Commissioner brief: Committee members

Senator the Hon Sarah Henderson, Chair

Senator for Victoria

Chair of Legal and Constitutional Affairs Legislation Committee

Deputy Chair of Legal and Constitutional Affairs References Committee

Party: Liberal

Webpage: www.sarahhenderson.com.au

Official biography:

Sarah, the oldest of three children of Ann and Michael Henderson, was born and raised in Geelong in a loving, community focused family. She went to school at Sacred Heart College and Geelong College. Her first family home was in Barrabool Rd, Belmont, adjacent to the Barwon River. Childhood summers were spent on the beach at Queenscliff, swimming and sailing, where her grandparents had built a beach house in the 1950s.

Sarah's father, Michael, was a Geelong solicitor, local councillor and mayor. Her mother, Ann, worked for Do Care, Deakin University and the National Trust before serving as the State Member for Geelong from 1992-1999. In her second term, she was Housing and Aboriginal Affairs Minister.

Sarah started her career as a cadet journalist with Channel 7 Melbourne in 1982. After stints at Channel 9 Brisbane and Channel 10 Melbourne as a reporter and presenter, in 1989 Sarah joined the ABC where she worked for *The Investigators* and *7.30 Report* including as its Victorian host. In 1996, she won a prestigious Walkley award for her coverage of the Port Arthur massacre.

In 1998, after obtaining an LL.B (Hons) from Monash University, Sarah turned to the law, joining commercial law firm Allens Arthur Robinson which included a period working for News Corporation in New York. This led to Sarah starting her own media consultancy before taking on various commercial roles as Network Business Manager Programming with Channel 10 Sydney and Legal and Business Affairs Manager with National Indigenous TV.

Sarah lives in Barwon Heads, still close to the Barwon River. Her greatest achievement is her son Jeremy who brings immeasurable joy and pride to her life every day.

Sarah proudly served as the Member for Corangamite from 2013 until May 2019. She was appointed to the Senate by a joint sitting of the Parliament of Victoria on 11 September 2019 to fill the casual vacancy caused by the retirement of Senator the Hon Mitch Fifield. Sarah was officially sworn in as Victoria's newest Liberal Senator on Thursday 12 September 2019.

Enquiries

Received

Types	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22
FOI	2,062	1,931	2,881	2,297	1,824	916
% changed compared prior year		-6%	49%	-20%	-21%	21%
Privacy & Other	16,793	19,407	17,445	14,842	11,647	5367
% changed compared prior year		16%	-10%	-15%	-22%	5%
Total	**18,855**	**21,338**	**20,326**	**17,139**	**13,471**	**6283**

- Enquiries received data includes all matters incoming to OAIC by telephone, written and in person channel.
- YTD FY2021/22 the data includes figures as at 31 December.
- The FY2021/22 percentage measures variance between FY2020/21 (From 1 July to 31 December).

FOI written enquiries closed within 10 days – Target 90%

Time taken to close (Days)	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22
% Enquiries closed in less than 10 days	88%	88%	94%	85%	76%	84%
Number enquiries closed in less than 10 days	509	517	776	654	559	354
% Enquiries closed in more than 10 days	12%	12%	6%	15%	24%	16%
Number enquiries closed in more than 10 days	90	67	49	124	175	69
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Privacy & other written enquiries closed within 10 days – Target 90%

Time taken to close (Days)	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22
% Enquiries closed in less than 10 days	78%	74%	92%	76%	63%	85%
Number enquiries closed in less than 10 days	2,712	3,294	3,703	2,841	3,207	1665
% Enquiries closed in more than 10 days	22%	26%	8%	24%	37%	15%
Number enquiries closed in more than 10 days	766	1,158	341	917	1,885	284
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

OAIC Staffing figures

Total Staff: Overview

Done ←

(As at)	31 December 2021	30 September 2021	28 April 2021	May 2020	May 2019	May 2018	May 2014
FTE	112	127	121	102	84	75	83
ASL	119	121	119	94	86	74	77
Headcount	124	142	136	109	95	91	97

FTE represents an 'as at' figure, whereas the ASL figure represents the average staffing from 1 July - 31 December 2021

Done ←

Funding: FTE

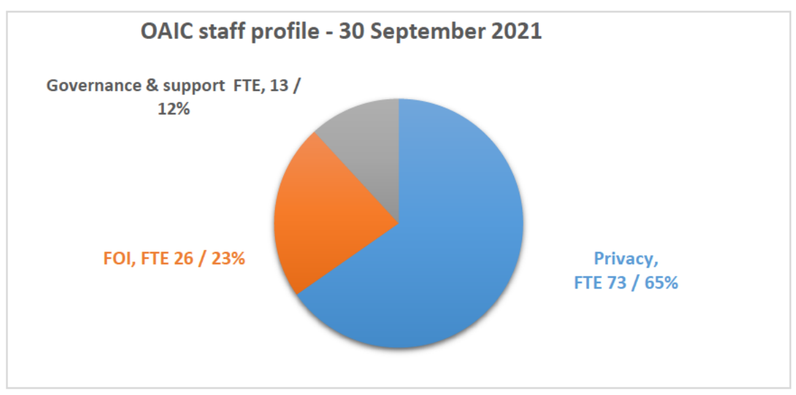
(As at)	31 December 2021	30 September 2021	28 April 2021	May 2020	May 2019	May 2018	May 2014
Budget	127	127	121	102	74	65	67
ADHA MOU	0	0	0	0	10	10	16
Total		**127**	**121**	**102**	**84**	**75**	**83**

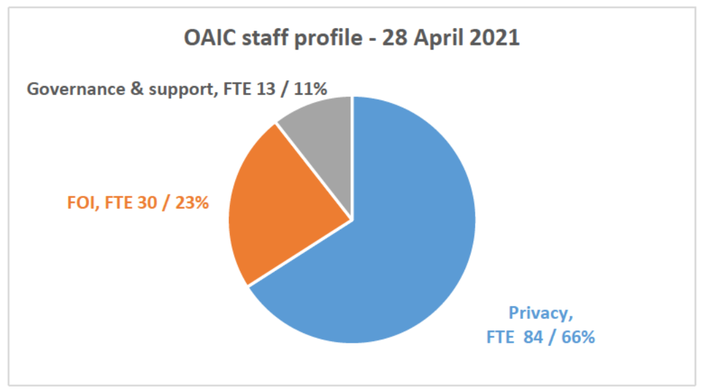
Represents FTE which can be afforded by internal budget

Done ←

Staffing allocation by function (APS staff)

	As at 31 December 2021		As at 30 September 2021	
	APS FTE	%	APS FTE	%
Privacy	73	65%	84	66%
FOI	26	23%	30	23%
Governance & support	13	12%	13	11%
Total	**112**		**127**	

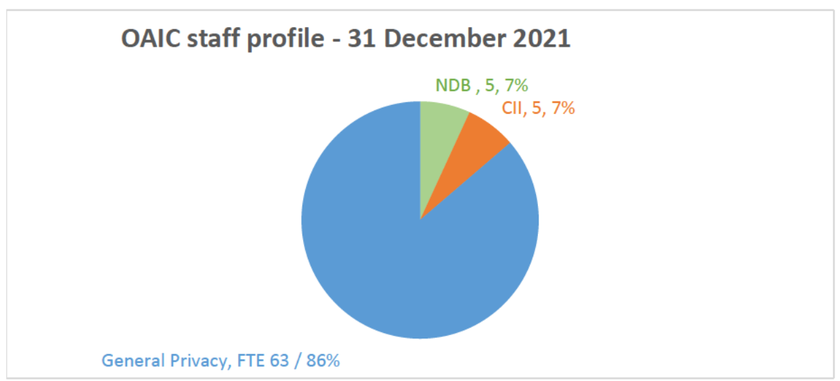


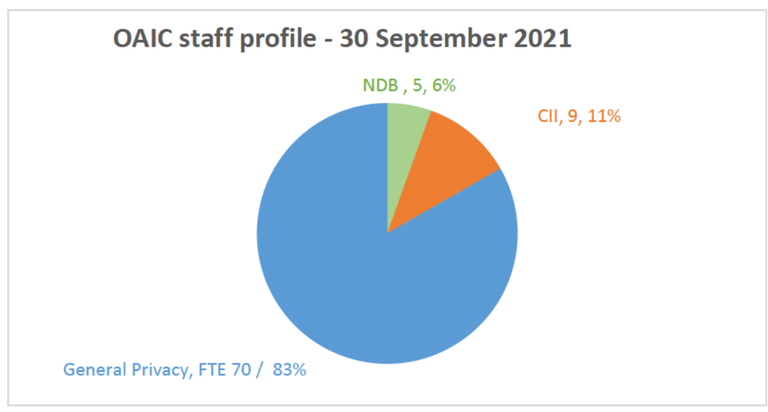


Done ←

CII & NDB allocation:

	As at 31 December 2021		As at 30 September 2021	
	FTE		FTE	%
NDB	5	7%	5	5%
CII	5	7%	9	11%
General Privacy	63	86%	70	83%
	73		**84**	

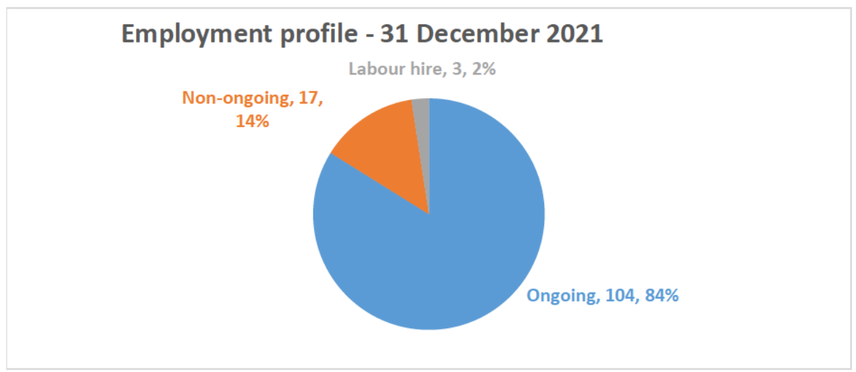


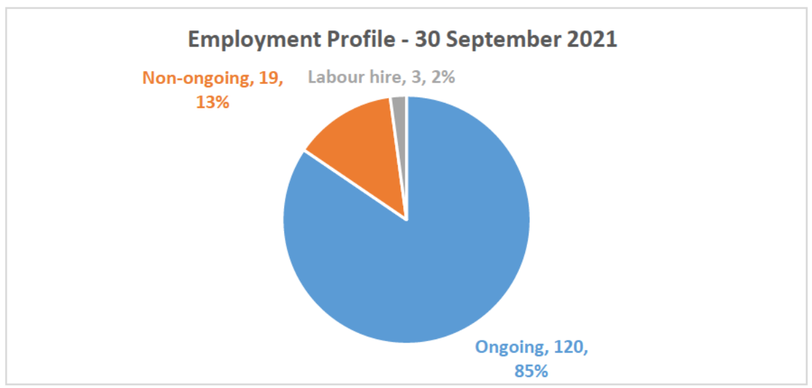


Done ←

Employment type:

	As at 31 December 2021		As at 30 September 2021	
	Headcount		Headcount	%
Ongoing	104	84%	120	85%
Non-ongoing	17	14%	19	13%
Labour hire	3	2%	3	2%
	124		**142**	





Done ←

General staffing details:

(Financial year)	2021/22 (as at 31 December)	2020/21	2019/20	2018/19	2017/18
Positions advertised	9	21	12	15	14
Engagements permanent	13	30	24	20	10
Engagements temporary	4	25	19	8	11
Internal Promotions	8	12	18	16	9
Total	**25**	**67**	**61**	**44**	**30**

(Financial year)	2016/17	2015/16	2014/15
Positions advertised	15	17	10
Engagements permanent	14	24	7
Engagements temporary	6	1	2
Internal Promotions	12	12	5
Total	**32**	**37**	**14**

Turnover: Terminations (APS staff only)

	2021/22 (as at 31 December)	2020/21	2019/20	2018/19	2017/18
Permanent	24	21	17	19	15
Temporary	7	13	9	5	3
Total	**31**	**34**	**26**	**24**	**18**
Turnover % (based on permanent staff cessations)	**23%**	**18%**	**18%**	**24%**	**21%**

	2016/17	2015/16	2014/15
Permanent	11	15	28
Temporary	2	1	3
Total	**13**	**16**	**31**
Turnover % (based on permanent staff cessations)	**13%**	**19%**	**48%**

Leave: Unplanned sick leave per FTE

(Financial year)	2021/22 (as at 31 December)	2020/21	2019/20	2018/19	2017/18
Hours	14.25	47.25	70.43	87.58	77.22
Days	1.9	6.3	9.39	11.68	10.33

(Financial year)	2016/17	2015/16	2014/15
Hours	83.23	83.38	80.71
Days	11.52	11.12	10.76

Ave small agencies: 2.7; APS average: 3.1

Leave: Excess leave (number of staff)

(As at)	2021/22 (as at 31 December)	2020/21	2019/20	2018/19	30/06/2018
Dispute resolution	14	13	0	3	4
Regulation and Strategy	5	2	0	1	2
Operations	5	5	0	2	
Executive	5	2	0	2	1
Total	**29**	**22**	**0**	**8**	**7**

(As at)	30 June 2017	30 June 2016	30 June 2015
Dispute resolution	6	0	0
Regulation and Strategy	3	3	1
Operations			
Executive	1	2	2
Total	**10**	**5**	**3**

Note 1: At present 29 staff are deemed to have excessive leave credits (ie 30+ days). As per OAIC's Enterprise Agreement, the Australian Information Commissioner or delegate may direct an employee to take annual leave within a reasonable period to reduce their accumulated annual to 6 weeks. The reasonable period would not usually be longer than 6 months but in exceptional circumstances may be a longer period. Due to the pandemic, the OAIC Executive has not exercised the discretion to deem officers to be on leave. This is closely monitored to ensure staff are taking appropriate time away from work. Over the new year period, 6 of the 29 staff have reduced their excess leave below 30 days, with 8 further staff with plans in place to reduce their excess throughout February and March 2022.

Commissioner brief: Budget and resourcing February 2022

KEY MESSAGES

- Total appropriation for 2021-22 is $26.730million
- 2021-22 ASL – cap 147; the internal budgeted cap 127; Actual FTE at 31 December 2021 is 111.
- The 2021-22 Budget provided ongoing funding for FOI Commissioner appointment.
- 2021-22 MYEFO provides additional $1.997million for transition of ICT services and Federal Court proceedings. It also provides $0.912 for the expansion of Digital Identity in 2022-23.
- Funding reduces from 1 July 2022 due to terminating measures.

