Commissioner brief: Budget and resourcing

KEY MESSAGES

- The OAIC incurred a $0.121million financial loss in 2019-20[1]
- Total revenue, including MOUs, for 2019-20 was $23.234million
- Total revenue, including MOUs, for 2020-21 is $23.271million
- 2020-21 ASL cap is 124 – actual ASL at 1 October 2020 is 112.

CRITICAL FACTS

- OAIC incurred a total (permitted) financial loss of $0.121million in 2019-20.
    - 2019-20 total revenue was $23.234million — $20.941million is appropriation, $2.323million is MOU and $36,000 received benefit for annual ANAO financial audit[2].
- 2019-20 Budget allocated $25.1 million over three 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
    - 2019-20 Budget allocated $329,000 to the 2018-19 base and $2.256million over the forward estimates for oversight of the expansion of Medicare data matching.
    - 2020-21 total revenue is $23.304million. $20.948million is appropriation and $2.323 million is MOU
- OAIC has not received additional resourcing for the Notifiable Data Breach Scheme (in 2018/19, 2019/20 or 2020/21).
- OAIC has not received additional funding for its COVID Safe App regulatory role.
- The OAIC did receive $12.911million over forward estimates for Consumer Data Right Scheme (**CDR**) in the **2018-19** Budget (including a once-off capital injection for new office space of $860,000). This is approximately $3,000,000 each year. (terminates following 2021-2022)
- s74 **External revenue (MOU)** increased from $2.257m in 2019-20 to $2.323m in 2020-21. The increase relates to the MOU with Department of Home Affairs relating to National Facial Biometric Capability.

[1] OAIC Underlying Operating Result is a surplus of $0.501 million. This is adjusted by deducting depreciation and amortization and adding the principal payment on lease liability leading to a loss of $0.121 Million. The outcome that appears in the audited financial statements and annual report is the loss of $0.121 million.

[2] A year end external audit is undertaken by ANAO for FREE, however for accounting purposes we need to recognize it as if it paid for. So our expenses include $36K for audit expense and to offset this we have $36,00 as ANAO revenue. This is called a 'received benefit'.

- In the forward estimates, MOU value is $75,000 in 2021-22 and nil after that. This is due to several MOUs (including ADHA at $2.070million) terminating at 30 June 2021 and yet to be renewed.

POSSIBLE QUESTIONS

Why did OAIC have a surplus in its underlying operating result[3]?

- Total loss is $0.121million, including depreciation and amortisation and the principal lease payment.
    - The OAIC is permitted to have a loss up to $622,000. This is the value of depreciation and amortisation, less the principal payment on lease liability.
- However, the OAIC Underlying Operating Result is a surplus of $0.501 million. This is adjusted by deducting depreciation and amortization and adding the principal payment on lease liability leading to a loss of $0.121 Million. The outcome that appears in the audited financial statements and annual report is the loss of $0.121 million.
- The Underlying Operating Result (surplus) is the result of the impact of COVID-19. Specifically, both the review of the *Privacy Act 1988* and the development of the Online privacy code were delayed as a result of the pandemic. The OAIC's planned recruitment activity was delayed and international and domestic travel halted also as a result of the pandemic. These initiatives are expected to recommence in the 2020/21 financial year.

Did the OAIC receive additional resources for the Notifiable Data Breaches scheme or the COVIDSafe App?

No, there were no additional resources provided for either function, work is prioritised within the existing resource allocation.

What activities will you undertake with the increase of funding by $25.121million allocated for over three years commencing in the 2019-20 Budget to undertake regulatory functions, including regulating the handling of personal information and taking enforcement action?

The OAIC continues to undertake careful planning to ensure that we identify the components of each of the new functions, consider sequencing and recruit people with the right skillset to deliver them. The OAIC's average staffing level increased from 85 in June 2019 to 95 by June 2020 to 112 at 1 October 2020.

Does this funding include an allocation for freedom of information?

No. The funding is for privacy functions. The office continues to look for and implement opportunities to increase productivity in relation to its freedom of information regulatory functions. There has been an increase of 72% in the number of IC reviews finalised by the OAIC between 2014-15 and 2019-20. However, it remains the case that although

[3] Senators will not have the Underlying Operating Result figure from the annual report. However, it is possible they may understand the financial approach and determine that there was a surplus or question the outcome.

demonstrated significant efficiencies have been found and applied, the function output has not kept pace with incoming IC reviews, FOI complaints, extension of time applications and applications for vexatious applicant declarations complaints and decision reviews. There has been a 186% increase in Information Commissioner reviews received between 2014-15 and 2019-20.

What activities are you undertaking with the increased of funding for Medicare data matching?

Enquiries, complaints, conciliation, investigation, CIIs, assessments.

The funding enables the OAIC to undertake two privacy assessments (audits) per year to proactively monitor whether information subject to the new arrangements is being maintained and handled in accordance with the relevant legislative obligations and recommend how areas of non-compliance can be addressed and privacy risks reduced.

Funding for Expanding Digital Identity commences in 2021-22. Are you required to undertake any activities this financial year and what will you do with the funding next financial year?

The OAIC is not receiving funding for activities in relation to this project in 2020-21, however we will continue to undertake our normal monitoring and guidance-related functions to help ensure that the expansion of the scheme includes appropriate privacy protections and aligns with the objects of the Privacy Act.

The funding in 2021-22 will enable the OAIC to undertake two privacy assessments (audits) to proactively monitor the privacy protections built into the Digital Identity program, which will assist the Digital Transformation Authority to mitigate privacy risks with the system. This funding also includes provision for the OAIC to develop two or three pieces of guidance about the privacy aspects of the Digital Identity system.

Will the growing workload result in greater backlogs?

The OAIC continues to implement efficiencies in the way work is completed. For example, the OAIC recently reviewed its workflow processes for the Dispute Resolution Branch to streamline the complaint handling process. The OAIC continues to look for and implement opportunities to further improve productivity to address the increasing volume of incoming work, within the resources available to us, and to prioritise as appropriate.

However, efficiencies cannot currently keep pace with the continuing rise in incoming FOI work.

KEY DATES

- 22 February 2018: NDB Scheme commenced, no additional funding received.
- 1 July 2018: 2018-19 Budget provides $12.91million over the forward estimates for CDR
- 30 June 2019: *Enhanced Welfare Payment Integrity – non-employment income data matching (commenced MYEFO 2015-16)* measure valued at $1.326million terminates.
- 1 July 2019: 2019-20 Budget provides $25.121million over three years to enhance funding for statutory obligations and social media.
- 1 July 2019: 2019-20 Budget provides $329,000 to the 2018-19 base and $2.256million over the forward estimates for the expansion of Medicare data matching.
- 24 June 2020: MOU funding with ADHA secured at $2.070million for one year.
- 1 July 2023: reduction in revenue due to terminating measure (statutory obligations and social media).
- 1 July 2021: 2021-22 Forward Estimates provides $0.261million for Expanding Digital Identity

FORWARD ESTIMATES

	2019-20	2020-21	2021-22	2022-23	2023-24
Appropriation	$20,941,000	$20,948,000	$20,711,000	$13,039,000	$13,089,000
MOUs	$2,257,000	$2,322,500	75,000	—	—
Total	$23,198,000	$23,270,500	$20,786,000	$13,039,000	$13,089,000
Difference from prior year		+$72,500	-$2,484,500	-$7,747,000	+$50,000

MOU detail

MOU	2019-20	2020-21	2021-22
ADHA	2,070,000	2,070,000	—
ACT Government	$177,500	$177,500	—
USI	—	—	—
DHA – NFBMC	—	$75,000	$75,000
Other revenue	$9,500	—	—
Total	$2,257,000	$2,322,500	$75,000

Statutory obligations and social media detail

	2019-20	2020-21	2021-22	2022-23
Appropriation	$7,734,000	$7,887,000	7,500,000	—
Capital	$2,000,000	—	—	—
Total	**$9,734,000**	**$7,887,000**	**$7,500,000**	**—**

Medicare data matching

	2019-20	2020-21	2021-22	2022-23
Appropriation	$571,000	$565,000	$560,000	$560,000
Capital	–	—	—	—
Total	**$571,000**	**$565,000**	**$560,000**	**$560,000**

CDR detail

	2018-19	2019-20	2020-21	2021-22	2022-23
Appropriation	$2,779,000	$3,178,000	$3,036,000	$3,058,000	Not identified
Capital	$860,000	—	—	—	–
Total	**$3,639,000**	**$3,178,000**	**$3,036,000**	**$3,058,00**	

Expanding Digital Identity

	2018-19	2019-20	2020-21	2021-22	2022-23
Appropriation	—	—	—	$261,000	—
Capital	—	—	—	—	—
Total	—	—	—	**$261,00**	—

2020-21 FUNDING

- 2020-21 total revenue is $23.270million, of this:
    - $20.948million is appropriation (including $7.887million for social media & $3.036 million CDR & $0.565million for Medicare data matching)
    - $2.322million is MOU based.

2019-20 OPERATIONAL PROFIT

Item	Amount	Note
Depreciation & amortisation	$2,234,000	Permitted loss amount
Principal Payment of Lease Liabilities	$1,612,000	Permitted loss amount
Unforeseen underspend	$501,000	This surplus is the result of the impact of COVID-19. Specifically, both the review of the Privacy Act 1988 and the development of the Online privacy code were delayed as a result of the pandemic. The OAIC's planned recruitment activity was delayed and international and domestic travel halted also as a result of the pandemic. These initiatives are expected to recommence in the 2020/21 financial year
Total Deficit per statutory financial accounts	**$121,000**	

2020-21 ASL

- OAIC's permitted ASL cap is 124 including:
    - 23ASL for statutory obligations and social media
    - 15ASL for CDR
    - 3 ASL for Medicare data matching

As at 1 October 2020

- Year-to-date ASL at 1 October 2020 is 112
- Year-to-date FTE at 1 October 2020 is 116 (detailed below)
- Current recruitment agency staff at 1 October 2020 is 6

- Full-time-equivalent (FTE) at 1 October 2020 is 116. That FTE is allocated to:

	1 October 2020	**20 February 2020**	**2 October 2019**	**20 March 2019**
OAIC	116 FTE	94 FTE	99 FTE	86 FTE
Privacy (including NDB)	76 / 65%	64 / 69%	65 / 66%	59 / 68 %
NDB (included in privacy)	5 / 7%	3 / 5%	4 / 11%	7 / 8%
FOI	25 / 22%	18 / 19%	20 / 20%	20 / 24 %
Governance & support	15 / 13%	11 / 12%	14 / 14%	7 / 9%

- Refer to Attachment **A** for excerpts of previously quoted ASL/FTE figures

BACKGROUND

- Attachment A: Excerpts — previously quoted ASL/FTE figures
- Attachment B: Background on MBS / PBS
- Attachment C: provides overview of the OAIC's budget from 2014-15 onwards

DOCUMENT HISTORY

Updated by	**Reason**	**Approved by**	**Date**
Mario Torresan	October 2020 Estimates		

Attachment A: Background on MBS / PBS

What is the Guaranteeing Medicare – improving safety and quality through stronger compliance measure?

