also analysed the phrase 'would, or could reasonably be expected to,' confirming that reasonableness relates to the expectation of damage, not to whether the expected damage is itself irrational or unreasonable. In other words, you would not ask whether it is reasonable for the foreign government to react in a particular way to a disclosure, but rather whether it is reasonable to expect the foreign government to react in that way. The test requires more than a mere allegation or possibility of damage: *Re Maher and Attorney-General's Department* (1985) 7 ALD 731 (**Re Maher**) at [742], but does not go so far as to require a probability of damage.

Degree of damage

In Xenophon, the Tribunal noted that 'damage' need not be catastrophic 'in the sense that the relationship is broken or irretrievably weakened for all time.' Damage of some substance is sufficient. In Summers, the Tribunal emphasised that it is not necessary to find loss or damage in monetary terms and referenced Davies J in Re Maher at [742] that damage 'comprehends intangible damage to Australia's reputation.'

Weight of senior deponents' evidence

In making a determination about the damage to international relations, the Tribunal determined that it could, and should, place significant weight on the evidence of senior public servants in the field. In Xenophon, evidence was led from Rear Admiral Greg Sammut as head of the Future Submarines Program and Mr Graham Fletcher, the First Assistant Secretary, North Asia Division, DFAT as a long-serving diplomat with particular expertise regarding Australia's relationship with Japan. In Summers,

Andrew Todd, First Assistant Secretary of the Consular and Crisis Management Division, DFAT and Mark Fraser LVO OAM, Official Secretary to the Governor-General gave evidence. They each had particular expertise in and responsibility for managing Australia's relationship with the Queen and the Royal Household.

The IC grants a vexatious applicant declaration: Services Australia and 'RS' (Freedom of information) [2020] AICmr 6 (24 February 2020)

The IC made a declaration under section 89K(1), FOI Act, that 'RS' (the respondent) was a vexatious applicant on the basis that they had repeatedly engaged in access actions and that the repeated engagement involved an abuse of process.

The terms of the declaration included that Services Australia was not required to consider any further access requests or applications for internal review of an access refusal decision by RS or process any outstanding request or application. As is commonly the case with declarations, the OAIC will also not consider any application by RS for permission to make requests to Services Australia unless the request meets the requirements of s 15, and is not vexatious. A further restriction was also included that the OAIC will not consider any applications for permission made within 90 days of a prior application having been received.

The case involved RS engaging in 122 separate 'access actions' with Services Australia over a period of 28 months and 12 days, comprising:

- 84 requests for access to documents made under s 15 (including 20 requests after the Services Australia applied for the vexatious applicant declaration)
- 14 internal review applications made under s 54B
- 24 applications for IC review made under s 54L.

RS also submitted over 60 external enquiries to Services Australia's FOI team and 7 FOI complaints about Services Australia to the OAIC.

Services Australia applied to the OAIC for a vexatious applicant declaration about RS under s 89K. After being notified of the application, RS sent a total of 59 pieces of correspondence plus attachments to the OAIC. In addition to objections to the validity of the s 89K process, correspondence included:

- nine invoices addressed to particular OAIC officers and Services Australia staff for the respondent's time spent on dealing with their matters before the OAIC provided on 12 separate occasions
- four pamphlets created by the respondent addressing protection of paedophile access supply lines, infant prostitution and the fertility of women provided on 17 separate occasions.

The key issues for the IC were whether RS repeatedly engaged in access actions (s 89L(a)(i)), and if so whether:

- the repeated engagement involved an abuse of process for the access action (s 89L(1)(a)(ii))
- the access actions harassed or intimidated an employee of Services Australia (s 89L(4)(a))
- the access actions unreasonably interfered with the operations of Services Australia (s 89L(4)(b)).

The IC was satisfied that the 122 access actions amounted to a repeated engagement in access actions, which involved an abuse of process for the access actions by harassing employees of Services Australia and unreasonably interfered with Services Australia's operations. The IC therefore declared RS to be a vexatious applicant. The key reasons for the decision were:

- the volume, frequency and repetitive nature of the access actions and FOI-related correspondence
- the content of the access actions and FOI-related correspondence, including requests for personal information of Services Australia employees and inclusion of distressing and offensive content written by RS irrelevant to the processing of the requests

- the tone and language of the access actions and correspondence, which often include derogatory language and allegations targeted at particular Services Australia employees
- the processing burden on Services Australia resulting from the access actions, as the nature and volume of the access actions do not appear to be proportionate to a reasonable exercise of the right to access documents
- RS' refusal and failure to alter dubious conduct after being requested to do so
- RS' apparent use of the FOI Act to prolong separate grievances against Services Australia and particular Services Australia staff.

The IC also found that Services Australia's failure to acknowledge the access requests within 14 days, its decisions to refuse access, and its FOI administration deficiencies, were not sufficient to justify RS' conduct and the extent of the access actions made. The IC particularly noted that RS was unwilling to discuss their access actions and whether they constituted an abuse of process or were manifestly unreasonable.

This is the ninth vexatious applicant declaration made by the IC and fourth such declaration in just over 12 months. This case featured one of the highest numbers of access actions by an applicant.

AGS assisted with this application and frequently works with agencies regarding ways to mitigate the impacts of individuals who make excessive or unproductive use of FOI and other access measures.

CONTACT US

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

Rosie Cham
Lawyer
T 02 6253 7438
rosie.cham@ags.gov.au

Canberra

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

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