KEY BUDGET NOTES

1 July 2021

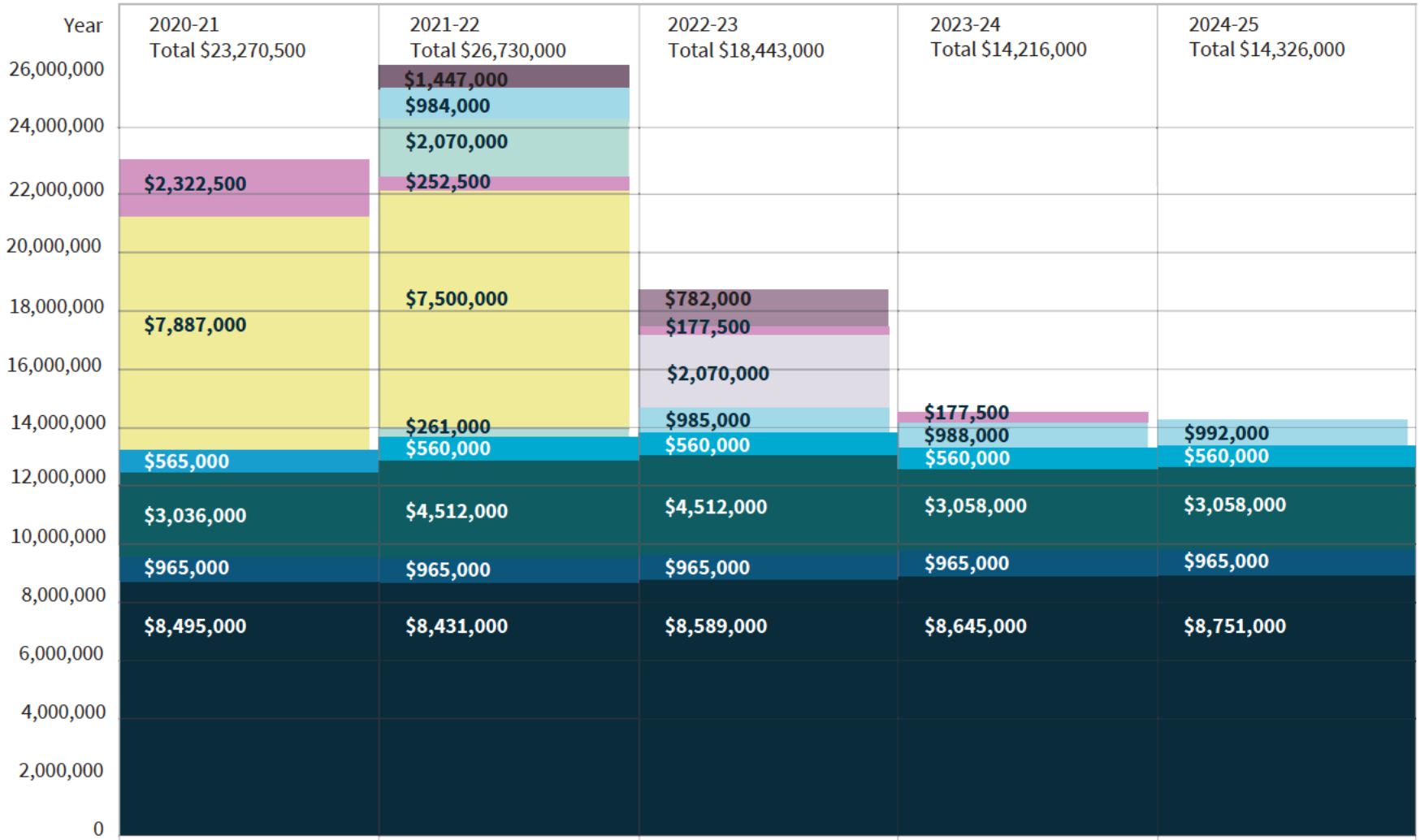
- MYEFO 2021-22 increased revenue by $1.447 million from $25.283million to $26.730million. Total capital revenue increased from nil to $0.550million.

  Funding is for:

  - Transition of ICT shared services [redacted]
  - Federal Court proceedings: [redacted]

- The published PBS includes $150,000 in MOU funding. Actual MOU is $252,500. (Actual figures will be updated in 2022-23 PBS.)
- Total MYEFO published funding is $26.880million including MOU and 147 ASL
- OAIC will seek permission to operate at loss of $1.630million for transition of payroll and finance services to Service Delivery Office. The transition is self-funded.
- The 2021-22 Budget provides $5.951million across five key areas:
  - Transition of ICT shared services [redacted]
  - Federal Court proceedings: [redacted]
  - Freedom of Information: [redacted]
  - Expansion of Consumer Data Right: [redacted]
  - Digital Health: [redacted]

Data showing funding from 2020-21 forward



NB: MOUs

Budget from MOUs is negotiated independently with the relative agencies including ACT, ADHA, PNR, Home Affairs.

Key

- MOU
- My Health Record
- Privacy complaints and social media
- Expanding Digital Identity
- FOI Commissioner & support
- MBS/PBS: Medicare data matching
- Consumer Data Right (ongoing)
- National Security (ongoing)
- Base
- DESE ICT & Legal
- Additional Digital

See over for more detail

Commissioner brief: Performance against MoUs

MOU: ACT Government Provision of Privacy Services

MOU value:

- 2017-18: $177,145.78
- 2018-19: $177,500.00
- 2019-20: $177,500.00
- 2020-21: $177,500.00

Deliverables under MoU				**OAIC Performance**			
2017-18	2018-19	2019-20	2020-21	2017-18	2018-19	2019-20	2020-21
Reporting One annual report on the operation of this MOU in a form that can be tabled in the Legislative Assembly (s 54 report)	**Reporting** One annual report for each year of the Term of the MOU about its operation in a form that can be tabled in the Legislative Assembly (s 54 report)	**Reporting** One annual report for each year of the Term of the MOU about its operation in a form that can be tabled in the Legislative Assembly (s 54 report)	**Reporting** One annual report for each year of the Term of the MOU about its operation in a form that can be tabled in the Legislative Assembly (s 54 report)	**Reporting** 2017–18 Annual Report made under ACT MoU deliverable met, and published on OAIC website	**Reporting** 2018-19 Annual Report made under ACT MoU provided but not tabled	**Reporting** Annual Report made under ACT MoU deliverable met, and published on OAIC website 2/12/20	**Reporting** Annual Report made under ACT MoU deliverable met, submitted to ACT on 27/07/21. Yet to be published on OAIC website, as not yet tabled in the ACT Legislative Assembly.

Commissioner brief: Performance outcomes

Key messages: 2021-22

- To date in 2021-22, the OAIC is currently meeting **2 of 8 PBS KPIs and** is on track to meet **2 of 8 KPIs**:
  - 80% of privacy complaints finalised within 12 months (91% completion)
  - 80% of FOI Information Commissioner Reviews are finalised in 12 months (81% completion)
  - 80% of Notifiable Data Breaches are finalised within 60 days (partially achieved 76%)
  - 90% of written enquiries are finalised within 10 working days (partially achieved 85%)
- In 2020–21 we achieved 3 PBS KPIs: finalising FOI complaints (82%), handling Notifiable Data Breaches (80%) and finalising privacy complaints (94%).

Key Facts, Figures and Funding

Performance actual achievements 2021–22 (to 30 December 2021 – YTD)	
Handling privacy complaints	
• 80% of privacy complaints are finalised within 12 months	• Currently above target: 91% of privacy complaints finalised within 12 months
Handling data breach notifications	

• 80% of Notifiable Data Breaches are finalised within 60 days
• 80% of My Health Record data breach notifications are finalised within 60 days
	• Not currently being achieve: 76%, down 4% compared to 2020-21
	• Currently not being achieved: 0%
	  ○ open case received 20/5/21
	  ○ *no cases received in 2021–22*

Conducting Privacy Commissioner-initiated investigations (CIIs)	
• 80% of privacy CIIs are finalised within eight months	• Not currently being achieved: 25% completed within 8 months • *Privacy CIIs are not meeting the KPI for finalisation within 8 months.*[1] • *No FOI CIIs have been opened during this financial year.*[2]
Providing an Information Commissioner review function	

[1] The new methodology implemented will impact reporting against this KPI in the future.
[2] Last Senate Estimates 3 CIIs were reported as finalised in the previous period. However only one CII proceeded to investigation (and finalisation) and the other 2 were closed with no investigation being commenced. The OAIC Annual Report 2020-21 refers to one FOI CII being closed during the reporting period.

Commissioner brief: OAIC's APS Census Results

Key messages

- The OAIC's 2021 APS Survey results overall demonstrated staff are highly engaged and committed and that there has been a pleasing improvement across a number of areas (including internal communications and management). It also highlights areas for improvement
- 80% response rate (1% increase)
- 75% overall employee engagement score (remains steady)
- 67% overall wellbeing index score (4% decrease)
- 64% overall innovation index score (-2% variance from APS average)

Areas of strength

- 91% believe strongly in the purpose and objectives of OAIC (8% higher than APS average)
- 97% are happy to 'go the extra mile' (5% higher than APS average)
- 70% are satisfied overall with their job (5% increase)
- 89% of staff consider they receive the respect they deserve from their colleagues (15% increase)
- 59% of staff are inspired to do their best work every day (7% increase)
- 65% of staff believe their immediate supervisor is invested in their development (6% increase)

Areas for further work

- 57% of staff consider the agency does a good job of promoting health and wellbeing (16% decrease from OAIC 2020 results)
- 34% of staff consider their workgroup has the tools and resources needed to perform well (29% lower than APS average)
- 88% of staff consider their workload to be above capacity [either slightly (36%) or well above (52%)]
    - At least to some extent both these issues speak to resourcing levels
- 66% of staff indicated they wanted to leave their position within the next two years (7% higher than APS average)
- 62% of staff are satisfied with the recognition they receive for doing a good job (7% decrease from OAIC 2020 results)
- 70% staff think their SES manager ensures work contributes to OAIC's strategic direction (7% decrease)

Next steps

- The OAIC Executive and senior leaders have met to consider the census results. The Highlights Report has been circulated to staff, discussed in an all-staff meeting and has been considered in further detail in small groups at a branch level.
- The Executive will draw upon outcomes of these discussions, and suggestions from focus group meetings held to consider the workload issues following the delayed 2020 census, to develop an action plan to identify short, medium and long term strategies.

Commissioner brief: Current media issues

Key messages

- This document is a collation of media clips relating to recent issues of note ahead of Senate estimates.
- It may be edited and expanded depending on events in the lead up to the hearing.

Critical facts

The media stories are broken down into 7 groups:

- NDB Resourcing
- Facial recognition
- Iview
- ACT data breach
- FOI/Public Servants
- George Christensen FOI
- Google cookies

Possible questions

- The material supplements the Media Folder and other Estimates briefs

Key dates

- The media articles are all sourced from November-2021 onwards.

Document history

Updated by	Reason	Approved by	Date
Andrew Stokes	February 2022 Estimates		

QoNs asked of other agencies – February 2022 Senate Estimates

Summary by topic

FOI

- Greens Senator Jordon Steele-John asked the **Department of Health** about what information it had given the OAIC in relation to a request for access to a document about the Opiate Dependence Treatment Program (ODTP). 1 He also asked the OAIC for information on the issue.2
- Labor Senator Murray Watt asked the **Department of Industry, Science, Energy and Resources** about the process in which grants recommended by Industry Innovation and Science Australia (IISA) went forward.
    - Of those that were recommended, how many were ultimately approved by the minister? And how many were rejected?
    - From the FOI, 17 projects scored 84 or higher. Were they the 17 that were approved?[3]
- Liberal Senator James McGrath asked **CSIRO** about an FOI request from the livestock industry about CSIRO's partnerships with animal activists.[4]
- Greens Senator Larissa Waters asked the **Department of the Prime Minister and Cabinet** whether, in light of Justice White's decision that National Cabinet documents are not subject to the Cabinet confidentiality FOI exemption, does the Minister or Department consider that the agenda and documents considered by the Women's Safety Ministers' Taskforce are confidential and exempt from disclosure under FOI?[5]
- Labor Senator Timothy Ayres asked the **Department of the Prime Minister and Cabinet** asked how many FOI requests for documents related to National Cabinet had the department received since 5 August 2021? How many applicants have received the documents they sought?[6]
- Independent Senator Rex Patrick asked the **Department of Veterans' Affairs** about FOI processing:
    - Do you have a measure of the average processing time of FOI requests? [7]

---

[1] Unanswered, overdue, Portfolio Question Number SQ21-000985
[2] Download question with answer. LCC-SBE21-054.pdf
[3] Unanswered. Portfolio Question Number SI-19
[4] Download question with answer. sSI-30_McGrath_FOI relating to plant-based companies_CSIRO.pdf
[5] Unanswered. Portfolio Question Number 235
[6] Unanswered Portfolio Question Number 335
[7] Download question with answer. QoN 10 - DVA.pdf

Commissioner brief: NDB overview

Key messages

- For the period 1 January to 31 December 2021, the OAIC received 910 NDB notifications.
  - The most recent 6 month reporting period (1 July to 31 December 2021) saw a 4% increase in notifications from the previous 6 month period.
  - During the July to December 2021 reporting period, 96% of data breaches affected 5,000 individuals or fewer, while 71% affected 100 people or fewer.
- Malicious or criminal attack has consistently remained the leading source of data breaches. The percentages below vary in the different 6 monthly reports – eg malicious or criminal was 55% in the most recent report.

Fiscal Year	2019-2020		2020-2021		2021-2022	
Source	Total	% of Total	Total	% of Total	Total	% of Total
Malicious or criminal attack	645	63%	584	60%	256	55%
Human error	330	32%	339	35%	190	41%
System fault	50	5%	45	5%	18	4%

- The health sector has consistently been the highest reporting industry sector.

Fiscal Year	2019-2020			2020-2021			2021-2022 YTD		
Sector	Total	% of Total	Ranking	Total	% of Total	Ranking	Total	% of Total	Ranking
Health service providers	229	22%	1	209	22%	1	83	17%	1
Finance (incl. superannuation)	149	14%	2	140	14%	2	57	12%	2
Legal, Accounting & Management services	67	6%	4	73	8%	3	50	10%	3
Australian Government	29	3%	10	67	7%	4	28	6%	7
Education	93	9%	3	59	6%	5	33	7%	5

- For FY2020-21, the OAIC finalised 80% of NDB notifications within 60 days, in line with the KPI of 80% within 60 days:

Time taken to close (Days)	2019-20	2020-21	2021-22
% closed in less than 60 days	62%	80%	76%
Number of cases closed in less than 60 days	603	790	394

  - The OAIC generally finalises notifications on the basis that the entity has met the requirements of the NDB scheme and taken steps to prevent reoccurrence. The OAIC may also finalise notifications where the matter has been escalated to investigation.
- The OAIC has no evidence that COVID-19 has directly impacted on notifications to the OAIC, in terms of numbers, sectors, or causes.

Commissioner brief: The effectiveness of the NDB scheme

Key messages

- Broadly the key objectives of the scheme are to improve consumer protection and increase accountability through transparency and to provide practical guidance on mitigating the risk of harm following a breach.
- The scheme also provides valuable insights into the data protection risks facing organisations and the ways that organisations can improve their security posture and processes to minimise the risk of data breaches.
- The OAIC considers that the NDB scheme is effective. Over 3,500 notifications have been received under the NDB scheme since it commenced in February 2018, representing a more than eight-fold increase on notifications made under the previous voluntary notification scheme – 344 in the 3 years prior.
- However, the OAIC has proposed a number of enhancements to the scheme in our submission to the review of the Privacy Act.

Critical Issues

Purpose of the NDB scheme

- The NDB scheme was designed to achieve three specific objectives.
    - First, to ensure that individuals at risk of serious harm as a result of a data breach involving their personal information are notified and able to take remedial steps to lessen the adverse impact of the breach, for example, monitoring their accounts, changing passwords and cancelling credit cards.
    - Second, it encourages, through the prospect of regulatory action for non-compliance, both proactive security practices to protect personal information, and full transparency and accountability by entities experiencing data breaches.
    - Third, it is intended to gather information to better inform policy makers, regulators, law enforcement and researchers about trends in the handling of personal information.

How does OAIC engage with notifying entities?

- The OAIC has worked closely with notifying entities to ensure that their responses to data breaches meet the requirements of the NDB scheme, and that they implement new practices, processes and technologies to reduce the risk of re-occurrence.
    - This may include requesting detailed information on the notifying entity's assessment process, or on technical elements of the breach, or requesting entities to re-issue their notification to ensure it meets the requirements of the scheme.