In May 2018, the Government announced an investment of $9.5 million over five years from 2017-18 to continue to improve Medicare compliance arrangements and debt recovery practices to ensure Medicare services are targeted at serving the health needs of Australian patients. This measure includes better targeting investigations into fraud, inappropriate practice and incorrect claiming and will use data analytics and behavioural driven approaches to compliance.

Did the OAIC receive additional resources for the regulatory oversight of a revised MBS/PBS scheme?

Yes. The OAIC received funding of $2.256 million over the forward estimates years from 2019-20.

What activities will you undertake with increase of funding for regulatory oversight of a revised MBS/PBS scheme?

The OAIC will be the complaint handling body for the regime, and will offer the mechanism through which consumers can seek a formal remedy to redress a breach of their privacy; and respond to general enquiries from the community. This includes investigating and taking enforcement action in relation to breaches of the scheme, including the conduct of Commissioner-Initiated Investigations

The funding will also enable the OAIC to undertake two privacy assessments (audits) per year to proactively monitor whether information subject to the new arrangements is being maintained and handled in accordance with the relevant legislative obligations, and recommend how areas of non-compliance can be addressed and privacy risks reduced.

Attachment B: Excerpts — previously quoted ASL/FTE figures

Legal and Constitutional Affairs Legislation Committee
03/03/2020
Estimates
ATTORNEY-GENERAL'S PORTFOLIO
Office of the Australian Information Commissioner

Office of the Australian Information Commissioner

[21:47]

Senator PATRICK: Thank you for coming along tonight, Ms Falk. I just want to know whether you could provide the committee with some information in relation to an investigation you conducted into the Prime Minister's office in respect of FOI performance.

Ms Falk **:** Yes, Senator.

Senator PATRICK: There was an article in the *Guardian* that talked about you having conducted a review or an examination into the Prime Minister's office. I don't want to rely on the media. I just would like a summary of your findings in relation to that.

Ms Falk **:** Under the FOI Act I have a statutory requirement to investigate complaints that are made to my office regarding the processing of FOI matters. This complaint was lodged with my office in 2018. The complaint progressed. It contained allegations of delay in relation to that particular department in relation to the complainant. There's a process that's undertaken in terms of receiving submissions and analysing the information. Then it falls to me to make investigation findings. In this matter, I concluded that there had been a delay without authorisation under the FOI Act. I can then make remedial recommendations to the agency.

Senator PATRICK: This was only related to one FOI?

Ms Falk **:** It was. In relation to the matter, I made recommendations. In relation to that particular department, they had been experiencing delays overall with their processing of FOI matters. In the 2018-19 financial year 72.6 per cent of all requests determined by the department were in time, which was a considerable improvement on the year before, at 35.5 per cent. I made four recommendations to the department and those recommendations were accepted by the department. I also asked for a report to be provided to me in relation to the implementation of the recommendations. I received that just last week and it is under consideration by my office.

Senator Payne: Just to be clear, Ms Falk: we're talking about the Department of the Prime Minister and Cabinet, aren't we?

Ms Falk **:** Yes, we are.

Senator Payne: So it's not the Prime Minister's Office, but the department.

Senator PATRICK: Okay, I apologise for my clumsiness.

Senator Payne: No, just clarifying.

Senator PATRICK: Thank you, Minister. I will say that I did ask questions about this and they indicated that they are now at 100 per cent compliance. So it looks like you may have done some good work on that, Commissioner.

Ms Falk **:** It's a very pleasing result.

Senator PATRICK: Can you provide an update on your investigation into Home Affairs?

Ms Falk **:** That matter remains ongoing. We have been working with the Department of Home Affairs, who have been very cooperative with the investigation. We have requested information from them and considered it, and we will be requesting further information. The matter is one that is under active consideration by the office.

Senator PATRICK: I was involved in a discussion with a constituent last week who said they had not received a response in over a year in relation to an FOI request. I'm not raising a complaint with you; I'm just wondering whether the scope of your current inquiry is likely to capture that sort of circumstance.

Ms Falk **:** The current investigation is in relation to the Department of Home Affairs' processing of non-personal information requests—so, other information—which is a much smaller cohort of the overall 17,000-plus requests that Home Affairs receives each year. But it is the area where timeliness seemed to be most acute, so whether the matter would be raised within its scope would depend on the particular nature of your constituent's issues. The scope of the investigation will be looking at issues of the timeliness for non-personal information and the processes in place to deal with those requests. At the conclusion of the investigation it is open to me to make recommendations to the agency head.

Senator PATRICK: You might find a couple of my FOI requests in there that weren't answered within the time frame!

Senator Payne: Surely not!

Senator PATRICK: In relation to my constituent, what's your recommended course of action in relation to an FOI that hasn't been responded to in over a year? Is it best to simply contact your office to make a complaint, make the claim of a deemed refusal and ask you to review it, or both?

Ms Falk **:** There are the two options available. My view is that where, at the heart of the matter for the individual, they are requesting access to documents, the matter is ordinarily better dealt with as an Information Commissioner review of a deemed refusal of those documents. In many of those cases the issues of process can be considered within the ambit of the Information Commissioner review. There are some cases where that is not the case, where really the heart of the matter is a complaint around service or a complaint around delay, in which case a complaint application is more appropriate. So it is a little circumstantial, but my guidelines issued do say that where IC review is available that would be the preferred course of action of my office.

Senator PATRICK: Thank you. I'll pass that on. As of 25 October 2019, according to an answer you provided, there were 361 open Information Commissioner reviews that had been on hand for more than 12 months. What's the figure as it stands today—how many reviews have been with you for more than a year?

Ms Falk **:** I might, if I may, make a couple of contextual remarks around that. You'd be aware that, since 2015, the numbers of Information Commissioner review requests to my office have increased by 82 percent. During that same period of time, due to the best efforts of my staff and process improvements, we've managed to increase our closure rates by 45 percent. But, unfortunately, the gap between the work coming through the door and that which we can process is there. That does mean that the time to resolve matters is more extended than would be certainly ideal. We currently have 991 IC, Information Commissioner, reviews on hand. Of those, 443 are more than 12 months old and 59 are more than two years old.

Senator PATRICK: So the situation isn't getting better. I know you'd had some consultants come in and you were looking for efficiencies.

Ms Falk **:** Senator, we have managed to—

Senator PATRICK: Where do you go from here? We know you're doing the work of three commissioners. There are three commissioners named in the act—an FOI Commissioner, a Privacy Commissioner and an Information Commissioner and—so please don't take this as a criticism of the office. But, at an inquiry in relation to an FOI bill that I had before the Senate, the department conceded there was a close-to-crisis situation. How do we resolve this?

Ms Falk **:** Senator, you've mentioned that we have been successful in terms of process refinements and we continue to do so. We have finalised last financial year more IC reviews than in the history of the office, so we continue to increase our productivity. We also are working within the resources that we have to look at issues that might be able to be of broader application throughout agencies that would then impact the system more broadly. So, to give an example: I encourage agencies to look at opportunities to give access to information administratively but also to look at opportunities for proactively publishing information that's often requested by citizens. So, in that way, people don't have to use the FOI Act to find the information. We're looking at those aspects to try and ensure the overall

efficiency of the system for everyone. But you have raised the challenge that arises with a considerable increase in the workload of the office and the issues that that raises.

Senator PATRICK: Have you looked at the number of reviews that you've done that lead to—in the case management phase, you might reach a negotiated settlement or indeed when you finally make a decision as to how many of those involved decisions where the department should have released the information. That is: if there's a culture of restraint in terms of providing information under FOI, a feeling of a tendency to release less than more, if across government that attitude was adjusted, would mean there would be fewer reviews. Have you looked to see if the number of reviews results from an increase in secrecy by departments?

Ms Falk **:** There are a couple of remarks I can make in relation to that. The first is to reiterate the pro-disclosure tenets of the FOI Act and my messaging to government agencies to take a proactive approach where that's appropriate. But, if I look at the agency's statistics that have to be provided to my office each year, that is really where I can see at least one indicator of the health of the system. If we look at last financial year, the percentage of matters where documents were provided, either in full or in part, is broadly consistent across the years from 2011-12. Thirteen per cent were refused last financial year, and that compares to 12 per cent back when the office was established. Similarly,in terms of the numbers where access was provided in full last financial year, it was at 52 per cent, and that compared to 59 per cent back in 2011-12, and for those provided in part last year it was 35 per cent, compared to 29 per cent.

You also raised the issue of my IC reviews and the extent to which—perhaps one way of looking at it is the number of matters where I'm affirming agencies' decisions or varying those decisions. I'd say that they're fairly even. A number of the decisions, however, that come to me have already been the subject of negotiation with my case officers and departments, and that may have enabled the agency to make a varied decision and release further documents. So it might be that the scope of what I'm looking at is much narrower than that of the original decision-makers.

Senator PATRICK: I'm just thinking of that *Utopia* clip on FOI. I'm sure you've seen it a few times?

Ms Falk **:** What would make you think that I watch *Utopia*, Senator?

Senator PATRICK: It's mandatory if you want to understand government. But anyway—

Senator PAYNE: It's a documentary, isn't it?

Senator PATRICK: That's correct. I refer to question on notice AE19-011 from 19 February 2019, so about a year ago. You provided a range of statistics in relation to disposal rates and so forth. One of the tables in there—I don't know if you have that question available, because I don't want to—

Ms Falk **:** Would you provide the number again please.

Senator PATRICK: It is AE19-011 of additional estimates 2018-19. It was in relation to a question I asked on 19 February 2019.

Ms Falk **:** I don't have it in front of me, sorry.

Senator PATRICK: Okay. I'll read this out. There was a table that you provided that said:

This table provides the forecast future pending-to-disposal rate (PDR) at the end of each year. The PDR can be used as a proxy for gauging future timeliness of matters to be disposed. For example, a PDR of 0.5 equates to an approximate average finalisation time of six months.