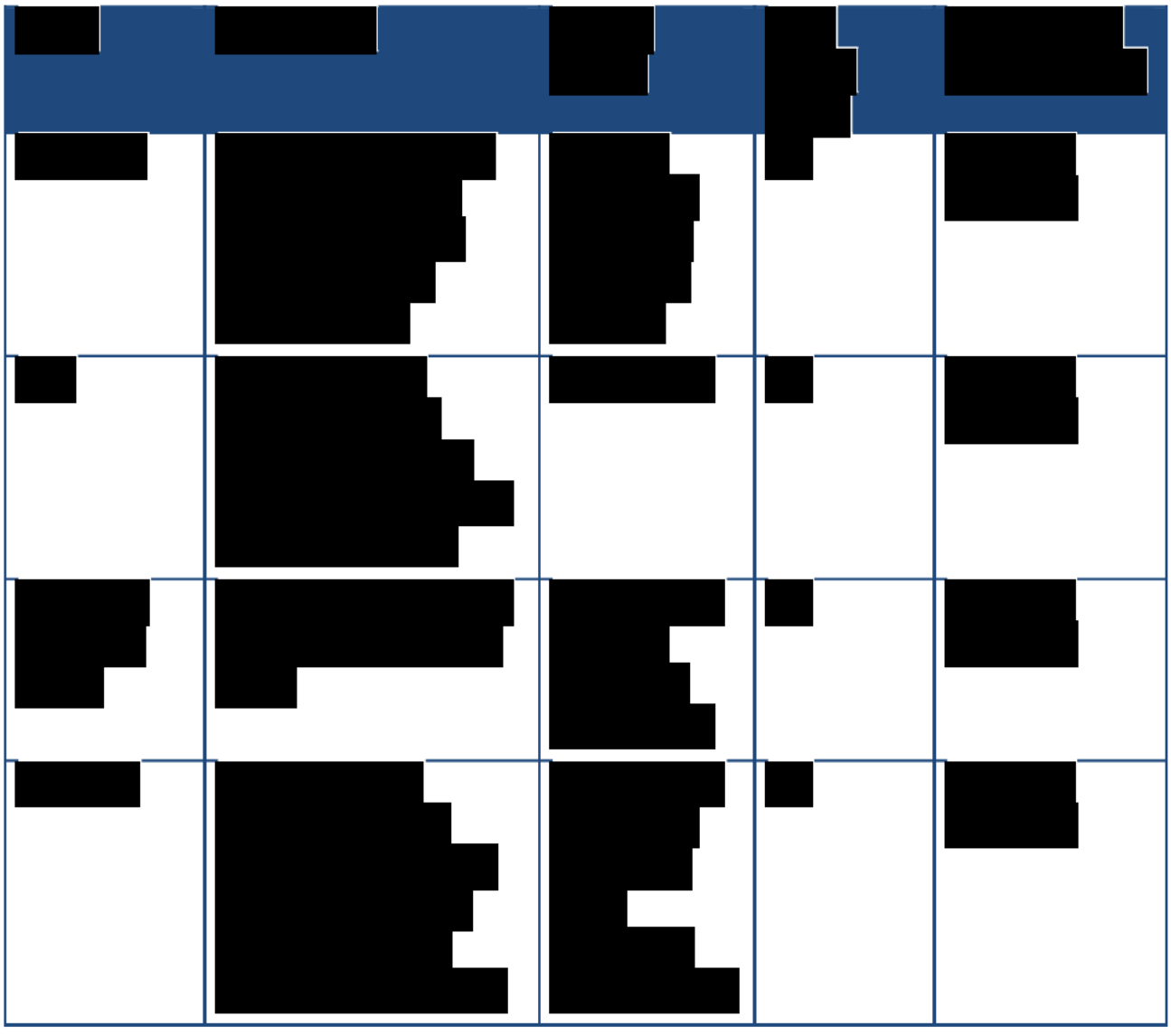
Commissioner brief: Summary of High Profile NDBs

Key messages

- Most of the breaches receiving significant media coverage in the last 12 months resulted from malicious or criminal attacks. Such attacks accounted for 55% of notifications to the OAIC in July to December 2021.
    - In a number of instances, the company experiencing the data breach issued a public statement, typically following formal notification to individuals potentially affected by the breach and to the OAIC, as required by the NDB Scheme.
- Media coverage of data breaches has helped build public awareness of privacy rights and issues and can also help consumers understand the risks associated with putting information online and the steps that they can take to protect themselves.

Critical issues

[redacted]



Commissioner brief: High profile PI's and CII's

Key messages

- As of 31 January 2022, the OAIC has 8 Commissioner initiated preliminary inquiries and 9 investigations open.
- The OAIC handles these matters in accordance with the OAIC's *Privacy regulatory action policy* and *Guide to privacy regulatory action.*

Critical facts

- The Commissioner may make inquiries **under s 42(2)** of the *Privacy Act 1988* (Cth) (the Privacy Act) of any person for the purposes of determining whether to investigate an act or practice under s 40(2) of the Privacy Act.
- **Under s 40(2)** of the Privacy Act, the Commissioner may, on the Commissioner's own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of Australian Privacy Principle 1, where the Commissioner thinks it is desirable that the act or practice be investigated.
- When considering whether to investigate an act or practice under s 40(2), the Commissioner has regard to the factors outlined in **paragraph 38 of our *Privacy regulatory action policy***. These factors include:
    - the seriousness of the incident or conduct to be investigated
    - the specific and general educational, deterrent or precedential value of the particular privacy regulatory action
    - whether the conduct is an isolated instance, or whether it indicates a potential systemic issue
    - the level of public interest or concern relating to the conduct, proposal or activity.
- Where a privacy incident is of community concern and has already been reported in the media, the OAIC may confirm publicly that it is investigating or making inquiries. The OAIC may also comment publicly where there is a public interest in doing so, for example to enable members of the public to respond to a data breach.
- The OAIC seeks to work in partnership with other data protection authorities where there is a shared interest - a coordinated and consistent global response can be an effective regulatory response to a global privacy issue.

Possible questions

How may CIIs does your office have open?

We have 9 open CIIs as at 31 January 2022.

These cover a range of sectors, including telecommunications, education, financial services, retail and not-for-profit.

Commissioner brief: DHA representative complaint

Key messages

- On 11 January 2021 the Australian Information and Privacy Commissioner made a determination[1] under s 52 of the *Privacy Act 1988* (Cth) (**Privacy Act**) in a representative complaint about the Department of Home Affairs (formerly the Department of Immigration and Border Protection) (**the Department**).
- The representative complaint followed the publication of a detention report on the Department's website on 10 February 2014 in error that contained embedded personal information of all 9,258 persons in immigration detention as of 31 January 2014.
- It is the first determination in a representative complaint where the Commissioner has awarded compensation for non-economic loss payable to individuals affected by a data breach.
- On 26 March 2021, the Office of the Australian Information Commissioner (**OAIC**) received notice from the Administrative Appeals Tribunal (**AAT**) of an application from an individual seeking review of the decision.
- On 21 June 2021, the AAT decided to 'stay' (that is, put on hold) the operation and implementation of the Commissioner's Determination until the AAT has made a decision in response to the application for review, and that decision has come into operation. That means that no assessment or payment of compensation under the Determination is currently taking place. A hearing took place on 13 and 14 December 2021. At this stage the AAT's review is expected to be completed in 2022.

Critical Issues

- The determination applies to 9,258 persons whose names were published by the Department on 10 February 2014, except for 7 individuals who opted out of being part of the Representative Complaint (**class members**).
- The Commissioner found that the Department had interfered with the privacy of the class members by disclosing their personal information on a publicly available website, in breach of Information Privacy Principle (**IPP**) 11 and failing to take such security safeguards as were reasonable in the circumstance to take against loss, unauthorised access, use, modification or disclosure, and against other misuse, in breach of IPP 4.
- The Commissioner determined that 1,297 class members who made submissions and/or provided evidence of their loss or damage (**Participating Class Members**) to the OAIC, and demonstrated that they suffered loss or damage as a result of the data breach, are to be paid compensation for non-economic loss under five categories of loss or damage, depending on the severity of the impact.

[1] 'WP' and Secretary to the Department of Home Affairs (Privacy) [2021] AICmr 2

Commissioner brief: [redacted]

Key messages

- [redacted] The matter remains open, however the OAIC does not report on matters under current inquiry or investigation and rarely reports where a matter is escalated to investigation.
- The APPs do not generally prevent an organisation from sending personal information overseas. However, organisations need to carefully consider steps that may need to be taken to comply with the APPs when doing so.
    - However certain types of personal information are subject to data localisation requirements. For example, part IIIA of the Privacy Act, restricts sending information held in the Australian credit reporting system overseas.

Critical facts

- [redacted]

Commissioner brief: Assessments program 2020-21 and 2021-22

Key messages

- The OAIC has a program of privacy assessments (or audits) to identify privacy risks in key programmes where agencies and organisations handle personal information. Where risks are identified, we make recommendations to address them.
- In the 2020-21 financial year we:
    - focused on digital health, COVID app data, Consumer Data Right (CDR), passenger name records (PNR), and telecommunications service providers' processes under the data retention scheme
    - closed 8 assessments.
- We have 12 privacy assessments open currently: 8 carried over from last financial year.
- 3 of these assessments are examining compliance of large cohorts of targets:
    - PIA Register assessment examines compliance of 169 agencies (estimated number of agencies covered by the Privacy Act), across 13 portfolios
        - 3 portfolios have been assessed
        - a further 3 portfolios are currently at various stages of assessment.
    - My Health Record access security policy assessments (2) seek survey responses from 300 GPs clinics and involve qualitative analysis of 20 GP clinics' policies.
- Assessments for the 2021-22 financial year, including those under memoranda of understanding (MOU) with Australian Government agencies and the Australian Capital Territory (ACT), will focus on:
    - digital health
    - Medicare data-matching
    - telecommunications service providers' record keeping under the data retention scheme
    - border clearance processes (PNR)
    - COVID app data
    - CDR
    - as well as initiatives like the Australian Government Agencies Privacy Code and Notifiable Data Breaches Scheme.
- The COVID-19 pandemic has impacted the way that the OAIC conducts assessments.

Commissioner brief: Comprehensive Credit Reporting & Hardship

Key messages

- On 16 February 2021, the *National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Act 2021* received royal assent.
- The Act introduced mandatory comprehensive credit reporting (CCR) and financial hardship information (FHI) reporting reforms.
- Our existing role in overseeing the consumer credit reporting system will continue despite the amendments – this includes working with entities to facilitate compliance and best practice and using our investigative and enforcement powers where a privacy breach may have occurred.
- The explanatory memorandum to the Bill anticipated that changes would be required to the Privacy (Credit Reporting) Code 2014 (the CR Code) as a result of the amendments.
- On 6 September 2021, the Australian Retail Credit Association (ARCA) (as code-developer for the CR Code) submitted an application to the OAIC to vary the CR Code to address the FHI reporting reforms. This application was made following public consultation by ARCA (5 July – 11 August 2021).
- The OAIC is currently considering this application and has conducted public consultation (September, October and December 2021).
- We anticipate that the application will be finalised and approved early this year. Following approval, steps will be taken to register the CR Code before it takes effect.
- The financial hardship provisions of the Privacy Act will come into effect on 1 July 2022.
- Our chief interest in deciding whether to approve the variation to the CR Code has been to ensure that any changes maintain an appropriate balance between facilitating an efficient credit reporting system and protecting individuals' privacy.

Critical issues

- The Act introduces financial hardship information into the credit reporting system.
- This reform has attracted strong views from industry and consumer groups during the hardship review run by the Attorney-General's Department.
- The reforms will require the Commissioner to approve a change to the CR Code.
- The Act also introduces the right for individuals to access their credit rating and information about how that rating is derived.
- The mandatory comprehensive credit reporting aspect of the reform that came into effect on 1 July 2021 will result in the bulk disclosure of credit information to CRBs.

Possible questions

- ***What is the OAIC's oversight role for proposed mandatory CCR?*** My existing oversight of the consumer credit reporting system will continue under the mandatory CCR

Commissioner brief: Consumer Data Right

Key messages

- The OAIC has continues to actively regulate privacy aspects of the 'Consumer Data Right' (CDR) and work closely with other CDR agencies to contribute to the development of the CDR regulatory framework. This has included:
    - published a suite of **guidance** for industry reflecting the amendments to the CDR Rules made by the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* (**'V3 Rules'**). The OAIC will continue to update its guidance, including the CDR Privacy Safeguard Guidelines, to reflect these and other amendments to the CDR regulatory framework.
    - published the summary of its **first privacy assessment** for the CDR, examining whether the 4 initial data holders (the major banks) managed CDR data in an open and transparent way, in accordance with Privacy Safeguard 1. The assessment found the banks were generally handling consumer data under the CDR in an open and transparent way with good privacy practices in place.
    - analysed the likely effect of making the draft Consumer Data Right (Telecommunications Sector) Designation ('draft telecommunications designation') on the privacy or confidentiality of consumers' information and **reported** to Minister Hume about that analysis, as required by s 56AF of the *Competition and Consumer Act 2010* ('CC Act'). The report provided to the Minister has been published on the OAIC's website.
    - as the primary complaint-handler, the OAIC has worked with the **ACCC** to improve the complaints and enquiries process, including implementing a central portal for CDR participants to lodge enquiries, reports and complaints (on the CDR.gov.au website).
    - **worked closely with other core CDR agencies** on the development of the CDR regulatory framework. This has included providing policy advice to **Treasury** and attending regular inter-agency meetings.
    - The OAIC also works closely with the **Data Standards Body (DSB)** on development of the CDR data standards, and is an observer on the Data Standards Advisory Committee.

Possible questions

How many CDR enquiries or complaints have you received?

- In preparation to receive and manage complaints in line with the 'no wrong door approach', we worked closely with the ACCC to ensure that, from 1 July 2020, consumers were able to lodge enquiries, reports and complaints via a central contact point (the CDR.gov.au website). Since 10 December 2020, contacts have been triaged through a

Commissioner brief: Biometrics

Key messages

- The OAIC has privacy oversight of Identity-Matching Services such as the National Facial Biometric Matching Capability (NFBMC) and the National Drivers Licence Facial Recognition Solution (NDLFRS), which involve the collection and handling of large volumes of sensitive information.
    - We are engaging with the Department of Home Affairs (Home Affairs) on an MoU to conduct 2 privacy assessments, one each for the NFBMC and NDLFRS.
- We continue to engage with Home Affairs to incorporate additional safeguards into the draft legislation and the NFBMC's associated governance framework. [redacted]
    - The Parliamentary Joint Committee on Security and Intelligence's (PJCIS's) advisory report on *the Identity-Matching Services Bill 2019* (the IMS Bill) recommended redrafting to include amongst other things more robust privacy safeguards (Rec 1).

Critical facts

- Home Affairs operates the NFBMC to prevent identity crime, and for general law enforcement, national and protective security, and identity verification purposes. The NFBMC facilitates the sharing of facial images between the Commonwealth and states and territories, through its identity-matching services.[1]
- The IMS Bill and the Australian Passports Amendment (Identity-Matching Services) Bill 2019 provide the legal framework for Home Affairs to operate identity-matching services. The OAIC made a submission to the PJCIS in 2018,[2] recommending that Home Affairs specified privacy protections applicable to the NFBMC within its overarching legislation. The OAIC has also provided Home Affairs with a range of policy advice in relation to the NFBMC's governance documents. [redacted]
- In December 2019, the Australian Human Rights Commission's (AHRC) released its Discussion Paper on Human rights and Technology recommending that the Australian Government implement a legal moratorium on facial recognition technology (FRT) until it introduces a suitable legal framework.[3]

[1] Services include the Face Verification Service ('one to one' matching) and Face Identification Service ('one to many' matching). The NDLFRS (as part of the NFBMC) will be a centralised database of driver licence holdings from every state and territory

[2] OAIC, *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018 — submission to Parliamentary Joint Committee on Intelligence and Security*, 2018 < https://www.oaic.gov.au/engage-with-us/submissions/review-of-the-identity-matching-services-bill-2018-and-the-australian-passports-amendment-identity-matching-services-bill-2018-submission-to-parliamentary-joint-committee-on-intelligence-and-security/>.

[3] See the Australian Human Rights Commission's Discussion Paper on Human rights and technology (2019), https://www.humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019.See proposal 11 at p.10.

Commissioner brief: International regulatory developments

Key messages

- Globally interoperable data protection laws are increasingly important to protect individuals online and reduce regulatory friction for business - particularly noting increased cross-border data flows. This was an important aspect of OAIC submission to the Privacy Act Review.

- The OAIC actively engages with a range of international privacy and data protection networks. Since October 2018, I have been a member of the Executive Committee of the Global Privacy Assembly. The Global Privacy Assembly is the leading global forum of data protection and privacy authorities with over 130 members across all continents.

- International engagement ensures the OAIC learns from others' experiences, identifies areas of synergy and facilitates international collaboration, including on enforcement. The OAIC has MOUs with the Data Protection Commissioner of Ireland (April 2014), the UK Information Commissioner's Office (January 2020) and the Singaporean Personal Data Protection Commission (March 2020). The OAIC is currently in discussions with the UK ICO and the Singaporean Personal Data Protection Commission to continue with the MOUs, given the benefits of these relationships. For example, under our MOU with the ICO we undertook a joint investigation into the information handling practices of Clearview AI.

- We work closely with Australian government agencies on initiatives that facilitate cross-border transfers of data while protecting privacy, such as working with the Attorney-General's Department to implement the APEC Cross-Border Privacy Rules (CBPRs) in Australia, and providing advice to the Department of Foreign Affairs and Trade in relation to Australia's Free Trade Agreements.

- In January 2021, the Australian Government elevated the bilateral relationship with Malaysia to a Comprehensive Strategic Partnership (CSP). As part of this, areas for data protection cooperation with the Malaysian Department of Personal Data Protection (JPDP) will be explored.

-

- We monitor international privacy developments, particularly in Europe, the UK, Canada and the USA, to inform both the advice we provide to Australian Government and our own regulatory action. For example, we have closely been monitoring the UK's
- children's code and the introduction of the Californian Consumer Privacy Act in light of the Government's proposed online privacy code.

Commissioner brief: My Health Record

Key messages

- Since 1 July 2021, the OAIC has been funded through a direct appropriation for its regulatory role in relation to the *Privacy Act 1988*, *My Health Records Act 2012* and *Healthcare Identifiers Act 2010*. This replaces the previous Memorandum of Understanding (MOU) arrangement with the Australian Digital Health Agency (ADHA). Under the new funding arrangement, the OAIC continues to undertake regulatory oversight of the privacy aspects of the My Health Record system, including:
    - responding to enquiries and complaints
    - handling data breach notifications
    - providing privacy advice, and
    - conducting privacy assessments
- The AHDA have advised the OAIC that the recommendations made in the Australian National Audit Office's (ANAO) performance audit of the My Health Record system (2019) have now been implemented. The OAIC continues to engage with the ADHA to ensure that the recommendations are incorporated into ongoing business practice and that oversight and compliance measures are maintained, including:
    - Reviewing the ADHA's end-to-end privacy risk assessment and engaging closely with the ADHA to ensure appropriate governance and ongoing compliance is in place (Recommendation 1)
    - Consulting with the ADHA on their Compliance Framework (Recommendations 2 and 4)
    - Delivering a suite of Emergency Access guidance for healthcare providers, in consultation with the ADHA and other key stakeholders (Recommendation 2).
- The My Health Record system is a key element of the ADHA's National Digital Health Strategy. The current strategy is due to end in 2022 and the ADHA are developing the next strategy, which will replace the existing strategy for the next five years. The OAIC has been updated on the broad progress of the strategy and we anticipate that we will be consulted on the draft strategy in the coming weeks.
- The OAIC is monitoring and engaging with the ADHA in relation to additional functionality being developed for the My Health Record system to support the rollout of Covid-19 vaccine records and pathology reports, including in the My Health Record mobile app environment.
- On 24 February 2020, Professor John McMillan AO was appointed to conduct a review of the *My Health Records Act 2012* (MHR Act). The OAIC made a submission to the review on 30 October 2020 which identifies a number of privacy risks and makes recommendations for legislative amendment.

Commissioner brief: Collection of personal information by businesses in compliance with State and Territory Health Orders

Key messages

- As a result of the COVID-19 pandemic, State and Territories have issued public health orders and directions (Health Orders) that set out requirements for businesses and venues collecting personal information for contact tracing purposes.
- Requirements in the Health Orders vary across jurisdictions. There are discrepancies regarding the type of data to be collected, how long it should be held, the secondary purposes for which it can be used and varying responsibilities for handling and protecting it.
- The OAIC along with state and territory privacy regulators produced Guidelines to support a nationally consistent approach to collection of contact tracing information underpinned by 5 privacy criteria including: (i) data minimisation, (ii) security, (iii) purpose limitation, (iv) retention/deletion and (v) regulation by the Commonwealth *Privacy Act 1988*.
- Australian Privacy Regulators consider that these harmonised privacy Guidelines are critical to ensure:
    - personal information is handled consistently;
    - businesses are supported to develop privacy protective mechanisms to collect contact tracing information; and
    - individuals have confidence to provide accurate personal information to support contact tracing efforts.

HISTORY OF DEVELOPMENT OF THE GUIDELINES FOR CONTACT TRACING

- 20 November 2020 – the OAIC and state and territory privacy regulators released draft Guidelines on 'requirements to collect personal information for contact tracing purposes' for public consultation.
- 24 December 2020 – the OAIC (on the advice of the then Acting Chief Medical Officer, Professor Paul Kelly) submitted the draft Guidelines to the Australian Health Protection Principal Committee (AHPPC) Secretariat for consideration.
- 14 January 2021 – a response was received from the AHPPC advising that the draft Guidelines were not endorsed. Health authorities in WA and QLD raised matters that required further consideration by the OAIC.
- 9 March 2021 – the OAIC met with QLD Department of Health to seek further feedback on the draft Guidelines.
- 16 April 2021 – the OAIC met with WA State Solicitor's Office to seek further feedback on the draft Guidelines.
- 27 August 2021 - the OAIC consulted with the National COVID-19 Privacy Team in relation to final version of the draft Guidelines.
- 3 September 2021 – the OAIC published the finalised 'Guidelines for state and territory governments – Creating nationally consistent requirements to collect personal information for contact tracing purposes'

Commissioner brief: Coronavirus – Emergency declaration

Key messages

- The Privacy Act is not a barrier to necessary information sharing in a declared emergency or disaster.
- Part VIA of the Privacy Act contains special provisions for the collection, use and disclosure of personal information in an emergency or disaster that affects Australians in Australia or overseas.
- These provisions take effect if the Prime Minister or Minister responsible for the Privacy Act (the Attorney-General) declares an emergency under Part VIA of the Privacy Act.
    - A declaration will assist agencies and organisations in applying the Privacy Act less restrictively and with greater confidence in regard to the personal information of deceased, injured and missing individuals involved in an emergency or disaster providing the purpose relates to the Commonwealth's response to the declared emergency/disaster (s 80H)
    - although the relevant Explanatory Memorandum frames the discussion around 'deceased, injured and missing individuals' it is arguably broad enough to accommodate outbreak of a serious infectious disease with pandemic potential [see in particular ss 80J–K and s 80P(1)].
- Entities will not be in breach of the Australian Privacy Principles (APPs) if they have complied with Part VIA.
- Coronavirus has not been declared an emergency under Part VIA of the Privacy Act.

Possible questions

How long is an emergency declaration in effect?

- The emergency declaration takes effect from when it is signed (s 80M) and applies for a maximum period of 12 months but may end earlier at a time specified in the declaration or if the declaration is revoked (s 80N).

Is an emergency declaration required for disclosure of personal information in an emergency or disaster?

- Entities may be able to use or disclose personal information in accordance with APP 6 where an emergency or disaster exists, but a declaration has not been made under Part VIA.
- Under APP 6, an APP entity may use or disclose personal information for a purpose for which it was collected or for a secondary purpose where an exception applies—

Commissioner brief: National Data Commissioner

Key messages

- The Office of the Australian Information Commissioner (OAIC) is supportive of the Productivity Commission's (PC) underlying policy objectives in its *Data Availability and Use Inquiry* report, which seek to enable better use of, and greater access to, valuable government-held data.
- The Data Availability and Transparency (DAT) Bill has now been introduced into Parliament. The Senate Finance and Public Administration Committee handed down its report on the Bill on 29 April. The OAIC understands that amendments are being made to the Bill before it's reintroduction into Parliament.
- The Commonwealth Privacy Act or equivalent State/Territory privacy legislation will continue to apply where data sets that are shared under this framework include personal information.
- The OAIC made a public submission to the Senate inquiry that identified opportunities to further enhance the privacy protections in the framework, for example, by placing a greater emphasis on agencies using datasets that do not contain personal information.
- We also raised the proposed consequential amendment to the Freedom of Information Act, which proposes to effectively exempt any data that government agencies share with each other through the scheme. The proposal seems unnecessarily broad and risks misalignment with the objects of the Freedom of Information Act to provide a legal right to access to documents. The proposal reduces the information access rights of individuals, impacting on their ability to seek access to their own personal information and understand how agencies are using this information.
- The Senate Committee report recommended that consideration is given to whether amendments could be made to the Bill, or further clarification added to the explanatory memorandum to provide additional guidance regarding privacy protections, particularly in relation to the de-identifying of personal data that may be provided under the Bill's data-sharing scheme.[1]
- The OAIC welcomes the collaborative approach that the Office of the National Data Commissioner has taken to developing this data sharing framework so far. We look forward to continuing to work with the ONDC to ensure that data can be shared safely and securely under this framework, and in line with community expectations, particularly through the Australian Information and Privacy Commissioner's membership on the National Data Advisory Council (NDAC).

[1] https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/DataTransparency/Report

Commissioner brief: Privacy law reform

Key messages

- The OAIC welcomes the Government's commitment to strengthen the Privacy Act to ensure Australians' personal information is protected in the digital age, including the introduction of higher penalties for privacy breaches, a code of practice for social media and online platforms (the online privacy code) and a review of the Privacy Act.
- The reforms outlined in the Government's response to the Digital Platforms Inquiry final report are critical to ensuring that our regulatory framework protects personal information into the future and holds organisations to account.
- The OAIC has worked closely with the Attorney-General's Department on developing options for reform for the Privacy Act Review Discussion Paper, and to finalise the draft legislation that will introduce the online privacy code framework. These were both released for public consultation in October last year.
- The release of the Discussion Paper is a critical step in ensuring our privacy framework can support fair and reasonable handling of personal information and protect Australians' data wherever it flows.
- The well-considered and reasoned proposals and options put forward in the Discussion Paper, were informed by hundreds of submissions and feedback from a diverse range of stakeholders in response to the Department's earlier Issues Paper.
- In our response to the Discussion Paper, we made detailed recommendations drawing on our regulatory experience and how these potential reforms would operate in practice.
- Our recommendations seek to ensure Australia's privacy regime continues to operate effectively for all and promotes innovation and growth by:
    - protecting consumers from individual and collective privacy risks and harms
    - empowering consumers to take control of their personal information through new rights and enhanced transparency requirements
    - enhancing the framework of organisational accountability and personal information handling to ensure regulated entities are confident to innovate and use data within the boundaries of the law, informed by community expectations
    - establishing a regulatory framework that supports proactive and targeted regulation, strategic enforcement, efficient and more direct avenues of redress for individuals, and appropriate deterrents against mishandling of personal information.
- The draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 will increase penalties for serious or repeated breaches of privacy,

Commissioner brief: ABC iview platform

Key messages

- On 18 June 2021, the ABC advised the OAIC that it had decided to delay the rollout of mandatory login on the ABC iView platform. I note that the ABC had initially intended to rollout mandatory login on iView during July and August 2021. I understand the ABC has recently indicated that it would commence a staged rollout of mandatory login on the iview platform in the next few months.[1]
- I was supportive of the ABC's decision to delay the rollout of mandatory login last year to enable a thorough consideration of privacy issues and the concerns raised by the community.
- As an agency under the *Privacy Act 1988* (Privacy Act) and the Australian Government Agencies Privacy Code, the personal information entrusted to the ABC must be respected, protected and handled in a way that is compliant with privacy law.
- The ABC has an opportunity to adopt a best practice approach, which together with effective communication and community engagement strategies, can help to ensure that the handling of personal information is both compliant with privacy laws and meets the community's expectations.
- To that end, a privacy impact assessment (PIA) is an important tool to help ensure compliance, facilitate a privacy-by-design approach, assess whether privacy impacts are reasonable, necessary and proportionate, and identify better practice.
- While the OAIC does not have a formal role in the development, endorsement or approval of PIAs, we do assist agencies with guidance and advice during the PIA resources (subject to available resources).
- The OAIC reviewed a draft PIA for this project and provided policy advice to the ABC in November last year. OAIC staff have liaised closely with the ABC since May 2021 and have provided guidance and advice on the key issues that should be addressed in the PIA.
- It is the responsibility of the ABC to determine whether the project complies with privacy laws and meets community expectations.
- However, a key privacy consideration in the current circumstances is whether the move to mandatory login is a reasonable, necessary and proportionate approach to achieving the ABC's objectives and, in particular, whether these objectives could be achieved by alternative less intrusive means (such as by retaining the existing voluntary login process). We provided additional guidance to the ABC about how this issue should be considered in the PIA for this project.

[1] https://www.innovationaus.com/privacy-warnings-wont-stop-abc-sharing-user-data/

Commissioner brief: Vaccine certificates

Key messages

- There are currently varied requirements at the federal and state and territory level for individuals to be vaccinated in order to undertake certain activities, including international travel, accessing venues such as hospitality and retail, and in order to undertake certain types of work.
- Where an individual is required to be vaccinated, there may also be requirements for that individual to provide proof of their COVID-19 vaccination status. Vaccination status information is sensitive health information and is afforded higher protections under the Privacy Act 1988.
- The OAIC has issued guidance for employers and employees as well as businesses in relation to their privacy obligations when collecting COVID-19 vaccination status information from employees, customers and other individuals.

Critical facts

Requirements within Australia to get vaccinated and provide proof of vaccination

- Fully vaccinated Australia citizens, permanent residents and eligible visa holders can now travel to and from Australia without needing to apply for a travel exemption if they can provide proof of vaccination. As of 19 October 2021, Australians who travel overseas can access an internationally recognised vaccination certificate to prove their vaccination status abroad. The international vaccination certificate includes a QR code that is readable globally and which complies with the standards set out by the International Civil Aviation Organisation. This is known as the Visible Digital Seal Non-Constrained Checker (VDS-NC). The certificate displays the individual's passport details to facilitate identity verification.
- State and territory governments have made public health orders requiring certain workers to be vaccinated against COVID-19. For example, there are public health orders that apply across jurisdictions in relation to aged care workers and health workers. Additionally, some industries or Australian businesses (such as Qantas and SPC) have mandated that their employees be vaccinated.
- Individuals can access their COVID-19 proof of vaccination in various ways, including through the Medicare Express app, their MyGov account and their My Health Record. Individuals can also choose to save a copy of their vaccination certificate to their digital wallet or share it with a state or territory check-in app.
- The OAIC published updated guidance for employers and employees in relation to the collection of vaccination status information on 23 September 2021. The key privacy considerations are:

Commissioner brief: COVIDSafe Assessment Program

Key messages

- The OAIC is conducting 5 assessments following the information lifecycle of COVID app data in the COVIDSafe System.
- On 16 May 2020 the Australian Government amended the Privacy Act to insert a new Part VIIIA to protect COVID app data and provide the OAIC with an oversight and assurance role.
- The provisions also extend existing regulatory powers to allow the OAIC to conduct an assessment of whether the acts or practices of an entity (including a state or territory authority) comply with the Australian Privacy Principles (APPs) or Part VIIIA, and to require an entity or authority to give information or produce documents.

Critical Issues

- A legal framework of privacy protections was established under Part VIIIA of the Privacy Act to protect COVID app data.
- Amendments to the Privacy Act expanded the OAIC's regulatory oversight role to include the handling of COVID app data by State and Territory health authorities, as well as by the National COVIDSafe Data Store.
- The Commissioner has strengthened assessment powers under s 94T of the Privacy Act in relation to the COVIDSafe System. Under this section the Commissioner has expanded powers to compel information and documents.

COVIDSafe assessments

- Under s 94T of the Privacy Act, the Australian Information Commissioner was given new powers to conduct assessments relating to COVID app data and to compel information and documents.
- The OAIC is undertaking a COVIDSafe assessment program - comprised of 5 risk and compliance based privacy assessments looking at the information lifecycle of COVID app data:
    - Assessment 1 is completed and was published on 25 June 2021
    - Assessment 3 is completed and was published on 26 October 2021
    - Assessments 2 and 4 are in progress.
- The OAIC engaged external consultants (PricewaterhouseCoopers) under section 24 of the *Australian Information Commissioner Act 2010* to assist in the delivery of this program and provide specialist technical expertise in relation to ICT components of the COVIDSafe System.