You indicated for Information Commissioner reviews that for 2019-20 you expected 0.5 and for 2020-21 you expected 0.5, getting to 0.4 in 2021-22 and 0.4 in 2022-23. Clearly, you're not hitting that, unless I misunderstand what you were referring to.

Ms Falk **:** That's a particular formula and I'd need to look at the data in relation to that particular construct. The information that I have in front of me this evening is around the length of time for allocation, average completion time of those that are finalised—around eight months—and that's remained fairly consistent. We have had an 11 per cent decrease in IC reviews in the first six months of this financial year. I would need to look at all of that.

Senator PATRICK: Is that decisions made?

Ms Falk **:** No, applications to my office.

Senator PATRICK: Applications?

Ms Falk **:** Yes.

Senator PATRICK: So you had made a prediction for 2019-20 of 1,322 applications?

Ms Falk **:** Yes.

Senator PATRICK: You've got fewer?

Ms Falk **:** Currently on hand we've got around 991.

Senator PATRICK: You said that's what you've got on hand. That might be different to those that apply—

Ms Falk **:** Applications received were 461 for six months.

Senator PATRICK: Okay. So that's down quite a lot. That's a good thing.

Ms Falk **:** It is 11 per cent.

Senator PATRICK: I will leave it at that. I might put the rest of my questions on notice.

Senator CHANDLER: What was the amount of the additional funding committed by the government for the OAIC in the last budget?

Ms Falk **:** It was $25.1 million over three years.

Senator CHANDLER: What was that specifically for?

Ms Falk **:** It was specifically to provide a timely privacy complaint handling service, and also to regulate and take action in relation to the privacy of Australians online.

Senator CHANDLER: Before I ask what good use you've been putting that $25.1 million over three years to, what were the policy reasonings behind that? Obviously we know that privacy in this world, where we all have mobile phones and computers, and the internet is readily available, is becoming a greater concern. Could you perhaps explain what the drivers were behind that increase?

Ms Falk **:** Yes. The work in terms of privacy to my office has continued to increase since 2015. There's been a significant increase in the number of privacy complaints made to my office. We've also established the Notifiable Data Breaches scheme. The government made legislation on that, which commenced on 22 February 2018. As you've pointed out, aside from a heightened community awareness of privacy issues, personal information is really what is driving the digital economy. It's also a key input into service delivery by government. So both of those factors together, coupled with new and perhaps unexpected uses of personal information, particularly online, I think, is some of the basis for, certainly from my perspective, the need for my office to have additional funding and also, from a regulatory perspective, to ensure that into the future we're able to have the capability within the organisation to take the regulatory action that's required, from education and voluntary compliance through to exercising some of the other powers that I have around taking action to the Federal Court for civil penalties.

Senator CHANDLER: I foreshadowed this in my last question, but what further initiatives have you been actioning that this $25.1 million is being spent on to target the issues you raised?

Ms Falk **:** The first is that we've been able to increase our staffing capability. From 93 staff, we now have an ASL cap of 124. We had a considerable backlog of privacy complaints. We had 300 matters awaiting early resolution. We no longer have a backlog. We've also had considerable backlogs for conciliation and investigation, and all of those matters are now being actively worked upon. We've also been able to establish a determinations team that can then prepare decisions for my ultimate decision-making around individual privacy complaints. At the same time, we've been increasing our capability for my office to take action on my own initiative. We now have a considerable body of intelligence from the Notifiable Data Breaches scheme, having operated now for two years, and there is an opportunity to look at systemic issues in terms of data security and where enforcement action might be necessary,

both in order to provide a remedy but also as a deterrent to ensure that entities are taking privacy of personal information and security seriously.

Senator CHANDLER: What are some of the concerns you've had out of that data analysis across your organisation?

Ms Falk **:** I released a report a couple of weeks ago which was a six-monthly analysis of July to December last year. That showed that predominantly the causes of data breaches are malicious and criminal attack. Of those, the main reason personal information is being compromised is individuals are being lured through phishing emails to provide their user name and password and that's enabling malicious actors to enter systems. One of the big issues that we have seen in that six-monthly report is the use of those credentials to access email systems and, within that, I've seen increased examples of entities storing sensitive personal information within email systems. So that sensitive information really should be stored in secure areas of organisations, not within email systems where it can be more readily accessed if it be breached.

Senator CHANDLER: Wonderful. You mentioned 'conciliation' in your response just now. I'm really interested to know—what does that look like in the privacy space and within the remit of your work?

Ms Falk **:** I might turn to my colleague, Ms Hampton, who's been doing the change management work in relation to the backlog strategy and the conciliation program.

Ms Hampton **:** In the first instance, when there is a complaint made to the office, we have an early resolution process whereby the parties are brought together and information is exchanged, and we establish whether or not the office has jurisdiction and there is a prima facie breach of the privacy law. Many cases resolve at that early stage, which generally takes place in the first month. But following that, there is a requirement under the Privacy Act that unless a matter is unable to be conciliated that a conciliation should be attempted as a method of resolving the matter prior to proceeding to investigation and determination, so it's an important and a statutory step in the process of resolving privacy complaints to the office.

Senator CHANDLER: Great. I don't think there's anything more I have on funding. Thank you very much.

Senator CHISHOLM: You might recall that at last estimates I asked some questions about the culture of secrecy within the Department of Home Affairs and its failure to comply with the Freedom of Information Act. I noticed that, following Senate estimates, you announced an investigation into Home Affairs compliance for the Freedom of Information Act. Is that correct?

Ms Falk **:** Yes, I did. That matter had been under consideration for quite some time. We had been analysing the statistics that agencies submit to my office at the end of the financial year and also monitoring the Information Commissioner review applications that were being received by my office relating to the Department of Home Affairs. So there were a number of factors that together led me to the conclusion that it would be a worthwhile use of public resources to investigate the matter and then to work with the Department of Home Affairs to improve their compliance.

Senator CHISHOLM: I wasn't seeking to take credit, for the record. How is the investigation going?

Ms Falk **:** It's continuing. The department's cooperating with the investigation. We've requested information that's been provided. There will be further requests for information being sought imminently, so the matter is under active consideration.

Senator CHISHOLM: How would you describe the Department of Home Affairs co-operation with your investigation? Have they responded promptly to your requests?

Ms Falk **:** Yes, they have.

Senator CHISHOLM: When would you be expect it to be completed?

Ms Falk **:** That's always the question, isn't it? It will in part depend on what we receive, in terms of the information requests that we make. And then one always has to make an analysis of whether that is sufficient or whether further information is required. I would think that it would be in the coming months and certainly by the end of this financial year.

CHAIR: We appreciate your evidence today. Thank you very much for your patience in the course of the day. We will see you next time estimates is on.

Ms Falk **:** Thank you, Chair.

CHAIR: The next agency we have on our list is the High Court of Australia.

Tuesday 22 October 2019 (Estimates):

Senator HENDERSON: Commissioner, I'd like to ask you about the funding for the Office of the Australian Information Commissioner; in particular, the amount of additional funding committed by the government for the office in the last budget.

Ms Falk: In terms of the operating budget of the Office of the Australian Information Commissioner, the total revenue for this financial year is $23.234 million. That includes appropriation of $20.941 million and a sum which comes to the office through memorandums of understanding of around $2.3 million. In terms of the second part of your question, around the additional funding provided to the office, the 2019-20 budget allocated $25.121 million over three years to undertake functions around the handling of personal information and taking enforcement action. The purpose of the funding is to ensure timely handling of privacy complaints, also particularly focused on regulating the online environment. It is envisaged that my office would create a regulatory code that would apply to online providers such as social media companies, and it would set out particular protections in terms of vulnerable Australians, including children…

…other text deleted…

…So one of the big shifts in my office at present is shifting from an organisation that has predominantly been, in terms of privacy, an alternative dispute resolution body focused on conciliation, with administrative decisions being made in only some cases. It's clear that the community expectation of regulators—also the government has announced its intention to increase penalties under the Privacy Act and the enforcement mechanisms available to me—that a strong enforcement approach is required. That means increasing our capability. We are increasing the ASL, up to 124 staff, this financial year. We are currently at around 90 and we will be looking particularly at increasing our capability to act in that enforcement role.

Senator KIM CARR: Did I hear you correctly in your opening statement? Did you actually say that you're under-funded?

Ms Falk: I did raise the issue of resourcing in terms of FOI. It's a matter that's been discussed before this committee on a number of occasions, where I've indicated that really where the stresses in the system lie, from the OAIC's perspective, are with the need for more staffing. I've set out the fact that we've had an 80 per cent increase in Information Commissioner reviews and I have worked very purposefully since being in the role on looking at how we can increase our efficiency. Over that same period of time—the four-year period—we have increased our efficiency by 45 per cent. But I've formed the view, having conducted a number of reviews of the way in which we're carrying out our work, that the only way in which the gap is to be bridged is for additional staffing resources to be provided.

Senator KIM CARR: I see. I was just trying to reconcile the line of questioning from Senator Henderson with your statement, that's all. When was the first time you requested additional funding?

Ms Falk: I'd need to take that on notice.

Senator KIM CARR: Are you sure you need to? Most officers in your position would be able to tell very quickly when they first sought additional resources, given the growth in the workload.

CHAIR: The question's asked and answered. She's taken it on notice.

Senator KIM CARR: I'm just surprised that you need to take that on notice. Because what—

Ms Falk: It's been a matter of discussion with this committee and also, of course, with government during my term. I'm just unable to recall, with accuracy, the first occasion on which that occurred.

Senator KIM CARR: I see what you mean. I do apologise. In my experience, officers in your position are able to identify at least the year in which they asked for additional resources.

Ms Falk: I have asked for additional resources since being appointed to the position in August last year but, in terms of the first occasion subsequent to that date, I would need to check.

Senator KIM CARR: I see. That's where the confusion lies. So, since August last year, you've been seeking additional support?

Ms Falk: Sometime after that date, Senator.

Senator KIM CARR: And what was the government's response?

Ms Falk: The government has acknowledged my request and is working through it in terms of normal budget processes. (QoN)

Senator KIM CARR: I appreciate that agencies will ask for additional resources and it won't necessarily be the same amount as the ERC thinks you're entitled to, but what is, in your assessment, the requirement? How much do you need to do your job in terms of the report that you've given to us today about the additional demand on your agency?

Ms Falk: The amount of additional resources depends on the objective which is sought to be achieved. Of course, the more staffing resources that you have for processing Information Commissioner reviews and complaints, the quicker they can be processed.