Commissioner brief: Digital Identity

Key messages

- The OAIC welcomes the development of and consultation on legislation for the Digital Identity System.[1]
- The legislation contains strong privacy protections applying to identity service providers, credential service providers, attribute service providers and identity exchanges to ensure that the identity information of Australians is protected. We are continuing to work with the DTA to ensure protections are appropriate.
- The OAIC is pleased to have been proposed as the independent privacy regulator in the draft legislation through the application of the APPs to accredited entities that are not subject to comparable state or territory privacy legislation and regulating the additional privacy protections that are introduced through legislation.
- The OAIC continues to regulate the Privacy Act as it applies to APP entities who have been accredited to participate in the Digital Identity system, prior to the commencement of the legislation.[2]
- The Digital Transformation Authority (DTA) has received funding to expand Digital Identity to connect a greater number of services to the system (including state and territory services) over the next three years. The OAIC received funding in the 2021-22 financial year to undertake two privacy assessments (audits) of the system and develop guidance materials.[3] The first assessment is planned to commence this quarter.
- The OAIC will seek additional funding to undertake it's expanded regulatory role under the Digital Identity legislation.
- We welcome the opportunity to continue engaging with the DTA in its development of a privacy protective scheme and governance mechanisms between the Oversight Authority and the OAIC through our monitoring, guidance and advice functions.

Critical Issues

- The DTA is currently undertaking two main areas of work in relation to Digital Identity:
    - Developing legislation to underpin this scheme. This will enable the scheme to be used by State and Territory governments and the private sector, in addition to

[1] On 30 September 2021 the DTA commenced exposure draft consultation on a legislative package for the Digital Identity System, consisting of the Trusted Digital Identity Bill, Trusted Digital Identity Framework Accreditation Rules and Trusted Digital Identity Rules.

[2] A number of Australian Government agencies are already accredited and participating in the Digital Identity system as an identity exchange (Services Australia), identity service providers (myGovID, operated by the ATO; Digital iD, operated by Australia Post), credential service providers and attribute service providers. Recent news reports indicate that private sector entities have also been accredited as an identity service provider (OCR Labs - click for media release) and an identity exchange (eftpos' connectID - click for media release) under the existing Trusted Digital Identity Framework, which has been operating for a number of years:

[3] See p 291 of OAIC 2020-21 PBS: https://www.ag.gov.au/system/files/2020-10/17%202020-21%20Office%20of%20the%20Australian%20Information%20Commissioner%20PBS.PDF

Commissioner brief: FOI IC reviews

IC review applications RECEIVED

The increase in ***IC review applications received*** from 2015-16 to 2020-21 was **140%**

When extrapolated from the first 6 months, the number of applications expected for 2021-22 is **1764**. That is a **246% increase** on 2015-16.

2015-16	*2016-17*	*2017-18*	*2018-19*	*2019-20*	*2020-21*	*2021-22 (to 31/12/21)*
510	632	801	928	1066	1224	882 38% increase on same period 2020-21

IC review applications FINALISED

The increase in ***IC review applications finalised*** from 2015-16 to 2020-21 was **124%**

When extrapolated from the first 6 months, the number of finalisations expected for 2021-22 is **1388**. That is a **206% increase** on 2015-16.

2015-16	*2016-17*	*2017-18*	*2018-19*	*2019-20*	*2020-21*	*2021-22 (to 31/12/21)*
454	515	610	659	829	1018	694 37% increase on same period 2020-21

The **average time to finalise** IC reviews has steadily increased:

2016-17	*2017-18*	*2018-19*	*2019-20*	*2020-21*	*2021-22 (to 31/12/21)*
190 days (6.3 months)	204 days (6.8 months)	237 days (7.8 months)	246 days (8.1 months)	252 days (8.3 months)	216 days (7.1 months)

Number **finalised in less than 12 months**:

2018-19	*2019-20*	*2020-21*	*2021-22 (to 31/12/21)*
481	597 (24.1% increase on 18-19)	740 (24% increase on 19-20)	562 (extrapolated to **1124 for full year**) (52% increase on 20-21) (134% increase on 18-19)

Commissioner brief: 2020-21 Australian Government agency and ministerial FOI statistics and trends in the use of exemptions under the FOI Act[1]

Key messages

- Under s 8J of the *Australian Information Commissioner Act 2010*, the Information Commissioner has power to collect information and statistics from agencies and ministers about FOI matters including:
  - the number of FOI requests and amendment applications received
  - outcomes
  - charges collected
  - number of internal reviews.
    - Agencies enter FOI statistics into an online portal each quarter. The statistics in this brief are based on the data reported by agencies and ministers.
- The **number of FOI requests** made to agencies and ministers in 2020-21[2] decreased by 16% over the previous year to 34,797 (when there was a 6% increase in the number of requests compared with the previous year).
    - The decrease in total number of requests in 2020-21 is largely the result of a decrease in requests for personal information experienced by Home Affairs, Services Australia, Veterans' Affairs and the National Disability Insurance Agency (NDIA).
    - The Department of Home Affairs, Services Australia and the Department of Veterans' Affairs together continued to receive the majority of FOI requests received by Australian Government agencies (68% of the total). Of these, 89% are from individuals seeking access to personal information.
- Of all FOI requests made to agencies and ministers, 77% were for **personal information** (26,715) and 23% for **non-personal** (8,802). This trend has been consistent over the past 4 years.
- 26,680 FOI **requests were decided**[3] in 2020-21.
    - 10,978 FOI requests were granted in full in 2020-21 (41% of all requests decided).
      - This is a decline on 2019-20, when 47% of all FOI requests decided were granted in full.
      - There has been a gradual decline in the number of FOI requests granted in full dating back to 2011-12.

1 All percentages have been rounded to whole numbers in this brief.
2 In 2020-21, 283 agencies and ministers reported FOI statistics to the OAIC.
3 Covers access granted in full, in part or refused.

Commissioner brief: FOI Complaint issues

Key messages

- Key activities:
  - Finalisation of a cohort of 17 complaints about the Department of Home Affairs' compliance with statutory processing periods (December 2021).
  - The OAIC is now monitoring agencies implementation of recommendations made under s 88 of the FOI Act (29 recommendation cases), including recommendations to:
    - issue statements – by the CEO or Secretary – to all staff highlighting the agency's obligations under the FOI Act
    - conduct audits on its processes
    - update its policies and procedures in relation to FOI processing consistent with the findings of specific investigations
    - take remedial action including contacting FOI applicants where I found that review rights had not been included in the response to FOI requests pursuant to s 26 of the FOI Act to advise them of their review rights
    - implement training processes for staff including the use of online training
    - improvements in processes to ensure compliance with Information Publication Scheme obligations
    - appoint an Information Champion to provide leadership, oversight and accountability necessary to promote and operationalise compliance by the agency
  - As at 8 February 2022, the OAIC website has been updated to include investigation outcomes conducted between 1 July 2019 and 22 December 2021.
- Complaint issues:
  - The most complained about issue is delay by agencies processing FOI requests.
  - Other complaints relate to (in order of most complained about):
    - failure to provide assistance during the practical refusal consultation process
    - the imposition of charges
    - failure to acknowledge FOI request
    - searches
    - extension of processing time to consult with third party but no consultation required
    - poor administration/customer service

Commissioner brief: FOI Regulatory functions

Key messages

- The OAIC is an independent statutory agency established under the *Australian Information Commissioner Act 2010* (AIC Act). The AIC Act confers the Information Commissioner with power to perform FOI regulatory functions, including:
    - review of FOI decisions of agencies and ministers
    - investigating FOI complaints
    - issuing FOI guidelines
    - monitoring agencies' compliance with the FOI Act
    - making decisions on extension of time requests and vexatious applicant declarations and
    - compiling FOI data and access trends.
- ***IC reviews:*** the numbers of IC reviews on hand has increased each year for the past four years.
    - In 2020-21 we received 1,224 applications for IC review.
        - The overall increase in IC review applications from 2015-16 to 2020-21 (up to 30 June 2021) was 140%.
    - As at 31 December 2021, the OAIC had 1,485 IC review applications on hand. While the office continues to look for and implement opportunities to increase productivity in relation to its freedom of information functions, it remains the case that although significant efficiencies have been found and applied the function has not kept pace with incoming reviews.
    - The IC review jurisdiction is complex and many documents subject to IC review are sensitive (including cabinet documents, national security, defence and international relations, legally privileged document, documents affected law enforcement, and confidential documents) and often affect third parties. A high proportion of matters involve consideration of various (more than one) exemptions and hundreds of folios of material that agencies and ministers contend is exempt under the FOI Act.
    - In the absence of supplementary FOI funding, the ability of the OAIC to keep pace with increases to the review caseload will continue to be challenged. (For further information, see Commissioner Briefs - *FOI IC reviews* (D2022/000231) and FOI process review D2021/002427).
    - On 21 September 2021 the OAIC published a new Direction as to certain procedures to be followed by applicants in Information Commissioner reviews under s 55(2)(e)(i) of the FOI Act. The Direction aims to clarify the procedure for applicants in the IC review process, and is intended as a

Commissioner brief: Department of Home Affairs Commissioner Initiated Investigation (CII)

Key messages

- **On 25 October 2019**, I commenced a CII into Department of Home Affairs processing of FOI requests relating to non-personal information. The investigation considered 41 FOI requests for non-personal information.
- **On 11 December 2020**, I finalised the CII.
- The investigation indicated that the Department did not have adequate governance and systems of accountability in place to comply with statutory time frames for processing FOI requests for non-personal information.
- The investigation report noted:
    - that over the past four financial years (2016-17 to 2019-20), more than 50% of the FOI requests to Home Affairs for non-personal information were processed outside of the statutory processing period.
    - many of the findings and recommendations have been the subject of previous reports, indicating the need for sustained rectification of issues of delay.
    - factors contributing to delays include inadequate processes for addressing the escalation and finalisation of decisions, and inadequate training of non-FOI staff engaged in specific FOI requests.
- I made 4 recommendations which I consider the Department ought to implement**:**
    1. **Appoint an Information Champion:** The Information Champion may be supported by an information governance board to provide the leadership, oversight and accountability necessary to promote and operationalise compliance by the Department with the FOI Act.
    2. **Prepare and implement an operational manual for processing FOI requests for non-personal information:** The manual should as a minimum specify the steps to be taken to ensure compliance with statutory processing requirements; the steps to be taken to ensure compliance with s 6C of the FOI Act; as well as including short form guidance to assist business areas process FOI requests for non-personal information.
    3. **Training:** Provide all staff who process FOI requests with training in the requirements of the operational manual and ensure that online training about processing FOI requests for non-personal information is available to all Departmental staff.
    4. **Audit of compliance:** Conduct an audit of the processing of FOI requests for non-personal information to assess whether recommendations 2 and 3 have been implemented and operationalised and whether those actions are sufficient to address the issues identified in the CII report. A copy of the audit report is to be provided to the OAIC.

Commissioner brief: FOI OAIC engagement and Guidelines update

Key messages

- The OAIC engages widely with Information Access practitioners across Australia and overseas. The breadth of our regulatory engagement is consistent with our strategic priority to advance domestic and international access to information laws. The key areas of focus include:
    - facilitating and encouraging practices that are 'open by design'
    - ensuring proactive publication of government held information, particular during the Covid-19 pandemic
    - producing a wide range of resources and guidance that is designed to assist FOI applicants and government agencies to engage positively with the FOI Act.

- ***Open Government Partnership (OGP)***
  The OAIC continues to engage with Australian government agencies and civil society in relation to the OGP. The OAIC contributed to the development of Australia's **third National Action Plan**, including by helping design a commitment in relation to access to government information. Further information regarding the OGP is at **Attachment A** .

- ***The Association of Information Access Commissioner (AIAC)***
  The Australian Information Commissioner continues to engage with Information Commissioners and Ombudsmen from other Australian jurisdictions through the AIAC. On 24 September 2021, Australian Information Access Commissioners published a statement to promote the proactive release of information. Further information regarding the AIAC is at **Attachment B.**

- ***International Conference of Information Commissioners (ICIC)***
  The Australian Information Commissioner also engages with Information Commissioners globally through international forums such as the ICIC. Key milestones include:
    - In April 2020, May 2020 and September 2020, the ICIC **issued statements** on the right of access to information in the context of the global pandemic, the duty to document decisions and reaffirming the importance of access to information laws in building greater public trust in government. In June 2021, the Australian Information Commissioner attended the **12th annual ICIC conference** and updated members on developments in access to information laws across other jurisdictions in Australia.
    - The OAIC also put forward a **resolution** calling for the proactive publication of information relating to the COVID-19 pandemic. The Resolution was adopted unanimously by all members of the ICIC through a joint statement issued on the ICIC website.
    - Further information regarding the ICIC is at **Attachment C.**

Commissioner brief: Proactive disclosure: Information Publication Scheme and disclosure logs

Proactive publication

- Strategic Priority 3 in the OAIC's corporate plan is to encourage and support proactive release of government-held information.

Open Government Partnership

The OAIC participated in the development of Australia's **third National Action Plan**, including by helping design a commitment in relation to access to government information. Relevantly, the proposed commitments include:

- Open by Design (Right to Know): To improve the accessibility of information held by government, or under government contractual or outsourcing arrangements, by developing key features for a nationally consistent approach to the proactive release of information commonly sought by members of the Australian community or which they identify as valuable and/or necessary for open and accountable government.
- Building trust in data sharing: The Office of the National Data Commissioner will promote good practice in government data sharing by implementing the Data Availability and Transparency legislation and by publishing guidance on sharing data safely and a data sharing agreement to help protect data.
- Improving transparency and trust related to the use of emergency and crisis powers: Involves developing a centralised online 'landing page' on Australia.gov.au which may include information such as legislation, regulatory and policy documents, advice about the introduction of new legislation and its timing, the amount and allocation of funding to facilitate the crisis response and information about oversight mechanisms.
- Best practice in dealing with FOI requests: will identify differences in the way Australian Government departments and agencies process and respond to FOI requests to identify how to ensure consistency in how applicants experience the FOI system.

Association of Information Access Commissioners (AIAC)

On 24 September 2021, Australian Information Access Commissioners published an authoritative statement to promote the proactive release of information (**Attachment A**). The *Open by Design Principles* were released ahead of International Access to Information Day on 28 September, and should be used by government agencies to encourage and authorise the proactive release of information and promote open government.

The principles recognise that:

- information held by government and public institutions is a public resource

Commissioner brief: FOI Extension of time applications

Key messages

- An agency or minister must make a decision on an FOI request within 30 days, unless the timeframe has been extended.
- Where an agency or minister is unable to process an FOI request within the processing period, they may request an extension of time (EOT):
    - from the FOI applicant (by agreement under s 15AA)
    - from the Information Commissioner under:
        - s 15AB (complex or voluminous)
        - s 15AC (where the agency or minister has been **unable to process the request within the statutory timeframe)**
        - s 51DA (where the agency or minister has been unable to process the request for **amendment or annotation)**
        - s 54D (where the agency or minister has been unable to process an **internal review application** within the statutory timeframe).
- Part 3 of the FOI Guidelines encourage agencies to seek agreement with the FOI applicant prior to lodging an extension of time request with the OAIC.
- EOT applications must include reasons why the request could not be processed within the statutory processing period and provide a plan on how the further time (if granted) will be utilised by the agency or minister.
- It is important for agencies and ministers to consider early in the process whether an extension of time is required, as an application for an extension of time is not an automatic grant and each application is considered on its individual merits.