Senator KIM CARR: So you don't have a figure?

Ms Falk: I think that there needs to be an increase in the staffing resources, and the quantum of that does depend on the time in which the backlog is sought to be addressed and also the ultimate goal in terms of how quickly Information Commissioner reviews should be handled.

Senator KIM CARR: So how much did you ask for?

Ms Falk: Senator, you appreciate that the information I've provided to government is through budget processes. I can give you an indication that, at present, my funding envelope allows for around 19 case officers to work on FOI reviews—there are additional staff who work on the FOI function more broadly—but just looking at FOI reviews, there'd need to be at least a half increase in the number of those staff.

Senator KIM CARR: What you mean by 'a half'?

Ms Falk: A half again.

Senator KIM CARR: So—

Ms Falk: Another nine staff.

Senator KIM CARR: What will that cost in terms of your normal profile?

Ms Falk: I'd need to see if we've got any figures to hand in relation to that, but it would be the cost of those staff.

Senator KIM CARR: It depends on what they're paid, doesn't it? Those nine staff are not all SES staff, are they?

Ms Falk: No, they're case officers.

Senator KIM CARR: So you'd be able to indicate roughly what it would cost to fund nine staff.

Ms Falk: I've put forward to government the cost of that and also any capital costs that might be needed to accommodate those staff.

Senator KIM CARR: Can you take that on notice, please? (QoN)

Ms Falk: Thank you.

Our reference: D2019/012893

Committee Secretary
Senate Standing Committee on Legal and Constitutional Affairs
PO Box 6100
CANBERRA ACT 2600

Clarifications to Hansard

I write to you concerning evidence provided to the Senate Standing Committee on Legal and Constitutional Affairs during the Supplementary Budget Estimates hearing on 22 October 2019.

The Office of the Australian Information Commissioner has the following clarifications:

Evidence of Ms Angelene Falk, Australian Information Commissioner and Privacy Commissioner

Clarification 1

On page 81 of the transcript, in an exchange with Senator Carr, Ms Falk said: "… at present, my funding envelope allows for around 19 case officers to work on FOI reviews".

The Office of the Australian Information Commissioner wishes to clarify that not all of the time of the 19 officers in the FOI section is spent on IC reviews.

That section also performs other FOI regulatory functions including processing FOI extensions of time applications and vexatious applicant declarations, investigating FOI complaints, updating the FOI Guidelines, undertaking FOI monitoring work including in relation to the Information Publication Scheme and Disclosure Logs and analysing and reporting FOI statistics provided by Australian Government agencies.

Response to QoN:

The response to the honourable senator's question is as follows:

The OAIC provided a submission to government in relation to additional resourcing, including for its FOI functions, in November 2018. An updated submission in relation to the OAIC's FOI function was provided to government in September 2019.

Response to QoN:

The response to the honourable senator's question is as follows:

The Office of the Australian Information Commissioner has estimated that the annual cost to fund nine (9) additional staff to undertake FOI regulatory work, including processing IC review applications, would be approximately A$1.65 million with an additional capital amount of approximately A$0.3 million for accommodation in the first year.

Tuesday 9 April 2019 (Estimates): reference to ASL

Senator PATRICK: Good morning, Ms Falk. I have a few lines of questioning. Firstly, in relation to the budget, it looks like you have a relatively significant increase in funding. Could you talk me through that funding and how you intend to use it?

Ms Falk: Since the last occasion that I appeared before the committee the government has announced a proposed provisions to strengthen privacy protections under the Privacy Act, including increased penalties and a new system of infringement notices. Importantly, my office will receive $25 million over three years to deliver new work, as well as to enhance the office's ability to prevent, detect, deter and remedy interferences with privacy. It is also intended that there will be an enforceable code to introduce additional safeguards across social media and online platforms that trade in personal information. The code will require greater transparency about data-sharing and requirements for the consent, collection, use and disclosure of personal information. This will incorporate stronger protections for children and other vulnerable Australians within the online environment. Accordingly, the OAIC will be focused on working collaboratively and constructively with all parties to enhance privacy protections both online and offline and to give Australians greater control over their personal information, ensuring that it is handled in a way that is transparent, secure and accountable.

Senator PATRICK: Does that new function have new employees attached to it?

Ms Falk: It does. At present we have an ASL cap of 93 staff, and that will be increased to 124. That takes account of this new measure. It also includes some additional staff for the consumer data right, a measure which was introduced in the last budget.

Senator PATRICK: Do I also detect an increase in capital expenditure?

Ms Falk: There is an increase of $2 million for capital. At present the OAIC requires additional accommodation, particularly with this new investment and increased staffing.

Senator PATRICK: You operate out of Sydney?

Ms Falk: That's right.

Senator PATRICK: Is that a lease of a building or something?

Ms Falk: It will be. We are making inquiries in relation to that at this time.

Senator PATRICK: We didn't really get much in the way of increased funding for FOI, I presume, based on that previous statement?

Ms Falk: There was no specific funding for FOI.

Tuesday 19 February 2019 (Estimates): reference to NDB

Senator PRATT: Journalists have been refused access to documents and are therefore raising concerns about the delays and the time it takes to have a government refusal of a decision reviewed by the Office of the Australian Information Commissioner. A key concern given to us is that, by the time a review is completed, the subject matter of the news story may no longer be current. This means that the government of the day may refuse an application entirely on spurious grounds, knowing that, even if the decision is ultimately overturned, the delay caused will ensure the information does not reach the Australian public in a timely and meaningful way. Would additional resources assist you in dealing with applications for the review of FOI decisions in a more timely manner?

Ms Falk: It's my responsibility to prioritise the appropriation that has been given to the office. I've talked through some of the strategies that we've put in place, including early resolution. We've tripled the number of matters for IC reviews that have been varied by agreement. There are early resolution processes that result in changed decisions, that result in further documents being provided to applicants. So we are seeing results. The figures that I've given you are a number of matters which are more complex in nature and have further exemption applications that may be applied to them.

…

Senator PATRICK: We'll go back once again to the burden of Senator Pratt's question. I'll just read the testimony of Mr Walter from the Attorney-General's Department. At a recent hearing he conceded, 'There are undoubtedly stresses in the system.' You're conceding that there are stresses in the system inherently by the fact that you have all these delays running through the system. I say this in the context that ASIC used to say: 'No, we've got enough resources. No, we've got enough resources.' When the whole system breaks the reality pops out. I cannot understand how you could be sitting in your position as a statutory officer with obligations, knowing that there are stresses and knowing that you're falling behind—notwithstanding that you are working as efficiently as you possibly can with the resources you have—and not be able to form the view that you require additional resources.

Ms Falk: I've not said today that I don't require additional resources—in fact, the contrary. I was asked a question earlier around the three-commissioner model and my answer went to the fact that I thought that that was working well at this time—if that were to change, I would advise government—but what is required is additional resources at the staffing level. I understand that that may not have been clear at the time. But I have been on record a number of times in terms of the increased workload and the fact that the ability of the office to keep up with that workload is being challenged. However, I don't think it's acceptable as a statutory officeholder to simply say that the office requires more resources with nothing else added to that. I think that would be simplistic.

It's incumbent on me to look at prioritisation across the office but also to understand the causes of the increased work, to work in terms of the proactive educative strategies that I've outlined and to ensure that we are taking a holistic approach to looking at our processes and that we are doing the best that we can. We can see over the last few years that we have continued to increase our throughput, and that's through trialling different pilots and different methodologies and looking very critically at our processes. I will continue to do that. There would be no regulator in the country, I'm sure, who wouldn't say that, inevitably, time frames couldn't be improved with additional resources, and I'm no exception to that.

Monday 22 October 2018 (Estimates): reference to NDB

Senator MOLAN: You spoke about finalising most data breaches—99 per cent within 60 days—but it may have deteriorated. Which of those figures deteriorated? Are you dropping the percentage? Or are you doing things faster? I was just a bit unsure.

Ms Falk: I've now got a note in front of me. In the first period of reporting, from when the scheme started on 22 February this year to 30 June, we resolved those data breach notifications in 60 days 99 per cent of the time.

Senator MOLAN: Good.

Ms Falk: We're now resolving those matters within 60 days 87 per cent of the time.

Senator MOLAN: Okay. That's not bad. And that's of the 305 that you've counted between the periods you mentioned?

Ms Falk: That's correct.

Senator MOLAN: How many staff are allocated to that function?

Ms Falk: There are a little over nine staff that are allocated at the moment, but they carry out a variety of roles.

Senator MOLAN: Out of how many total in the organisation?

Ms Falk: At present the total number in the organisation is 88 full-time equivalent.

Monday 22 October (Estimates): reference to FOI and other areas

Senator PRATT: Thank you. If you could take on notice the statistics for each quarter over the last couple of years, that would be great. Clearly the workload is increasing. How many staff do you have handling FOI matters?

Ms Falk: In relation to FOI at present—and it's always a point-in-time snapshot—we have around 22 full-time-equivalent staff.

Senator PRATT: Have you increased the number of staff handling FOI matters from the point last year where you had 168 to the point now where you have 281 matters?

Ms Falk: Yes, we have. There was a return of some funding from the AAT and, as a result of the return of that funding, we've increased the FOI staff. In August of this year, we implemented a new structure in our FOI area to give greater capacity.

Senator PRATT: You've currently got 22 staff.

Ms Falk: Yes.

Senator PRATT: What was it at the time when you had 168 matters?

Ms Falk: I would have to take that on notice. (QoN)

Senator PRATT: Okay, thank you. How does that compare to the number of staff you have handling other matters, and what is the time taken on average? Has the time to resolve FOI matters increased as the workload has increased?

Ms Falk: In terms of other matters, we have around seven staff that work across the office on our governance and support, and then we have around 61 people who work on privacy matters. We received some additional funding in this budget for the proposed consumer data right, which we have responsibility for implementing with the ACCC, and that provided an extra 10 FTE. I also mentioned earlier that there were some specific MOUs in relation to privacy.

Senator PRATT: Thank you.

Response to QoN:

The response to the honourable senator's question is as follows:

The 22 staff represent the contribution to delivering FOI functions from across the Office of the Australian Information Commissioner.

Following the reallocation of FOI funding from the Administrative Appeals Tribunal the Office of the Australian Information Commissioner assigned an additional three staff to handle FOI matters.

Friday 16 November 2018 (FOI hearing): reference to FOI and general resources

Senator PRATT: So, in that sense, you are identifying these problems? Are you trying to paper over the nature of that problem because it is a political decision that there is only one commissioner at this point in time?