Commissioner brief: FOI funding and workload

Item/Year	**2013-14**	**2019-20**	**2020-21**	**2021-22**
Staffing	• 13 May 2014 x 25 staff headcount (budget night) • 7 October 2014 x 13 staff headcount • Excludes Executive • Excludes areas that contribute to FOI	30 June 2020: • 17 x staff headcount • Excludes Executive • Excludes areas that contribute to FOI	30 June 2021: • 21 x staff headcount • Excludes Executive • Excludes areas that contribute to FOI	As at 31 December 2021: • 21 x staff headcount • Excludes Executive • Excludes areas that contribute to FOI • A/g FOI Commissioner appointed Aug 21 • Assistant Commissioner FOI appointed Nov 21
Funding	Internal budget for 2014-15 not located. The 2014-15 financial statements show $9.365million spent on staffing. Total headcount at 30 June 2014 was 91. Therefore, approximate cost of 25x FOI staff was $2,573,000.	FOI appropriation funding not traced. However, internally allocated budget is: • FOI division: $2,430,000 • Areas contributing to FOI: $570,000 • Total FOI allocation: $3,000,000 The above figures exclude FOI overhead costs, such as rent and shared services. D2020/010201	FOI appropriation funding not traced. However, internally allocated budget is: • FOI division: $2,566,000 • Areas contributing to FOI: $605,000 • Total FOI allocation: $3,171,000. The above figures exclude FOI overhead costs, such as rent and shared services. D2021/013198	FOI appropriation funding not traced. However, internally allocated budget is: • FOI division: $2,884,000 • Areas contributing to FOI: $933,525 • Total FOI allocation: 3,818,000 The above figures exclude FOI overhead costs, such as rent and shared services. D2021/021260
IC reviews	30 June 2014: • 525 received • 646 finalised	30 June 2020: • 1,066 received • 829 finalised Comparison to 30 June 2014: • Received 103% more • Finalised 28% more • 32% fewer staff.	30 June 2021: • 1,224 received • 1,018 finalised YTD comparison to 30 June 2014: • Received 133% more • Finalised 58% more • 16% fewer staff. D2021/016546	31 December 2021: • 882 received • 698 finalised Forecast to 30 June 2022 • Forecast based on average YTD rate of receipt and finalisation. • 1,764 received • 1,396 finalised • 5% more staff.
FOI Complaints	30 June 2014: • 77 received • 119 finalised	30 June 2020: • 109 received • 71 finalised Comparison to 30 June 2014: • Received 42% more • Finalised 40% fewer • 32% fewer staff.	30 June 2021: • 151 received • 174 finalised Comparison to 30 June 2014: • Received 96% more • Finalised 46% more • 16% fewer staff.	31 December 2021: • 99 received • 97 finalised Forecast to 30 June 2022 • Forecast based on average YTD rate of receipt and finalisation. • 198 received • 194 finalised • 5% more staff.

Commissioner brief: Use of Apps to conduct government business

Key messages

- **Application of FOI Act to apps:** The term 'document' is broadly defined in the *Freedom of Information Act 1982* (FOI Act) and includes but is not limited to messages on mobile devices and messaging applications.
- **Importance of record keeping / OAIC jurisdiction:** The right of access to documents under the FOI Act is contingent on proactive information collection and retention of relevant information assets (records, information and data) by Commonwealth agencies and ministers, including information contained on mobile devices and messaging applications, and other electronic mediums, where the technology is used to conduct official government business. Issues relating to record keeping under National Archives legislation are outside the OAIC's jurisdiction and are a matter for the National Archives of Australia.
- **Agencies/reviews relating to use of apps:** A number of agencies/reviews in recent years have emphasised the importance that this type of information should be properly retained and managed to meet accountability requirements:
    - On 13 October 2015, **Mr Allan McKinnon, Deputy Secretary, National Security** advised the Prime Minister that any documents relating to ministerial duties are subject to the *FOI Act 1982*, regardless of what system that are held in. Official government information that is unclassified, sensitive or otherwise caveated can be conveyed on non-government devices and systems if done so in accordance with Information Security Manual controls.
    - **National Archives of Australia** (NAA) has published guidance about "Managing information on mobile devices", encourages emails, SMS, instant messaging and voicemails captured on mobile devices to be managed as a Commonwealth record if the information relates to an agency's business activities.
    - On 12 March 2021, the **Functional and Efficiency Review of the National Archives** led by former Department of Finance Secretary David Tune published its full report. The report noted the Archives Act is pre-digital and requires modernisation. The definition of a 'record' needs to more clearly provide for direct captures of records that are susceptible to deletion, such as emails, texts or online messages. On 19 August 2021, the Australian Government published its Response to the Tune review, agreeing to all 20 recommendations, in full or in principle. This includes Recommendation 16, which relates to modernising the Archives Act to bring it into the digital age.
    - The **Australian National Audit Office** (ANAO) has also expressed a view that a WhatsApp chat around the processes of executive government is a record, and it should be maintained and held on the record (see evidence provided by the

Commissioner brief: National Cabinet

Key messages

- On 13 March 2020, a 'National Cabinet' was established as an Australian intergovernmental decision-making forum composed of the Prime Minister and state and territory Premiers and Chief Ministers.
- The Administrative Appeals Tribunal (AAT) considered the application of the Cabinet exemption of documents of a National Cabinet. On 5 August 2021, Justice White, as a judicial member of the AAT, made a decision of *Patrick and Secretary, Department of Prime Minister and Cabinet (Freedom of Information)* [2021] AATA 2719 (5 August 2021) (see case summary at **Attachment A**).
- His Honour decided that 'National Cabinet', which consists of the Prime Minister and State and Territory Premiers and Chief Ministers, did not satisfy the requirements of 'Cabinet' as required under s 4(1) and did not constitute 'a committee of the Cabinet' for the purpose of s 34 of the FOI Act.
- On 2 September 2021, the Government introduced the COAG Legislation Amendment Bill 2021 into Parliament.
- On 2 September 2021, the Senate referred the COAG Legislation Amendment Bill 2021 (the Bill) to the Finance and Public Administration Legislation Committee for inquiry and report by Thursday, 14 October 2021.
- On 24 September 2021, the OAIC made a submission to the Committee, which was supported by all State and Territory information access commissioners and ombudsmen.
- On 27 September 2021, the Information Commissioner and staff appeared before the Committee to give evidence.
- On 19 October 2021, the Committee published its report.
- The Committee made only 1 recommendation: that the Bill be passed (at 3.89 of the report)
- Labor Senators, Australian Greens and Senator Patrick provided dissenting reports all opposing the inclusion of Schedule 3 of the Bill among other matters.
- The Bill's current status is 'before the House of Representatives'.

Commissioner brief: FOI - official ministerial documents and incoming government briefs

Key messages

- The OAIC has issued guidance for the public on accessing official documents of a minister: https://www.oaic.gov.au/freedom-of-information/your-foi-rights/requesting-official-documents-held-by-a-minister/
- A ministerial diary would be considered an 'official document of a minister' if the diary is held by the minister in their capacity as a minister, and the entries relate to the affairs of an agency.
- New technologies, such as messages in WhatsApp and Wickr, broaden the range of documents falling within the definition of 'document' in s 4(1) of the FOI Act, which includes 'any other record of information'. Agencies are expected to conduct searches of mobile devices when they may contain documents of an agency or official documents of a minister. TRIM link for reference: Commissioner brief - Guidance regarding new technologies and archives: D2019/001017; Commissioner brief – Use of Apps to conduct government business D2022/000242
- Where there is a change of minister in the course of an FOI request or an IC review, the new minister is the respondent to the FOI request or IC review.[1] This may cause the FOI Act to no longer apply to a document if the new minister does not hold a copy or does not have access to the requested document. See **Attachment 1**.
- This issue was the subject of questioning by Senators at the hearing into the COAG Legislation Amendment Bill 2021 on 27 September 2021. See **Attachment 2**.
- The National Archives of Australia (NAA) has issued the 'National Archives: General Records Authority 38' (GRA38), which sets out the types of records that must be retained by a minister or transferred to NAA under the *Archives Act 1983* (**Attachment 4**). GRA38 applies to all ministerial records, including diaries. GRA38 does not apply to Cabinet documents as defined in the Cabinet Handbook. Cabinet documents must be managed in accordance with the Cabinet Handbook or as directed by the Cabinet Secretariat, and the *Archives Act 1983.*
- The FOI Act applies to Incoming Government Briefs (IGB), as they are considered a 'document of an agency'. There is no exemption that applies universally to IGBs; rather, the question of whether an exemption applies to part of an IGB must be assessed on a case-by-case basis, with reference to the particular material in the brief.

Critical facts

Current IC reviews

- The OAIC is currently assessing a cohort of IC reviews where there has been change of Minister during the current term of the government. See **Attachment 3**. The issue in

[1] *Acts Interpretation Act* s 20.

Commissioner brief: FOI Bill report

Key messages

- On 22 August 2018, Senator Rex Patrick introduced the *Freedom of Information Legislation Amendment (Improving Access and Transparency) Bill 2018* to the Senate.
- The Bill proposed a number of amendments to the FOI Act, including requiring the positions of Information Commissioner, FOI Commissioner and Privacy Commissioner to be filled, allowing applicants to bypass the OAIC and go to the AAT if their review would take more than 120 days to finalise, preventing agencies from changing exemptions during IC review and requiring agencies to publish their external legal expenses for each IC review/AAT FOI matter.
- The Bill was referred to a Senate Committee. The OAIC made a written submission to the Committee (**Attachment 2**). I appeared at a hearing before the Committee to provide further evidence.
- On 30 November 2018, the Committee published its report recommending that the Senate not pass the Bill.
- On 31 August 2020, there was a 70-minute, second reading debate of the Bill, during which both Liberal and Labor Senators did not support the Bill being passed by the Senate. As at 5 October 2021, the Bill's status remains as 'Before Senate'.
- In recent media reports (see **Attachment A**), Senator Patrick has reaffirmed his commitment to move to amend FOI laws to streamline the review process and reduce the workload on the OAIC.
- The amendments proposed are similar to those in the 2018 Bill. Senator Patrick's amendments would require the OAIC to decide within **90 days** if a matter should be referred directly to the AAT, and if a review takes longer than six months, automatically refer it to the tribunal. The 2018 Bill proposes that applicants could proceed to the AAT after **120 days**.
- The Bill's status remains as 'Before Senate' on the Australian Parliament House website.

TRIM link for reference: Executive Brief on FOI Bill: D2018/015033
See also Com brief - FOI - IC review: D2022/000231

Critical facts

- On 22 August 2018, Senator Rex Patrick introduced the *Freedom of Information Legislation Amendment (Improving Access and Transparency) Bill 2018* to the Senate. The Bill seeks to improve the effectiveness of FOI laws 'to address the considerable dysfunction that has development in our FOI system which is now characterised by chronic bureaucratic delay and obstruction, unacceptably lengthy review processes and

Commissioner brief: FOI Act Reforms

Key messages

- The FOI Act provides a sound basis for providing access to government held information to the Australian public through formal FOI requests, the disclosure log and the Information Publication Scheme. However there is room for improvement. Possible areas for review include:
    - Examining the language of the Act, particularly in the context of the digital environment (including the use of word 'document' rather than 'information)
    - Examining the operation of other domestic and international legislation which could further promote more timely and more proactive publication of documents that are routinely requested under the FOI Act, for example, Question Time Briefs, ministerial and senior official diaries
    - Reviewing the recommendations made by the Hawke Review undertaken in 2013, including the recommendation to review the agencies listed in Part 1 of Sch 2 of the FOI Act
    - Reviewing the current structure of the Australian Information Commissioner Act 2010, particularly in relation to the power to delegate decision making
    - Reviewing Part VII of the FOI Act relating to the Review by the Information Commissioner to assist in further increasing efficiencies in the process.

- On 18 March 2021 the *Archives and Other Legislation Amendment Bill 2021* was introduced to Parliament and read before the Senate:
    - The Bill amends the *Freedom of Information Act 1982* to exclude a right of access to documents provided to, or created by, the Independent Review into the workplaces of Parliamentarians and their staff conducted under the Australian Human Rights Commission Act 1986 by the Sex Discrimination Commissioner; and Archives Act 1983 to provide that these documents would not come into the open access period until 99 years after the year the documents came into existence.
    - On 25 March 2021, during the second reading before the House of Representatives, Ms Zali Steggall OAIM, MP, Member for Warringah New South Wales proposed an amendment to the bill regarding the exclusion of material handed to the inquiry from ministers' offices and departments, so that the bill does *not* affect existing FOI rights. (Schedule 1, item 7, page 4)
    - On 11 May 2021, Senate agreed to the House of Representative amendment above and the Amendment Bill passed both Houses on the same day.
- The 2013 Hawke Report into the FOI Act, identified a number of areas in which changes could be made to the FOI Act which will increase its ability to delivery transparency and accountability for the Australian public.

Commissioner brief: Grata Fund FOI Report

Key messages

- On 19 August 2021, the Grata Fund (a not for profit organisation sponsored by the University of NSW), published a report *FOI Litigation Hit List* on Australia's FOI system (**Attachment A**).
- The reports identifies a number of systemic issues in the administration of the FOI Act including:
    - overuse and under justification of exemptions
    - unreasonable delays and failure to comply with statutory timeframes
    - unreasonable expense
    - a culture within government of resisting FOI applications.
- The report sets out four areas where the handling of FOI requests would 'most likely be found unlawful' and contemplates using strategic litigation to test a series of issues before the federal court or administrative appeals tribunal. These are:
    - inappropriate use of cabinet confidentiality to block requests
    - refusal of FOI requests because of a change in or resignation of a Minister
    - the unreasonable refusal of FOI requests seeking text, Whatsapp, Signal or other electronic messages.
    - unreasonable delay by the OAIC in deciding reviews
    - overuse of exemptions without substantiation by government agencies or Ministers, in particular:
        - Personal privacy (s 47F)
        - Certain operations of agencies (s 47B)
        - Enforcement of law and public safety (s 37)
        - Deliberative processes (s 47C)
        - Confidential information (s 45)
        - Trade secrets and commercially valuable information (s 47)
- The report states that 'clarification of these provisions of the FOI Act, through the AAT or Federal Court, would create enforceable obligations on government bodies to apply the exemptions consistently with the Court's or Tribunal's rulings.'
- The report uses statistics from the OAIC's 2019-20 annual report to support some of its findings.

Commissioner brief: Investment Funds Legislation Amendment Bill 2021

Key messages

- On 25 August 2021, the Investment Funds Legislation Amendment Bill 2021 was introduced (**Attachment A**).
- Schedule 2 of the Bill inserts a provision which would make documents handled by the Future Fund Board of Guardians and the Future Fund Management Agency in relation to the board's investment activities, exempt under Division 1 of Part II of Schedule 2 of the FOI Act.
- This means all documents that relate to investment activities of the board would be excluded from release under the FOI Act.
- The FOI Act would continue to apply to the board and agency in respect of documents concerning non-investment activities, such as operational functions.
- On 7 July 2021, the FOI Regulatory Group provided a bill scrutiny response to the Attorney-General's Department (AGD) (**Attachment B**). In summary we said:
    - most of the types of documents in Part II of Schedule 2 of the FOI Act relate to intelligence agencies and the commercial activities of agencies
    - the protection of sensitive government information should be achieved by applying existing exemptions to specific documents, rather than applying exemptions to agencies' functions
    - the OAIC considers the existing exemptions in the FOI Act will provide appropriate protection for sensitive information held by the agency and board.
- On 2 September 2021 the Bill was referred to the Senate Finance and Public Administration Legislation Committee. The committee held a public hearing on 28 September 2021.
- On 14 October 2021, the committee published its report. The committee recommended that the Bill be passed.
- The committee concluded that 'the partial FOI exemption is needed to provide certainty to the Future Fund Board and Agency, and its investment managers, that commercially sensitive information relating to the fund's investment activities would not be at risk of FOI disclosure. The

Commissioner brief: Deputy Commissioner role

Key messages

- On 26 February 2021 Senator Murray Watt asked a *Parliamentary Question on Notice* (SQoN 3223) of the Minister representing the Attorney-General in the Senate relating to the Office of the Australian Information Commissioner (OAIC).
- The SQoN 3223 was comprised of a series of questions about the appointment of the current Deputy Commissioner to the OAIC and the Deputy Commissioner's work both in her current position and in her previous roles within the Department of Home Affairs.

Critical facts

- The SQoN 3223 was originally directed to Senator the Hon Marise Payne, the Minister at the time representing the former Attorney-General, the Hon Christian Porter MP. (The Minister to whom the question was asked, in their capacity as the Attorney's representative, is responsible for answering the question in the Senate).
- Input to the SQoN 3223 was sought, and provided by (on 12 March 2021), from the Department of Home Affairs (DHA) on questions relating to positions held by the Deputy Commissioner in the Home Affairs portfolio.
- The draft response to the SQoN 3223 was authorised by the Australian Information Commissioner and forwarded to the Attorney-General Department's Cabinet, Legislation and Estimates team on 12 March 2021.
- The question was answered on 22 March 2021 – refer: https://www.aph.gov.au/Parliamentary_Business/Chamber_documents/Senate_chamber_documents/qon.

Possible questions

1. **What was the nature of the questions concerning the Deputy Commissioner?**

   The *Parliamentary Question on Notice, SQoN 3223*, related to the recruitment, employment, and management of conflicts of interest regarding the Deputy Commissioner.