CHAIR: That's not a very fair question to the commissioner.

Ms Falk: I'm happy to answer it, because the answer is no. I'm giving my considered view, having worked both in the office for over 10 years and then as the appointed commissioner, as to where I see the challenges in the process and where I think we can best address those issues. Should that situation change, then that's something, of course, that I would continue to monitor. But, at present, the one-commissioner model is not the subject or the cause of some of the issues that I think have been brought to bear by evidence today; it's an overall resourcing issue. Having said that, I want to acknowledge the incredible work of my staff in terms of dealing with an increased workload, working to look for more efficiencies and always working in the public interest. I'd like to put that on record.

Senator PRATT: If you, as commissioner, did have more resources and, therefore, there were a speedier triage, could that not accelerate the number of cases that you're ultimately responsible for making a decision on?

Ms Falk: Alternatively, it could resolve more that no longer require a decision, because that would mean that we're engaging with higher numbers of parties more quickly when there perhaps is more of a willingness to reach an agreement in relation to the matter.

Thursday 24 May 2018 (Estimates): Commissioner Falk – opening statement

Turning briefly to some of the other priorities for the OAIC, we're focused on implementing the new notifiable data breaches scheme, which is in its early stages. We're also preparing the OAIC and government agencies for the commencement of the Australian Government Agencies Privacy Code on 1 July, including providing detailed guidance and resources. The committee may also be aware that the OAIC has received additional funding of $12.9 million over the forward estimates to support strong privacy protections under the government's proposed consumer data right.

Thursday 24 May 2018 (Estimates): financials and staffing

Senator PRATT: That makes sense. So it's not therefore a lack of—I was going to say that therefore all senior roles in the commission are not permanent, but there's some permanency there because Ms Falk has been the deputy commissioner. Ms Falk, I'd like to ask you some questions about funding. You were allocated $16.1 million for the next financial year—no, that doesn't sound right. Can you tell us what your allocation is for the most recent budget?

Ms Falk: Under the current budget for 2017-18, the appropriation is $10.74 million. There's an additional amount that the OAIC receives from government agencies to MOU funding of $3.021 million. Then, in

2018-19, we will receive $13.496 million. That includes an additional $2.779 million, which I mentioned in my opening statement, for the proposed consumer data right.

Senator PRATT: As far as I can see, there's a cut over the period of the forward estimates in what you were allocated for the next financial year versus what falls over the forward estimates.

Ms Falk: At 30 June 2019, there will be a measure that terminates. That's the enhanced welfare payment integrity non-employment income data-matching measure. That will terminate, as I said, on 30 June 2019.

Senator PRATT: What was the allocation attached to that?

Ms Falk: It is approximately $1.3 million.

Senator PRATT: What's the total decline over the forward estimates relative to your income for this next financial year?

Ms Falk: There are no other significant decreases in terms of terminating measures. The only other decreases relate to efficiency and other measures that occur throughout the portfolio, and they're allocated to the OAIC accordingly.

Senator PRATT: Okay. I'm trying to see if I've got an attachment that shows this. Can I ask about whether you've had to cut any staff to absorb funding cuts?

Ms Falk: We have not had to cut staff in this financial year.

Senator PRATT: Looking forward, do you expect that your staffing allocation will remain the same?

Ms Falk: Our staffing allocation will increase next financial year. We'll move from having an ASL of 75 to having an increased ASL of 92. That takes account of the new budget measure on the consumer data right. We are in a fortunate position of actually being able to go out to recruit, and we're, at the moment, making arrangements in order to move that forward.

Senator PRATT: Okay. You look like you're having an ASL increase, despite what looks like a decline over the forward estimates. How are you funding that?

Ms Falk: As I mentioned, there is the additional appropriation for the consumer data right. What the forward estimates don't specify is the amount that we're likely to get under the memorandum of understanding. The only memorandum of understanding remuneration that's mentioned there relates to two MOUs that we know are on foot now and will continue next financial year, and that's $2.07 million for the digital health system and an MOU we have to regulate the unique student identifier, for $100,000. We have a number of other MOUs that are terminating at 30 June, and we're in negotiations to renew those. As I said, they currently amount to over $3 million for this financial year, and we would expect funding in relation to a commensurate amount to continue over the forward estimates.

Senator PRATT: If you could you tell us on notice which programs that aren't covered in your base allocation you've got over the forward estimates, which ones are finishing and which ones you're working on having renewed, that would be—

Ms Falk: Thank you. We will.

Senator PRATT: And the value of the budget attributed to each of those. (QoN)

Ms Falk: Thank you, Senator.

Thursday 24 May 2018 (Estimates): Staffing/NDB

Senator STEELE-JOHN: Just finally—and I'm all done—how many staff have you allocated to handle these notifications and have you received additional funding to support the NDB Scheme?

Ms Falk: We've not received additional funding. In relation to staff handling the matters, we have around five staff at present who are handling notifiable data breaches and also our proactive commissioner-initiated investigations. They would also have a privacy complaint caseload as well.

Thursday 24 May 2018 (Estimates): Staffing/FOI

Senator PATRICK: Ms Falk, with respect to the question that Senator Steele-John was asking, how many overall staff do you have at the Office of the Australian Information Commissioner?

Ms Falk: We have 75 FTE at present.

Senator PATRICK: Split between privacy and FOI?

Ms Falk: Yes, that's right.

Senator PATRICK: Is there a mud map in your annual report, as to the positions and what functions people perform?

Ms Falk: There is information in the annual report in terms of the way in which the organisation is structured into two branches. We have our dispute resolution branch that deals with both privacy and dispute resolution, and also Information Commissioner reviews and complaints. Then we have a regulation strategy branch, which is around our guidance, advice, monitoring and also conducting assessments.

Senator PATRICK: When you said that five people have been transferred or are now looking at the NDB complaints, what were those people previously doing?

Ms Falk: They've not been transferred. They're people who were dealing with the voluntary data breaches in the scheme that we ran before the mandatory scheme. They also deal with commissioner initiated investigations and inquiries, and they would also have a privacy caseload.

Senator PATRICK: How does that gel in terms of workload, now that they've got a new function?

Ms Falk: There has been an increase in that workload. We have had to put in place different systems and processes, and use our IT environment in new ways to try and create some efficiencies there. There's definitely a workload increase across the office. I'm very grateful to the staff for the very flexible approach that they're taking to manage the work. There's a commitment to look at what our ongoing needs are going to be into the future, and I've certainly been in discussion with the department in relation to that.

Response to QoN:

The table below contains Memorandum of Understandings that provide funding in addition to departmental appropriation:

Description	**Type of funding**	**End date**	**Amount**	**Status as at 26 June 2018**
Australian Bureau of Statistics: Provision of Privacy Advice	Memorandum of Understanding	30 March 2018	$175,000 for 2017-18	Finalised MOU
Department of Home Affairs: Visa Reform Program	Memorandum of Understanding	30 March 2018	$75,000 for 2017-18	Finalised MOU
ACT Government: Provision of Privacy Services	Memorandum of Understanding	30 June 2018	$177,146 for 2017-18	Renewal anticipated
Department of Immigration and Border Protection: Passenger Name Record data	Memorandum of Understanding	30 June 2018	$65,000 for 2017-18	Renewal anticipated
Department of Human Services: Priority Privacy Advice	Memorandum of Understanding	30 June 2018	$220,000 for 2017-18	Renewal anticipated
Australian Digital Health Agency: My Health Records Act 2010 and Healthcare Identifiers Act 2012	Memorandum of Understanding	30 June 2019	$2,070,000 for 2018-19	Current MOU
Department of Education and Training: Student Identifiers Act 2014	Memorandum of Understanding	30 June 2019	$100,000 for 2018-19	Current MOU
Attorney-General's Department: National Facial Biometric Matching Capability	Memorandum of Understanding	30 June 2019	$75,000 for 2018-19	Current MOU

Attachment C: Post 2014-15 Budget overview

Year	Total	Commentary	
2014-15			**ASL: 63.77**
Appropriation	$9,963,000	Total appropriation was $9,963,000. Prior to efficiency dividends amounts include: • initial appropriation $7,191,000 • $2,812,000 in the Supplementary Budget Estimates	
MOU	$2,824,000	Includes Dept. Health amount of $1,976,000	
2015-16			**ASL: 63.90**
Appropriation	$9,328,000	Total appropriation was $9,328,000. Prior to efficiency dividends amounts include: • Initial appropriation of $5,698,000 for the privacy function and $1,709,000 for continued FOI function • New measure: National Security $1,130,000 • MYEFO measure: Welfare Data Matching: $818,000	
MOUs	$2,440,000	Includes Dept. Health amount of $1,865,500	
2016-17			**ASL: 71.00**
Appropriation	$10,622,000	Total appropriation was $10,622,000 million	
MOU	$2,824,000	Includes ADHA amount of $2,076,700	
2017-18			**ASL: 75.00**
Appropriation	$10,711,000	Total appropriation was $10,711,000. Prior to efficiency dividends amounts include: • $379,000 return of FOI from AAT in MYEFO	
MOU	$2,590,000	Includes ADHA amount of $1,688,400	
2018-19	$16,162,000		**YTD ASL: 86.00**
Appropriation	$13,825,000	Total appropriation is $13,825,000. Prior to efficiency dividends amounts includes: • New measure: Consumer Data Right $2,779,000 • New measure: Medicare data matching $329,000	
MOU	$2,337,000	Includes ADHA value of $2,070,000	
Capital	$860,000	Once-off equity injection	
2019-20	$23,263,500		**ASL cap: 124**
Appropriation	$20,941,000	Total appropriation is $20,941,000. Prior to efficiency dividends amounts include: • New measure: statutory obligations and social media $7,734,000 • New Measure: Medicare data matching $571,000	
MOU	$2,322,500	ACT / ADHA / Home Affairs MOUs	
Capital	$2,000,000	Once-off equity injection	

Attachment D: COVID-19 & OAIC Funding Article – Innovation Australia D2020/010421

Data (https://www.innovationaus.com/category/data/)

Privacy safeguards useless without funding

Australia's privacy office "urgently" needs more funding to properly conduct its oversight role of the COVIDSafe contact tracing app, with Labor calling for three standalone commissioners to also be appointed.

Legislation passed last week handed significant oversight duties to the Office of the Australian Information Commissioner (OAIC) for the controversial contact tracing app, with accountability for all data usage by state and territory health bodies, the app itself and the Commonwealth's data store.

The OAIC is to conduct its own investigations, handle complaints by users, refer matters for criminal investigation and produce a report on the app every six months.

These new duties are a "top priority" for the OAIC, Information Commissioner Angelene Falk said, but the government will not be providing any additional funding or resources to the agency to undertake them.

Privacy oversight: The commissioner needs more resources to get the job done

This is despite ongoing concerns around the resourcing of the OAIC in the face of significant increases in privacy and Freedom of Information request complaints, and a series of new duties surrounding the mandatory data breach notification scheme, the Consumer Data Right and now the COVIDSafe app.

Attorney-General's department officials told a senate hearing earlier this month that the OAIC did not need any additional funding to undertake the new role, while the government has now said it is in discussions with the office over the funding issues.

Labor raised the OAIC's funding with Attorney-General Christian Porter in discussions on the COVIDSafe legislation, and is now pushing for additional resources and for three standalone commissioners to be appointed.

Despite the legislation providing for separate freedom of information, information and privacy commissioners, Ms Falk has occupied all three of these roles since 2018 under the Coalition.

"If the Morrison government is serious about building public confidence in this app, now, more than ever, the Attorney-General must appoint a standalone, dedicated Privacy Commissioner," shadow Attorney-General Mark Dreyfus told InnovationAus.

"Back in October last year the Information Commissioner told Senate Estimates that her office is already severely under-resourced. It's absurd for the government to assert that the Information Commissioner can now be given a range of additional oversight responsibilities while continuing to do three jobs, without additional funding."

Privacy-enforcing legislation like the COVIDSafe bill won't be effective unless there is a strong and well-funded privacy body, Digital Rights Watch board member David Paris said.

"A well-resourced OAIC is essential for maintaining public confidence in digital initiatives undertaken by the government. The urgency our current circumstances created has put the OAIC under enormous pressure," Mr Paris told InnovationAus.

"They not only have to play a vital oversight role, they are often put in a position where they need to advocate for the better interests of the public, many of whom may not be aware of the full consequences of what the government is doing, or their rights in such situations.

"Any statement from the government that takes our rights seriously without it materialising in proper resourcing for the OAIC suggests that such a claim is more about image than substance.

> *"Any shortfalls in the independence or resourcing of the OAIC puts trust in government at risk, and we've seen how critical that trust is in a crisis like the one we're in now."*

A number of Labor MPs and Senators spoke in Parliament last week on the need to provide more funding to the OAIC.

"The OAIC should not be stretched or have to reduce its other capabilities to undertake these important COVIDSafe app oversight duties," shadow Home Affairs minister Kristina Keneally said.

In response, Foreign Affairs Minister Marise Payne said government would work with the OAIC in the lead-up to the next federal budget, now due in October.

"I would affirm for the record that, since this government was elected, funding to the OAIC has increased by over 75 per cent. As we do with all agencies, we'll continue to work with the OAIC to understand their resourcing requirements moving forward," Senator Payne said.

The OAIC did receive a $25 million funding boost from the government in 2018. But this was used to conduct its new duties under changes to the Privacy Act rather than address its existing workload and backlog. The OAIC used this funding to increase its staffing levels to 124.

But each element of the OAIC's work is rapidly increasing, including privacy complaints and FOI review requests. From July, the OAIC will also have an oversight and enforcement role for the open banking scheme, and this will be extended to other sectors soon too.

The OAIC had previously provided quarterly reports on the mandatory data breach notification scheme but is now only releasing one annually. It is also investigating controversial AI firm Clearview and has launched legal proceedings against Facebook.

Do you know more? Contact James Riley via Email (mailto:james@innovationaus.com) or Signal (https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en_AU).

Related: Angelene Falk (https://www.innovationaus.com/tag/angelene-falk/) | Christian Porter (https://www.innovationaus.com/tag/christian-porter/) | David Paris (https://www.innovationaus.com/tag/davidparis/) | Digital Rights Watch (https://www.innovationaus.com/tag/digital-rights-watch/) | Kristina Keneally (https://www.innovationaus.com/tag/kristina-keneally/) | OAIC (https://www.innovationaus.com/tag/oaic/) | Office of the Information Commissioner (https://www.innovationaus.com/tag/office-of-the-information-commissioner/) | Privacy (https://www.innovationaus.com/tag/privacy/)

Commissioner brief: Complaint backlog strategy

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.

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.
- The 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

  - substantially increasing the number of conciliations conducted to seek to reach resolution by agreement
  - providing additional resources to assist with the determination of matters where appropriate.

- The project started on 4 November 2019, with the first phase completing at end January 2020 and the second in mid-May 2020.
- At the end of June 2019, we had 1465 complaints on hand with 316 awaiting allocation and had closed 727 matters (compared with 690 closed the previous year) with an average handling time of 5.4 months.
- After completion of the project by end June 2020, we had 785 matters on hand with 79 awaiting allocation and had closed 554 matters with an average handling time of 5 months.
- Although the numbers of complaints received in financial year 2019-20 had decreased by 19% compared with the previous financial year, the number of matters closed increased by 15%, being 3366 compared with 2920.
- For Quarter 1 2020-21 July- September 2020, we received 691 complaints and closed 515. Our average handling time for complaints in the financial year Q1 is 4.4 months.
- Matters are now listed for a conciliation within 14 – 21 days of receipt from the early resolution team, with few exceptions.

Information about the Early Resolutions Team's project

- The Early Resolution (ER) team ran a 3-month backlog project from 1 November 2019 to 31 January 2020.
- The ER Team reviewed its current work in progress and set aside any complaint received between 17 July 2019 and 25 October 2019 and placed those 324 matters in a 'backlog' queue.
- The ER Team engaged 3 FTE contractors to replace three officers in the Privacy ER Team, as those officers formed the ER Backlog Team. The total cost of these 3 contractors was $114,101.63 (inc gst).
- The team took a strategic approach to the problem which included having a small team in a separate space focused only on the backlog, batching complaints and administrative improvements that made issues easier to identify. They also improved templates, tightened timeframes and streamlined processes.
- At the end of the project: the team had closed 226 matters; 33 matters were referred to the Investigations/CII team and the remaining 64 matters were finalised in following weeks.

DR Investigation & Conciliations team's results

- The Investigation & Conciliations team ran its project from 4 November 2019 to 18 May 2020.
- The team reviewed and amended its processes, had staff trained as accredited mediators and appointed FTE contractors to fill vacant positions.
- In the first phase the team focussed on reviewing older more complex matters, preparing matters for investigation with conciliation at week 6, and finalising matters against new time frames.
- By early February 2020, all matters in the investigation intake queue had been assessed and moved to either a conciliations or an investigations queue.
- In the second phase, the team moved to a full conciliation model, with conciliation attempted prior to opening an investigation. At the time approximately 70% of conciliations led to a resolution.
- Three FTE officers were dedicated to conciliating matters, a part time officer was re-deployed as a conciliation listing clerk and two external conciliators were engaged. On 1 July 2019, the total backlog for the team was 639 matters of which 367 matters were awaiting allocation. By 18 May 2020, the total backlog for the team was 200 matters with 86 matters awaiting allocation, 67 listed for conciliation and 47 under investigation.
- At the end of the 2019-20 financial year, the team had 195 active matters with 74 awaiting allocation, 56 in conciliation and 65 under investigation.
- By end September 2020, the team had 172 matters with 77 awaiting allocation, 38 in conciliation and 57 under investigation.

Information about the Determinations Team's approach

- The Determinations Team (DT) is comprised of one EL2 FTE, one APS 6 FTE and one APS5 FT contractor. It commenced on 4 November 2019.
- DT has received complex complaints which have not resolved over a lengthy conciliation and investigation period.
- DT drafts preliminary views (PVs) which are the precursor to a determination under s 52 of the Privacy Act, setting out a view on whether there has been a privacy breach and recommended declarations. On receipt of a PV, the parties may decide to settle the matter or provide submissions to the OAIC. On receipt of submissions from the parties, DT assists the Commissioner by preparing the matter for determination.
- DT also uses powers under s 44 of the Privacy Act to complete investigations as required and provides advice to investigations officers about evidence gathering.
- The DT has established new processes and templates to support this function.

- DT has drafted 23 PVs and has finalised 8 determinations. To date, no parties have successfully settled their matters after receipt of a PV.

Possible questions

- ***Was the backlog project successful?***

  During the first 3 months of the backlog project (4 November 2019 – 31 Jan 2020) the OAIC closed 905 complaints. Compared to the same period the last year (609 complaints) this was an increase of 296 complaints, or a 48% increase.

  We have also seen further increases in the numbers of complaints finalised. In the 2017-18 financial year, the average number of complaints closed per month was 230.5, which increased to 243.5 in the 2018-19 financial year. For the 2019–20 financial year, the average was 280.5 complaints closed per month.

  Since end January 2020, with changes in procedures we are also seeing earlier resolution of matters allocated to conciliation and investigation.

- ***How did the average time taken to close a complaint improve during the backlog project?***

  For the backlog project period 4 November 2019 to 31 January 2020, the average time taken to close a complaint was 132 days, or 4.3 months. This was a significant improvement from the start of the 2018-2019 financial year, as from 1 July 2019 to 3 November 2019 the average time taken to close a complaint was 5.1 months.

  For the financial year 2019–20 overall, the average time taken to close a complaint was also 5.1 months and by end of September 2020 it was 4.4 months.

- ***Have waiting times for allocation improved?***

  The waiting times for allocation improved in the Early Resolution space following the backlog project. Before the backlog project the oldest matter awaiting allocation was just over 4 months old, and following the ER backlog project (and first three months of the Investigation backlog project) the oldest matter awaiting allocation was just over 1 month old (as at 6 February 2020).

  In the Investigation & Conciliations team, all matters awaiting allocation to investigation have either been to conciliation and not resolved or assessed as not suitable for conciliation.

  Conciliation are now listed for a conciliation within 14 – 21 days of receipt from the early resolution team, with few exceptions.

  How much was spent on external conciliators?

  External conciliators were appointed to end June 2020, and the cost of these conciliations was $26,666.49.

Key dates

- Backlog project commenced on 4 November 2019
- The Early Resolution team's project finalised in 31 January 2020 (phase one)
- The Investigation & Conciliations team's project finalised in mid May 2020 (phase two)
- From 1 February 2020, the Investigation & Conciliation team began working on the conciliation focussed model that is now in place.