2. **What date did the OAIC provided its response to the Attorney-General's Department?**

   The OAIC provided its draft response to the SQoN 3223 to the Attorney-General's Department on 12 March 2021.

Commissioner brief: Monitoring agency and ministers' compliance with the FOI Act

Key messages

The table below sets out key statistics related to the compliance of particular agencies and Ministers with the FOI Act.

Agency	2020-21 FOI requests received	2020-21 FOI requests finalised	2021-22 FOI requests received to 31/12/21	2020-21 Decisions made out of time	2020-21 Complaints received	Complaints on hand (as at 9/2/22)	2020-21 IC reviews received	2021-22 IC reviews received (to 31/12/21)	IC reviews on hand	2020-21 IC reviews - % deemed	2021-22 IC reviews - % deemed to 31/12/21	2020-21 EOT applications received requiring IC decision
PMC	181 (down 47% on 19-20)	151 (down 34% on 19-20)	164 (328 p.a)	5	2 (4 in 21-22)	5	28	16	49	18% (5/28)	6% (1/16)	24 (up 118% on 19-20)
PMO	61 (down 40% on 19-20)	36 (down 46% on 19-20)	42 (84 p.a)	22	N/A	N/A	12	4	18	67% (8/12)	100% (4/4)	7 (up 250% on 19-20)

Commissioner brief: FOI Regulatory Action Policy
D2021/002429

Key messages

- On 19 September 2017, the Australian National Audit Office (ANAO) tabled and published a report on its performance audit on the administration of the FOI Act.
- The ANAO recommended that the OAIC develop and publish a statement of its FOI regulatory approach.
- The OAIC published a 'Freedom of information regulatory action policy' on 22 February 2018.
- The OAIC is currently reviewing the FOI Regulatory Action Policy.

Critical Issues

- On 19 September 2017, the ANAO published a report auditing the administration of the FOI Act. The ANAO observed that since 2012 the OAIC has undertaken limited FOI regulatory action and does not have a statement of its regulatory approach in relation to FOI.
- The ANAO recommended that the OAIC develop and publish a statement of its FOI regulatory approach. The OAIC agreed to this recommendation.
- The OAIC's 2017–18 Corporate Plan contained a commitment to develop an FOI regulatory action policy which outlines the OAIC's regulatory approach with respect to FOI functions.
- The OAIC developed a policy outlining and explaining the Australian Information Commissioner's approach to using FOI regulatory powers. The policy covers all FOI powers and functions conferred on the Information Commissioner by the *Australian Information Commissioner Act 2010* and the FOI Act.
- The policy should be read together with the Guidelines issued by the Australian Information Commissioner under s 93A of the FOI Act (FOI Guidelines).
- The policy documents:
    - the Commissioner's goals in taking FOI regulatory action
    - the Commissioner's regulatory action principles
    - the Commissioner's regulatory powers, which include IC review, investigating FOI complaints, issuing FOI Guidelines, extending the time to decide FOI requests, declaring a person to be a vexatious applicant, making disclosure log determinations, overseeing the Information Publication Scheme, raising awareness of FOI and educating Australians and agencies about their rights and obligations, compiling FOI data and assessing trends, and making recommendations on the operation of the FOI Act.
    - the approaches to regulatory action in relation to each power

Commissioner brief: OAIC Commissioner structure'

Key messages

- Angelene Falk is the Australian Information Commissioner and Privacy Commissioner. The Australian Information Commissioner also currently exercises the freedom of information (FOI) functions provided in the *Australian Information Commissioner Act 2010*.
- Recently the Office of the Australian Information Commissioner (OAIC) has welcomed additional funding ($1 million a year) as announced in the 2021-22 Federal Budget which will assist with the freedom of information (FOI) functions within the OAIC, including the appointment of a Freedom of Information Commissioner and an additional Assistant Commissioner.
- The OAIC has operated under a 'one Commissioner model' since August 2015, under Timothy Pilgrim PSM until March 2018 and since then under Angelene Falk until August 2021.
- Deputy Commissioner Elizabeth Hampton was appointed to act as Acting FOI Commissioner, for a term of 3 months, beginning on 13 August 2021 or until substantive appointments have been made, depending on which date is earlier.

The OAIC is currently advertising for an Assistant Commissioner, Freedom of Information to support the new FOI Commissioner.[1] **Critical facts**

In Australian and international jurisdictions, Information Commissioners are typically appointed by relevant ministers or heads of state following consultation or on recommendation.

The OAIC model

- The *Australian Information Commissioner Act 2010* (AIC Act) establishes the OAIC and provides for the appointment of the Australian Information Commissioner, the Privacy Commissioner and the Freedom of Information Commissioner (FOI Commissioner).
- The Information Commissioner is the agency head and responsible for the information policy function. As the agency head, the Information Commissioner also has formal responsibility for the FOI and privacy functions, and for exercising the powers conferred by the *Freedom of Information Act 1982* and the *Privacy Act 1988.*
- Since July 2015, the OAIC has operated with a 'one Commissioner model'. That is, the same person occupies the roles of Information Commissioner and Privacy Commissioner and as well carries out the FOI functions.
- Angelene Falk has been reappointed as both the Australian Information Commissioner and Privacy Commissioner, for a term of 3 years, beginning on 16 August 2021.
- Angelene Falk will be supported by a newly appointed FOI Commissioner.
- Deputy Commissioner Elizabeth Hampton was appointed to act as Acting FOI Commissioner, for a term of 3 months, beginning on 13 August 2021 or until substantive appointments have been made, depending on which date is earlier..
-

Legislative framework

- Section 7 of the *Australian Information Commissioner Act 2010* defines **information commissioner** functions as follows:
  (a) to report to the Minister on any matter that relates to the Commonwealth Government's policy and practice with respect to:

[1] https://www.oaic.gov.au/assets/about-us/join-our-team/Candidate-information-pack-Assistant-Commissioner-Freedom-of-Information.docx

Commissioner brief: Entities excluded from the Privacy Act and FOI Act

Key messages

Press Freedoms / FOI

- Most Australian Government agencies are subject to the FOI Act but there are some exclusions, principally for intelligence agencies.
- Although Criminal Code makes unauthorised disclosure of information by a public servant a criminal offence, s 38 of the FOI Act allows agencies to refuse access to documents if disclosure is prohibited by law.
- The PJCIS conducted an inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press. In August 2020 the Committee published a report entitled *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press*.[1]

Privacy Act / data matching

- The Privacy Act excludes certain entities, including intelligence agencies such as ASIO or ASD (s7)
- There are restrictions around which entities can access the different functions of identity-matching services. These exclusions are particularised in the IMS Bill and the subordinate agreements.
- There are also exceptions in certain Australian Privacy Principles (e.g. APP 3.4; 6.2) that allow for the collection, use and disclosure of personal information by enforcement bodies
- Recent legislative amendments did not change the entities that are currently excluded by the Privacy Act.[2] In reviewing the Privacy Act, the OAIC will consider the coverage of the Privacy Act, current exemptions and whether to make recommendations on the removal of any exemptions.

Background

Agencies excluded from the FOI Act

The *Freedom of Information Act 1982* (**FOI Act**) applies to Departments of State, 'prescribed authorities' and Norfolk Island authorities.

Generally all Australian Government agencies (i.e., Departments of State, prescribed authorities and Norfolk Island authorities) will be subject to the FOI Act *unless the FOI Act expressly provides otherwise*.

The FOI Act contains a number of exclusions to this general rule. These exclusions relate to:

1. Specific agencies – see Table 1 at **Attachment A**.
2. Courts and tribunals with respect to their judicial functions – see Table 2 at **Attachment A.**
3. Particular types of documents held by specific agencies – see Table 3 at **Attachment A.**

Ministers are also subject to FOI Act but only in relation to 'official documents of a Minister'. An 'official document of a Minister' is a document in the minister's possession that relates to the affairs of an agency or Department of State. This excludes documents relating to party political or personal matters.

Interaction between Australia's secrecy laws and the FOI Act

[1] Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (August 2020) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/FreedomofthePress/Report>.

[2] *Privacy Amendment (Public Health Contact Information) Act 2020*.

Commissioner brief: Libra/Novi Financial

Key messages

- The OAIC is working with interested Commonwealth regulators and international data protection authorities to provide a co-ordinated response to this project.
- The OAIC is considering information provided by Novi Financial and Diem (the former Libra Association) so that it can properly assess the privacy implications of this new cryptocurrency and wallet.
- The OAIC understands that Diem and Novi Financial will launch in Australia when they have received appropriate regulatory approvals. A date has not been confirmed to the OAIC.

Critical Issues

- The global scope of this project amplifies privacy risks.
- This is particularly due to the potential participation of large personal information holders such as Novi Financial (subsidiary of Facebook) and Uber (a member of the Diem).
- The multi-national nature of the project may also raise jurisdictional issues, meaning that it is important to ensure that entities that hold the personal information of Australians are captured by the Privacy Act.

Possible questions

- **What will the OAIC's oversight role be for the proposed Diem cryptocurrency?** I am seeking further clarification on the structure of the Diem and Facebook's subsidiary Novi Financial. It is expected, however, if Diem and Novi Financial are offering services to individuals in Australia, these entities will fall under my office's existing oversight of the Privacy Act. These include powers that allow me to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred.
- **What are the next steps?** I am currently considering information from Diem and Novi Financial about the privacy implications of the Diem cryptocurrency and Novi Financial's digital wallet. I will also continue to engage with international privacy regulators to ensure a co-ordinated international response to this project.
- **What actions can the OAIC take if Diem is launched before the project receives regulatory approval?** I have a range of enforcement powers under the Privacy Act which may be appropriate depending on the particular circumstances. For example, the Privacy Act gives me the power to conduct investigations on my own initiative where an act or practice may be an interference with the privacy of an individual or a breach of the APPs. I can also apply to the Federal Court or Federal Circuit Court for an injunction where a person has engaged, is engaging or is proposing to engage in any conduct that constitutes or would constitute a contravention of the Privacy Act.

Key dates

- 18 June 2019 – Libra Association announces the Libra cryptocurrency and Facebook announces the creation its subsidiary Novi Financial
- 9 July 2019 – Interested Commonwealth regulators meet with Facebook
- 6 August 2019 – OAIC join with global privacy regulators to issue joint privacy expectations for the Libra Association, Novi Financial and future Libra digital wallet providers

Commissioner brief: OAIC regulation of privacy matters relating to offshore contracts

Key points

- Under the *Privacy Act 1988* (Privacy Act), entities have a number of privacy obligations in regard to offshore contracts:
    - For example under section 95B agencies have obligations in relation to Commonwealth contracts to take contractual measures to ensure that a contracted service provider (CSP) for the contract does not do an act or engage in a practice that would be a breach of the APPs if done by the agency.
    - APP entities (agencies and organisations) have obligations under APP8 to ensure that if an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.
    - An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (s 16C).

Previous assessment - DIBP's offshore contracts

- Under the Privacy Act, the Department of Immigration and Border Protection (DIBP) (now Home Affairs) has a number of privacy obligations in regard to its CSPs.
- In 2016, the OAIC assessed DIBP's contract management in relation to privacy matters for the CSPs operating at its regional processing centres (**RPCs**). Specifically, whether DIBP met its obligations under APP 1.2 (Open and transparent management of personal information) and APP 11 (Security of personal information), and s 95B of the Privacy Act.
- At that time, the OAIC found that DIBP did not have in place adequate formal policies for engaging DIBP's privacy staff and that contractual terms did not adequately safeguard personal information that may be held by the CSPs.
- The OAIC recommended that DIBP include additional provisions relating to privacy and information security in its contracts for services in its RPCs, its contracts for services in its RPCs should include specific

Commissioner brief: Surveillance in Australia

Key messages

- 'Protection from surveillance is a fundamental form of protection of privacy, particularly in the digital era' – 'Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (Report 123)'.
- There are many different forms of surveillance including physical surveillance, communications surveillance, data surveillance, and body surveillance, and numerous different Commonwealth, State and Territory, or local government laws that can apply depending on the particular act or practice in question.
- The OAIC is interested in forms of surveillance where an act or practice involves the collection of personal information. Where surveillance activities involve the collection of personal information, this can raise privacy issues involving notice, gaining meaningful consent, potential secondary uses of personal information, security of datasets and the potential for datasets to be combined with others to create a detailed picture of individuals.

Critical facts

- The *Privacy Act 1988* (Cth) (Privacy Act) recognises that the right to privacy is not absolute and must be balanced with the interests of entities in carrying out their functions or activities. The impact on privacy of any proposed surveillance activities by Australian Government agencies should therefore be reasonable, necessary and proportionate to achieving a legitimate public policy objective.
- The Privacy Act applies to surveillance activities undertaken by Australian Government agencies and private sector organisations covered by the Act, where the activities involve the handling of personal information.
    - There are specific exemptions from the Privacy Act (or parts of the Privacy Act) for entities or acts and practices, such as intelligence agencies under s 7 of the Privacy Act. These exemptions are contained in the Privacy Act itself or in other legislation.
- Surveillance activities will usually involve the collection of personal information and may often involve the collection of sensitive information (e.g. through biometric scanning and security cameras). Sensitive information includes information about an individual's racial or ethnic origin, religious beliefs or affiliations, health information and biometric information.
- Where sensitive information is collected, the Privacy Act requires entities to obtain consent to the collection, or rely on another exception to permit the collection, such as if the collection is required or authorised by an Australian law or a court/tribunal order.
- The OAIC has published guidance on several different types of surveillance including: Security Cameras, Drones, ID Scanning and Biometric Scanning and has also published extensive guidance on the collection, use and disclosure of 'personal information' under the Privacy Act which can extend to some forms of surveillance.
- Changing and emerging technologies allow for increased collection of personal information which can then be used to drive mass surveillance activities.
- The OAIC is considering its approach to surveillance activities in today's changing technological environment, particularly as new forms of health surveillance emerge during the COVID-19 pandemic.

Commissioner brief: FOI process review D2021/002427

Key messages

- In April 2019, the OAIC engaged an external consultant, Synergy, to further explore opportunities for efficiencies in the IC review process.
- Opportunities and improvements identified by Synergy generally fall into 2 categories:
  - use of technological tools to reduce administrative processes
  - streamlining case management and clearance processes.
- Some of the opportunities and improvements identified were already in the process of implementation, while others have now been implemented.
- In the absence of supplementary FOI funding, the ability of the OAIC to keep pace with increases to the review caseload will continue to be challenged.

Critical facts

- There has been a year-on-year increase in the number of IC review applications received by the OAIC since 2014–15.[1] In 2020-21, there was an 15% increase the number of applications received when compared with 2019-20.
- Synergy conducted preliminary research and preparatory activities, including meetings with the Deputy Commissioner, Principal Director and FOI Regulatory Group, as well as facilitating a business planning workshop in April 2019 which sought to:
  - develop the FOI Regulatory Group's priorities for the next three months;
  - examine the current IC Review business process to identify pressure points and opportunities for improvement; and
  - conduct a high-level assessment of the environmental factors that influence the efficiency and effectiveness of the FOI Regulatory Group and the IC Review process.
- The three key objectives identified by the FOI Regulatory Group were:
  (1) Improve IC Review timeliness,
  (2) 50% of matters allocated as at 1 July 2019 that are 12 months or older, to be finalised within three months, and
  (3) Work with the Information Commissioner to drive best practice FOI regulatory action across government and to support objectives (1) and (2).
- In relation to objective (2), the FOI Regulatory Group achieved 50% of the target, which resulted in 25% of reviews that were over 12 months old as at 1 July 2019 being either finalised or progressing to the Executive for clearance/consideration.
- These cases are complex and may not always be resolved informally.
- Opportunities and improvements identified by Synergy generally fall into 2 categories:
  - use of technological tools to reduce administrative processes

[1] In 2020-21, there was a 15% increase in the number of IC review applications compared with 2019-20. In 2019-20, there was a 15% increase in the number of IC review applications compared with 2018-19. In 2018-19, there was a 16% increase in IC reviews compared with 2017–18. In 2015–16 there was a 37% increase on 2014–15, in 2016–17 a 24% increase and 2017–18 a 27% increase. Between 2014–15 and 2019-20 there was a 185% increase in IC reviews.