Document history

Updated by	Reason	Approved by	Date
Cecilia Rice /Sara Peel/Cate Cloudsdale.	October 2020 Senate Estimates	Angelene Falk	October 2020

Commissioner brief: My Health Record

Key messages

- After the end of the opt-out period on 31 January 2019, the Australian Digital Health Agency (ADHA) created My Health Records for all individuals. The records are available to individuals and participating healthcare providers.
- During 2019-20, the OAIC's regulatory work relating to MHR has focussed on:
  - 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;
  - engaging with the ADHA about the Australian National Audit Office's (ANAO) performance audit of the My Health Record system and the ADHA's implementation of the ANAO's recommendations, as well as privacy aspects of the system more generally;
  - promoting guidance materials, including the Guide to health privacy, a privacy action plan for health practices, and a new data breach action plan for health service providers;
  - promoting consumer resources including information about privacy and the My Health Record system;
  - providing preliminary input and preparing a formal submission to the Review of the *My Health Record Act 2012* (MHR Act), which is due to finalised by 1 December 2020.
- On 26 June 2020, the OAIC and ADHA signed an updated MOU, effective from 1 July 2020 until 30 June 2021, to provide $2,070,000 for its regulatory functions relating to the MHR system under the *Privacy Act 1988*, *My Health Records Act 2012* and *Healthcare Identifiers Act 2010*.
- On 25 November 2019, the ANAO released its audit report: Implementation of the My Health Record system. The objective of the audit was to assess the ADHA's effectiveness in its implementation of the MHR system under the opt-out model. Then ANAO report contained 5 key recommendations to improve risk management and evaluation across the MHR system. On 20 February 2020, the ADHA published its Implementation Plan in response to the audit report. The OAIC is closely engaging with ADHA in relation to its implementation of the ANAO recommendations.

Enquiries, complaints and NDBs

- During the 2019–20 financial year, the number of MHR enquiries and complaints received by the OAIC decreased significantly compared to the 2018–19 financial year. The decrease can be attributed to lower community interest in the MHR system compared to the previous financial year when there was high community interest in the My Health Record system during the opt-out period, which occurred from 16 July 2018 to 31 January 2019.

	July 2012 (MHR system commencement) to 30 June 2018	1 July 2018 to 30 June 2019	1 July 2019 to 30 June 2020
Enquiries	83	155	7
Complaints	12	104 (62 received, 42 finalised)	41 (10 received, 31 finalised)
Mandatory data breach notifications	88	35	1

- The number of data breach notifications has also significantly decreased in the 2019/20 financial year. The OAIC is not aware of any change in work to identify intertwined records, and this decrease could be attributed to a lower incidence of intertwined medical records than in previous financial years. Specifically:
    - intertwined Medicare records of individuals with similar demographic information, resulting in Medicare providing data to the incorrect individual's MHR, and
    - findings under the Medicare compliance program that certain Medicare claims were made in an individual's name due to an attempt to commit fraud and were uploaded to the individual's MHR.

Assessments

- In September 2020, the OAIC completed 3 assessments that looked at whether new participants in the MHR system had appropriate governance and information security arrangements to manage access security risks.
    - The OAIC surveyed 14 pharmacies, 8 pathology and diagnostic imaging service providers and 2 private hospitals under APP 1.2 and 11, and Rule 42 of the My Health Records Rule 2016 (MHR Rule). The OAIC also conducted fieldwork for the 2 private hospital assessments.
    - The finalised reports were published on our website in September 2020.

- These Assessments identified privacy issues relating to information security and access control practices of healthcare provider organisations including in relation to:
    - instances where policies required under MHR Rule 42 not being in place, lacking necessary detail, not being reviewed, not being properly communicated to staff including contractors and consultants
    - instances where training was not being provided to staff (including contractors and consultant) before they are granted access to the MHR system
    - the ADHA's password standard of 13 or more characters not being applied, and
    - audit logs not being used or being used in a limited way.

- In September 2020 the OAIC published guidance on security requirements of Rule 42 of the My Health Records Rule.
- Between April 2014 and June 2020 the OAIC completed 15 privacy assessments of the MHR system and Healthcare Identifier service.
    - Seven of these assessments focused on security aspects of the system, with a view to identifying risks to ensure the safety and integrity of the data held in the MHR system.
    - Assessments targeted the System Operator (ADHA) and its management of the National Repositories Service (NRS - the database system operated by the System Operator which holds the key data sets which make a My Health Record), Department of Human Services (now Services Australia), and end users of the system including GP clinics and hospitals.
    - Assessments identified privacy issues relating to:
        - end point user access and security risks (healthcare providers accessing the system)
        - inconsistent implementation of 'privacy by design' by the System Operator when there were major changes or upgrades to the MHR system involving personal information
        - incident management, in particular how personal information is shared among MHR stakeholders in the context of managing information security and privacy incidents
        - documentation of privacy and information security policies and procedures.
    - The OAIC made recommendations to address these risks, including:

        - ensuring healthcare providers improve access security measures (such as documented access security policies and procedures and consideration of audit logs)
        - implementing a 'privacy by design' approach through the use of privacy impact assessments (PIAs)
        - implementing security measures when personal information was shared among MHR stakeholders in the context of managing information security and privacy incidents (such as encryption of personal information and deletion of data)
        - ensuring the System Operator had appropriately documented privacy and information security policies and procedures in place.
    - For the last assessment of the system operator (completed June 2020), the ADHA (and previously the Department of Health) responded to and accepted almost all of the OAIC's recommendations. The OAIC intends to follow up the implementation of the recommendations with ADHA in July 2021.
- Findings from these assessments informed policy guidance recently released by the OAIC relating to access security for healthcare providers accessing the MHR system.

ANAO Audit

- On 25 November 2019, the ANAO released its final audit report on the Implementation of the My Health Record system. The objective of the audit was to assess the effectiveness of the implementation of the MHR system under the opt-out model.

- Generally, the ANAO found that:
    - implementation of the MHR system was largely appropriate
    - implementation planning for and delivery of MHR under the opt-out model was effective
    - risk management for the expansion program was partially appropriate
    - monitoring and evaluation arrangements are largely appropriate.

- The report made five recommendations:
    - **Recommendation 1:** ADHA conduct an end-to-end privacy risk assessment of the operation of the My Health Record system under the opt-out model, including shared risks and mitigation controls, and incorporate the results of this assessment into the risk management framework for the My Health Record system.
    - **Recommendation 2:** ADHA, with the Department of Health and in consultation with the Information Commissioner, should review the adequacy of its approach and procedures for monitoring use of the emergency access function and notifying the Information Commissioner of potential and actual contraventions.
    - **Recommendation 3:** ADHA develop an assurance framework for third party software connecting to the My Health Record system — including clinical

software and mobile applications — in accordance with the Information Security Manual.
    - **Recommendation 4:** ADHA develop, implement and regularly report on a strategy to monitor compliance with mandatory legislated security requirements by registered healthcare provider organisations and contracted service providers.
    - **Recommendation 5:** ADHA develop and implement a program evaluation plan for My Health Record, including forward timeframes and sequencing of measurement and evaluation activities across the coming years, and report on the outcomes of benefits evaluation.

- The Australian Digital Health Agency and the Department of Health agreed with the ANAO's recommendations.

- On 20 February 2020, the ADHA published its Implementation Plan in response to the audit report. The OAIC is closely engaging with ADHA in relation to its implementation of the ANAO recommendations.

Review of the My Health Records Act

- On 24 February 2020, Professor John McMillan AO was appointed to conduct a review of the MHR Act, and to provide a report to the Minister for Health by 1 December 2020.

- The review is required under s 108 of the MHR Act and aims to ensure the legislation underpinning the My Health Records system is enabling the system to work as well as it can for all Australians.

- The formal consultation period for the review opened on the 25 September 2020, with submissions due by 21 October 2020. The OAIC is currently preparing its submission to inform the review.

New Guidance

- In our meetings with ADHA on 7 April 2020 and 5 May 2020, the ADHA requested that the OAIC develop guidance about emergency access use and security requirements for healthcare providers, to be published on OAIC's website. The security requirements (Rule 42) guidance has been published and the emergency access guidance is currently under development.

Possible questions

What is the OAIC's role and regulatory experience in the MHR system?

- The OAIC is the independent regulator of the privacy provisions relevant to the MHR system. This role is funded through an MOU with the ADHA.
- The OAIC responds to enquiries and complaints; receives mandatory data breach notifications; conducts privacy assessments; and advises on the privacy aspects of the system. The MHR Act and Privacy Act provide a range of investigative and enforcement mechanisms to the OAIC.

What are the OAIC's views on the system's security arrangements?

- A key focus of the OAIC's MHR assessments in 2019-20 has been
    - Healthcare provider organisations who are new participants in the MHR system and whether they have appropriate governance and information security arrangements to manage access security risks
    - compliance with the requirements of Rule 42 of the My Health Records Rule 2016 for healthcare provider organisations to implement an MHR access security policy that addresses certain matters, including security controls, employee training, identification processes for access and risk mitigation strategies.
    - the reasonable steps taken by healthcare provider organisations to protect personal information and implement practices, procedures and systems to ensure compliance with the Australian Privacy Principles (APPs), pursuant to APPs 1.2 and 11 for the MHR context.
- The OAIC's MHR assessments in 2019-20 provide examples of compliance, non-compliance or partial compliance by registered HPOs in the MHR system with the APPs/Privacy Act and the MHR Rule. These Assessments identified privacy issues relating to information security and access control practices of healthcare provider organisations, including:
    - Instances where policies required under MHR Rule 42 not being in place, lacking necessary detail, not being reviewed, not being properly communicated to staff including contractors and consultants
    - instances where training was not being provided to staff (including contractors and consultant) before they are granted access to the MHR system
    - the ADHA's password standard of 13 or more characters not being applied, and
    - audit logs not being used or being used in a limited way.

What is the OAIC's response to the ANAO audit report on the implementation of the My Health Record system?

- The OAIC has considered the findings of the final audit report and the ADHA's implementation plan as part of our ongoing regulatory role. The report identifies a number of privacy-related risks which were also under consideration by the OAIC, such as in our recent privacy assessments.

- The OAIC supports the recommendations made and has welcomed the opportunity to work with the ADHA, Department of Health and any other relevant stakeholders towards implementation of the recommendations, where appropriate.

- The OAIC notes that the report makes observations about the OAIC's 'failure to complete' privacy assessments under the 2017-19 MOU. While it is correct that under the 2017-19 MOU no assessments had been completed (that is, a finalised report issued to the entities involved), at the time the OAIC had conducted the document review and fieldwork component for four privacy assessments – including providing feedback to entities during an exit interview - within the MOU timeframe. Reporting for these assessments has been finalised.