Commissioner brief: Vexatious applicant declarations

Key messages

- The Information Commissioner has the power to declare a person to be a vexatious applicant if they are satisfied that the grounds set out in s 89L of the FOI Act exist.
- A declaration has the practical effect of preventing a person from exercising an important legal right conferred by the FOI Act. For that reason, a declaration will not be lightly made, and an agency that applies for a declaration must establish a clear and convincing need for a declaration.
- A declaration by the Information Commissioner can be reviewed by the Administrative Appeals Tribunal.
- To date, no Information Commissioner has made a decision to declare a person a vexatious applicant on their own initiative and there would need to be compelling circumstances for the Information Commissioner to consider exercising this discretion.
- Part 12 of the FOI Guidelines provide details of the process undertaken by the Information Commissioner when considering her discretion whether or not to declare a person to be a vexatious applicant.
- Part 12 of the FOI Guidelines were updated in November 2019 to reflect recent Information Commissioner decisions, provide further guidance on the steps agencies and ministers should take before and after making an application for a vexatious applicant declaration and further guidance on the circumstances in which the Information Commissioner declare a person to be a vexatious applicant.

Year	Number of applications received	Number of applications finalised
2017-18	0	2 (from previous year)
2018-19	9	8 (3 made; 3 refused; 2 withdrawn)
2019-20	3	1 (1 made)
2020-21	3	5 (2 made; 1 refused; 2 s 89M refusals)
2021-22	5	2 (1 refusal; 1 withdrawn)

See table at **Attachment 1** for details of the declarations made in 2018-19, 2019-20, 2020-21 and Q1 of 2021-22. Information Commissioner vexatious applicant declarations are generally published on AustLII.

Possible questions

When would the Information Commissioner declare a person to be a vexatious applicant?

- Part 12 of the FOI Guidelines explain that the Information Commissioner may declare a person to be a vexatious applicant only if the Commissioner is satisfied that:
  (a) The person has repeatedly engaged in **access actions** that involve an **abuse of process**.
  (b) the person is engaging in a particular access action that would involve an **abuse of process**, or
  (c) a particular access action by the person would be **manifestly unreasonable** (s 89L(1)).
- An '**access action**' is defined under s 89L(2) as:

Commissioner brief: Complaint backlog strategy and 3 year funding

Key messages

- In 2019, the OAIC was provided with an additional $25.1 million over 3 years (including capital funding of $2.0 million) to facilitate timely responses to privacy complaints and support strengthened enforcement action in relation to social media and other online platforms that breach privacy regulations.
- The OAIC used part of this funding to reduce the backlog of privacy complaints.
- The OAIC took a multi-pronged approach, focusing on the processes around new incoming complaints, the older complaints awaiting investigation, conciliation, and the matters requiring determination by the Commissioner.
- Due to these efficiencies—and with the support of additional funding—the OAIC closed 3,366 privacy complaints during the 2019-20 financial year–a 15% improvement on 2018–19, and xxxx privacy complaints during the period 1 July 2020 to 1 March 2021.

Critical facts

- Over the last few years, until the Covid-19 pandemic, the OAIC has experienced a steady increase in the number of complaints received. This, coupled with static resourcing and staffing levels, resulted in an increase and backlog of complaints waiting to be allocated to case officers: for early resolution, and if not resolved, for investigation.
- In the first year of the privacy backlog project relevant Directors and Team Managers reviewed statistics and team processes to consider any efficiencies that might be achieved both within each team, and to the overall complaint process.
- Contractors were engaged to increase the number of staff in each complaint team, and to establish a new determinations team.
- The Directors of the two complaint teams (Early Resolution and Investigation & Conciliations) and the new Determinations team worked closely together to develop new strategies and processes to streamline the complaint process. These included:
    - reviewing our complaint management system to identify any changes that would assist staff in processing matters more swiftly
    - establishing new queues in our complaint management system, to further differentiate types of matters
    - updating template letters to ensure key messages were communicated to parties
    - introducing tighter timeframes in the complaint handling process to streamline matters through early resolution
    - establishing tight timeframes for completion of an investigation where early resolution was not successful

Commissioner brief: Data Encryption

Key messages

- The encryption technology that can obscure criminal communications and threaten our national security is also used by ordinary Australians to exercise their legitimate rights to privacy.
- However, the OAIC recognises that there are new and complex challenges facing law enforcement agencies in the digital age. There is a need to provide these agencies with greater access to encrypted information to address national security threats, serious criminal activities, and to enable timely international cooperation.
- The OAIC has provided submissions in relation to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (the Act) since the Exposure Draft stage. While some mechanisms have been built into the Act to reduce privacy risks, including the requirement to take account of privacy considerations before issuing notices, the OAIC has recommended:
    - judicial oversight at the time notices are issued
    - judicial review of decisions
    - ongoing legislative review of the Act as a whole.
- On 30 June 2020, the Independent National Security Legislation Monitor (INSLM) completed his report to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the Act and related matters. The INSLM's 33 recommendations agreed (or partially agreed) with our recommendations made to him on 20 September 2019, and our outstanding privacy concerns generally.
- We understand that the PJCIS's review is continuing and will 'build on the findings presented in the INSLM's report.'[1]

Critical facts

- To date, we have made five submissions on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Act) (Bill) and the Act:
    - Home Affairs public consultation (12 September 2018)
    - First Inquiry of the PJCIS (15 October 2018)
    - Second PJCIS Inquiry (27 February 2019)
    - Third PJCIS Inquiry (25 July 2019)
    - INSLM Review (20 September 2019).

INSLM report to the PJCIS

[1] https://www.aph.gov.au/About_Parliament/House_of_Representatives/About_the_House_News/Media_Releases/Intelligence_Committee_publishes_INSLM_report_reviewing_telecommunications_amendments

Commissioner brief: Data Matching Department of Human Services/ Services Australia/Centrelink

Key messages

- Automated data matching streamlines and enhances the accuracy of Government department welfare program service delivery. Data matching activities using personal information must accord with the Privacy Act and associated legislative requirements.
- The OAIC has regulatory oversight of government data matching under:
    1. The *Data-matching Program (Assistance and Tax) Act 1990* (the Data Matching Act) and the Guidelines for the Conduct of Data-Matching Program (the statutory guidelines) which apply when Tax File Numbers (TFNs) are used for data matching.[1] Only Services Australia and the Department of Veterans' Affairs (DVA) reported using these Guidelines during the 2019-20 FY. The Guidelines will sunset 1 October 2021. My office will continue to liaise with Services Australia and DVA to facilitate the remaking of these Guidelines.
    2. Part VIIIA of the *National Health Act 1953* matching of information held by the Chief Executive Medicare for the purposes of ensuring the integrity of Medicare programs including the Medicare Benefits Schedule and Pharmaceutical Benefits Scheme (MBS/PBS).[2]
    3. The Guidelines on Data Matching in Australian Government Administration (voluntary guidelines). Several agencies have adopted the voluntary guidelines and must seek an exemption from the Commissioner to depart from them (despite breaching the voluntary guidelines not necessarily being a breach of the Privacy Act). The OAIC is currently considering the Guidelines.
- The OAIC have undertaken six privacy assessments examining government data-matching practices. Five assessments have been finalised and for one assessment the OAIC is consulting with the targets regarding the draft report prior to publication .
- The OAIC's assessment of Services Australia[3] Pay-As-You-Go (PAYG) program (which utilised Centrelink's compliance program) found that Services Australia has taken some steps to address issues with the quality of the personal information it collects, but also identified potential privacy risks associated with the PAYG program and made five recommendations to address these risks. All recommendations have been implemented.

[1] TFNs can also be used by agencies when undertaking data-matching outside of the Data Matching Act, for example under the voluntary guidelines, provided that their handling is in accordance with legislative obligations relating to the handling of TFNs found in the *Privacy (Tax File Number) Rule 2015* issued under s 17 of the Privacy Act and other laws including (but not limited to) the APPs and the *Taxation Administration Act 1953*.

[2] The *Health Legislation Amendment (Data-matching and Other Matters) Act 2019* amended the Privacy Act and added s 33C(f) which states that the Commissioner may conduct an assessment of whether the matching of information under Part VIIIA of the National Health Act 1953, and the handling of information relating to that matching, is in accordance with that Part.

[3] Formally known as Department of Human Services' (DHS)

Commissioner brief: Data Retention Regime

Key messages

- The data retention regime (Regime) under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) requires telecommunication service providers (service providers) to retain telecommunication metadata for a minimum of two years. Sections 306 and 306A of the *Telecommunications Act 1997* (Telecommunications Act) require carriers, carriage service providers, and number-database operators, to make records of their disclosure of certain information, including the information disclosed under the TIA Act. The OAIC has the role of overseeing record keeping practices under s 309 of the Telecommunications Act.
- On 28 October 2020, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) handed down its report on the statutory review of the Regime. The review made 22 recommendations which aim to enhance the Regime's operation, governance, and oversight, and to improve transparency, proportionality, and accountability.
- The Review echoed eight recommendations made by the OAIC in its July 2019[1] and February 2020 submissions.[2] This includes recommendations to limit authorised disclosures to agencies listed in s 110A of the TIA Act, define the terms 'content or substance', and amend the Privacy Act to capture state and territory enforcement agencies under the notifiable data breach scheme. The OAIC has been consulting with the Department of Home Affairs and the Attorney-General's on the Government response to the Review.

Critical facts

- Since 2015, the OAIC has undertaken work to identify and mitigate key privacy risks in the information handling lifecycle of Regime data. This includes undertaking inspections and follow-up assessments of Telstra, Optus, Vodafone, and TPG's record keeping practices under s 309 of the Telecommunications Act in 2015[3] and 2017.[4]
- In 2016-2017, the OAIC assessed four service providers' information security practices under Australian Privacy Principle (APP) 11.[5]
- Across the 2017-18 and 2018-19 financial years, the OAIC undertook another series of APP 11 assessments of four service providers' implementation of their requirements under the Regime. The OAIC published a summary of these assessments in February

[1] https://www.oaic.gov.au/engage-with-us/submissions/review-of-the-mandatory-data-retention-Regime-submission-to-the-parliamentary-joint-committee-on-intelligence-and-security-pjcis/.
[2] https://www.oaic.gov.au/engage-with-us/submissions/review-of-the-mandatory-data-retention-regime-supplementary-submission-to-the-parliamentary-joint-committee-on-intelligence-and-security/
[3] https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-oaics-inspection-of-telecommunications-organisations-records-of-disclosure-under-the-telecommunications-act/.
[4] https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-follow-up-of-s309-telecommunication-inspections/
[5] https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-oaic-assessment-of-telecommunication-organisations-information-security-practices-when-disclosing-personal-information-under-the-telecommunications-interception-and-access-act-1979/.

Commissioner brief: Public servants' names and contact details D2020/017455

Key messages

- On 1 July 2019, the OAIC published a discussion paper on the disclosure of public servants' names and contact details in response to FOI requests. The consultation period was initially for four weeks, but was extended until 9 August 2019 at the request of interested parties.
- The purpose of the consultation was to canvass views on the issues raised in the paper and to consider whether there was evidence to support change to the FOI Guidelines.
- The OAIC received 51 submissions:
  - 34 from Australian Government agencies
  - 9 from individuals
  - 6 from other Information Commissioners/Ombudsmen
  - 2 from organisations (OpenAustralian Foundation and the CPSU).
- On 20 August 2020, the OAIC issued a position paper outlining our approach to this issue (**Attachment C**).
- The OAIC considered the submissions in the context of a broader review of the FOI Guidelines.
- The OAIC is currently updating Parts 3 (Processing and deciding requests for access) and 6 (Conditional exemptions) of the FOI Guidelines to reflect the position outlined in the paper.
- The paper was recently considered by the Administrative Appeals Tribunal in *Warren; Chief Executive Officer, Services Australia and (Freedom of information)* [2020] AATA 4557 (9 November 2020).

Critical facts

- On 1 July 2019, the OAIC published a discussion paper '*Disclosure of public servants' names and contact details'* on the OAIC website.
- The purpose of the discussion paper was twofold:
  - to provide greater awareness of the guidance and decisions regarding disclosure of public servants' names and contact details, including when they may be released and when they may be exempt
  - to explore agency concerns and practices (**Attachment A**).

Commissioner brief: DHA [redacted]

Key messages

- On [redacted] a person in immigration detention made a privacy complaint to the OAIC about the Minister for Home Affairs.
- An investigation was commenced on [redacted] and is in its final stages.
- The OAIC is committed to ensuring that all public statements on its privacy regulatory action are accurate, fair and balanced, and comply with the OAIC's legal obligations with regards to privacy, confidentiality, and secrecy.
- Generally, I do not comment publicly on the specifics of my investigations until the matter has been finalised.[1]
- The OAIC handles privacy complaints, including those against Government Ministers, in accordance with the OAIC's *Privacy regulatory action policy*[2] and *Guide to privacy regulatory action.*[3]
- Particular considerations and reasons for my decisions are set out in my determinations available on the OAIC website.[4]

Critical issues

[redacted]

[1] *Privacy regulatory action policy.* Paragraphs [53] - [59]. https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/#public-communication-as-part-of-privacy-regulatory-action
https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/
[2] https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/
[3] https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/
[4] https://www.oaic.gov.au/privacy/privacy-decisions/privacy-determinations/

Commissioner brief: PJCIS Press Freedom Report Recommendations D2021/002429

Key messages

- On 4 July 2019, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) commenced an inquiry into 'the impact of the exercise of law enforcement and intelligence powers on freedom of the press'.
- You appeared as a witness at a public hearing on 13 August 2019, with the Deputy Commissioner and Principal Director, FOI Regulatory Group.
- You responded to questions on notice, in the form of written submissions, on 27 August 2019 and 16 September 2019.
- On 26 August 2020, the PJCIS published its final report.
- Recommendation 16 recommends 'that the Australian Government review and prioritise the promotion and training of a uniform Freedom of Information culture across departments, to ensure that application of the processing requirements and exemptions allowed under the *Freedom of Information Act 1982* are consistently applied.'
- The Government's response to the PJCIS report was published on 16 December 2020. In relation to recommendation 16, the Government states that the Attorney-General and the Attorney-General's Department will identify additional opportunities to promote training material prepared by the OAIC and associated training opportunities across its department.
- One of the draft commitments proposed in Australia's third Open Government Partnership National Action Plan builds on recommendation 16 of the PJCIS report in relation to culture within government and consistency of decision making. This commitment proposes to develop '**Best practice in dealing with FOI requests**' by surveying differences in the way Australian Government agencies process FOI requests and respond to applicants. The project will identify divergent practices and provide guidance to agencies.
- The PJCIS report recommendation is also relevant to Recommendation 2 of the Senate Environment and Communications Reference Committee's **Freedom of the press** report issued on 19 May 2021. This recommends the government work with the OAIC to identify opportunities to promote a culture of transparency consistent with the objectives of the FOI Act among Ministers, Senior Executive Service and other Freedom of Information decision-makers.
- In the lead up to International Access to Information Day on 28 September 2021, the OAIC joined information access commissioners and ombudsmen across Australia to

Developments in the online platform's environment

Law reform and Government

Key Points

- Google and Apple have recently announced key changes to their privacy practices which may have implications across the online platforms.
- Google has announced that it:
    - Intends to phase out cookies by 2022 without replacing them with another identifier to track individuals while they browse the web.
    - Will introduce a suite of privacy changes to its products and next Android 12 IOS update.
- Apple has also made several announcements including:
    - That it will require all apps on its latest operating system for iPhone to seek individual consent to share information for advertising purposes.
    - The creation of the Apple AirTags, a location tracking product to help users find their personal items which has been criticised as not doing enough to prevent misuse and potential stalking.
- Domestically, regulators are undertaking initiatives that will impact online platforms including the ACCC's adtech inquiry, the proposed Online Safety Bill and the voluntary code into disinformation and misinformation to be reviewed by ACMA.

Google ceasing to use cookies

- Timeline - Google's privacy sandbox
    - **22 August 2019** - Google announced the creation of a privacy sandbox aimed at developing solutions to protect individual privacy while supporting the advertising-based business model for the internet.
    - **14 January 2020** - Google announced that it intended to phase out the use of third-party cookies used to track people as they browse across the internet by 2022.
    - **3 March 2021** - Google stated that once third-party cookies were phased out, it will not build alternate identifiers to track individuals as they browse across the web, or use alternate identifiers in its products.