Key dates

- On 25 November 2019, the ANAO released its audit report: *Implementation of the My Health Record system*.
- On 20 February 2020, the ADHA published its Implementation Plan in response to the ANAO's audit report on the MHR system.
- On 26 June 2020, the ADHA and the OAIC signed an updated MOU effective 1 July 2020 to 30 June 2021.
- The review of the MHR Act is currently underway and is due to be completed by 1 December 2020.
- The opt-out period started on 16 July 2018 and concluded on 31 January 2019 (having been extended on two occasions).

Document history

Updated by	Reason	Approved by	Date
Diana Weston	September 2020 Senate Estimates	Kellie Fonseca	25 September 2020

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 digital platforms and a review of the Privacy Act.
- The reforms outlined in the Government's response to the Digital Platforms Inquiry final report will ensure that our regulatory framework protects personal information into the future and holds organisations to account.
- The OAIC looks forward to continuing to work closely with the Attorney-General's Department during its review of the Privacy Act throughout 2020 and 2021.

Critical Issues

- The Australian Government's response to the ACCC's *Digital Platforms Inquiry Final Report*, included commitments to:
    - consultation on draft legislation for the reforms announced in March 2019 to increase the penalties under the Privacy Act to match the Australian Consumer Law and require development of a binding online privacy code
    - Consult on recommendations to:
        - Update the definition of personal information
        - Strengthen notification requirements
        - Strengthen consent requirements and pro-consumer defaults
        - Introduce direct rights of action for individuals
    - Conduct a broader review of the Privacy Act and related laws to consider whether broader reforms are necessary in the medium-to-long terms.
- We understand that the passage of development of the draft legislation and the broader review of the Privacy Act have been delayed as a result of COVID-19 priorities for AGD and the Government.
- The interaction between the Privacy Act and other regulatory regimes will be a key aspect of the review. In particular, the intersection between consumer/competition law and privacy law is an area of interest for regulators across the world, and the OAIC is engaging with our international networks to consider these issues.

Possible questions

Are you happy with the Government's timeline for privacy law reform?

Yes. I welcome the commitments to reform made in the Government's response to the DPI report. The reforms are an important step in enabling effective regulation of personal information handling, in line with community and business expectations for the digital environment. A privacy framework that empowers consumers and allows them to trust that their personal information will be protected supports both innovation and economic growth. It is regrettable that the reform timeline has been delayed, however this is understandable given the other issues of national importance that the Government has been grappling with this year.

How will your office participate in this law reform process?

As Australia's national privacy regulator I look forward to working with the Government and other stakeholders throughout the reform process by sharing our expertise and the intelligence gathered through our regulatory work.

I have created a dedicated team to lead the development of the code and the OAIC's engagement with the Privacy Act review. We will be drawing on our regulatory experience to make recommendations to Government about improvements to Australia's privacy framework that support my four key priorities:

1. Enabling privacy self-management — ensuring there are sufficient clear and understandable options built into the system
2. Organisational accountability — ensuring there are sufficient obligations on organisations that deal with personal information built into the system
3. Global interoperability — making sure our laws continue to connect around the world, so our data is protected wherever it flows and reduce the regulatory burden on international businesses
4. A contemporary approach to regulation — having the right tools to regulate in line with community expectations.

Do we need GDPR style protections in Australia? What can we learn from other data protection regimes that may be of benefit to Australians?

My Office is actively considering what lessons can be learned from the GDPR and other international privacy regimes. The OAIC will seek to draw on the GDPR where it provides a useful and feasible model for reform in Australia, but will also seek to provide advice and insight to Government on other options for reform that will best suit the needs of Australians and the digital economy, where appropriate.

The OAIC supports greater interoperability of our privacy rules with other jurisdictions, as this will help minimise regulatory friction for business and ensure Australians' data is protected wherever it flows.

We have commissioned a number of research pieces that consider international experiences to analyse how they could be of benefit to the Australian privacy framework,

and these findings will be fed into our submissions to the Privacy Act review and our broader regulatory work.

Key dates

- The public timetable for reforms remains that set out in the Governments response to the DPI.

Key Facts

- The reforms will be an important step in enabling effective regulation of personal information handling, in line with community and business expectations for the digital environment.

- The OAIC sees value in maintaining Australia's technology-neutral, principles-based law, supplemented by particularisation through Codes.

- The review of the Privacy Act could consider additional rights for individuals and provide greater accountability for organisations, drawing upon lessons learned from the GDPR and other international privacy regimes.

- The OAIC will also be seeking amendments to enhance both its information sharing powers and selected regulatory powers to ensure it can perform as a contemporary and effective regulator.

- To facilitate our active participating in the law reform process, we have commissioned external research into the following subject matter areas:
    - The definition of personal information
    - Notice and Consent
    - Harms in the digital age
    - Children and vulnerable groups
    - Certification schemes
    - Online identifiers and cookies
    - Direct right of action
    - Facial recognition and biometrics

Document history

Updated by	Reason	Approved by	Date
Melanie Drayton	Estimates March 2020		
Sarah Croxall	Estimates October 2020	Angelene Falk	October 2020

Commissioner brief: International regulatory developments

Key messages

- As personal information moves across borders and privacy threats and challenges extend internationally, a coordinated and consistent global approach to privacy concerns is essential.

- The OAIC actively engages with a range of international privacy and data protection fora, e.g. in October 2018, I was elected to the Global Privacy Assembly the leading global forum of data protection and privacy authorities with more than 120 members across all continents. I have been actively involved in a number of ExCo initiatives (Statement on contact tracing measures and COVID-19 pandemic). I have recently taken the position of chairing the Strategic Direction Sub-Committee, which has responsibility for overseeing the implementation of the Global Privacy Assembly's Strategic Plan.

- We are committed to engaging with our counterparts across the globe, to ensure that we can learn from their experiences, identify areas of synergy and be at the forefront of international collaboration. We have recently signed MOUs with the UK Information Commissioner's Office and the Singaporean Personal Data Protection Commission to strengthen our collaboration with these two jurisdictions.

- We also 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.

- We are monitoring international privacy developments, particularly in Europe and the USA. For example, in January 2020 the Californian Consumer Privacy Act came into force in California. My office has spoken with officers at the California Attorney General's Department to discuss the implementation of the new legislation.

Critical facts

1. Global Privacy Assembly

- Virtual Engagement: Global Privacy Assembly's Closed Session, 2020:
    - Due to the COVID-19 pandemic, the Global Privacy Assembly's (GPA) Annual Conference was virtually from 12 October to 16 October. Angelene Falk and Elizabeth Hampton attended the conference.
- COVID-19 related activities:
    - The GPA's Executive Committee has established a GPA COVID-19 Taskforce to consolidate data protection authorities and stakeholders' efforts, maximise the voice of the GPA, gather expertise, and assist GPA members and observers in addressing emerging privacy issues posed by COVID-19.
    - As part of its efforts to promote capacity building and share insights and best practice responses to COVID-19, the GPA has run, jointly and singularly, several webinars to address and consider privacy and data protection challenges and issues arising from the COVID-19 pandemic. These webinars include:
        - GPA-OECD: 'Addressing the data governance and privacy challenges in the fight against COVID-19' – 15 April 2020.
        - GPA COVID-19 Taskforce: 'Contact Tracing and the Apple and Google Solution: In conversation with the technical specialists' – 6 July 2020.
        - GPA COVID-19 Taskforce: 'Data Protection Authorities as Enablers and Protectors: The Role of Data Protection Authorities as they confront COVID-19 – Contact Tracing and the Recovery Response – 23 July 2020. Angelene Falk moderated the panel for this webinar.
        - GPA COVID-19 Taskforce-Centre for Information Policy Leadership: 'Data Protection Reimagined: Digital Acceleration, New Emerging Issues and the Role of Privacy Regulators in the COVID-19 era' – 6 August 2020.
        - GPA COVID-19 Taskforce-IAPP: 'New Normal: Data Protection, Security, Privacy and Safety in the Workplace' – 25 August 2020.
        - OECD-GPA COVID-19 Workshop: 'The Road to Recovery: Lessons learned and challenges ahead' – 16 September 2020.

2. Asia Pacific Privacy Authorities (APPA) Forum

- Upcoming Virtual Engagement: 54th APPA Forum, 2020:
    - The next APPA Forum will be hosted by the Office of the Victorian Information Commissioner from 8 to 10 December 2020.
- Virtual Engagement: 53rd APPA Forum, 2020:
    - On Tuesday 2 June to Thursday 4 June, Angelene Falk, Elizabeth Hampton and Melanie Drayton attended the APPA Forum virtually, which was hosted by the Singaporean Personal Data Protection Commission. During the Forum, OAIC Executive discussed with Privacy Commissioners and professionals from the Asia Pacific region topical issues in privacy regulation, privacy challenges and issues raised by COVID-19, and best practices in responding to such challenges.

  - The OAIC presented on the Australian experience encountered in response to privacy issues raised by the COVID-19 pandemic, and Australia's upcoming review of the *Privacy Act 1988*.
  - APPA held a webinar side-event on COVID-19, which explored privacy opportunities and challenges brought about by COVID-19; partnerships between data protection authorities, industry and public health care authorities in managing COVID-19; and data protection and privacy in the "new normal".
- Philippines: APPA Forum
  - On 2 December to 3 December 2019, Angelene Falk and Melanie Drayton attended the 52nd APPA Forum in Cebu, Philippines and met with Privacy Commissioners and professionals from the Asia Pacific region to consider best practices on privacy regulation, new technologies and the management of privacy matters.

3. Australian Government - Agreements with Foreign Counterparts

- Singapore: Australia-Singapore Digital Economy Cooperation Initiative
  - Australia and Singapore signed an enhanced digital economy cooperation Agreement (on an economy wide level) on August 2020, having concluded negotiations in March 2020.
  - OAIC provided advice to DFAT on Australia's privacy framework and landscape.

OAIC MOU with the UK ICO

- The OAIC and the ICO have recently negotiated and signed an MOU to increase collaboration between our offices (Link to the signed MOU: D2020/001291).
- Potential areas of collaboration between the ICO and the OAIC include:
  - Technology (Artificial Intelligence and facial recognition technology and surveillance),
  - Regulatory activity (Regulatory sandboxes and Regulatory and enforcement activity)
  - Policy (Cybersecurity, certification schemes and children's privacy).
- The OAIC also commenced a joint investigation with the UK ICO into the information handling practices of Clearview AI. This joint investigation is being conducted under the MOU and the Global Cross Border Cooperation Enforcement Arrangement.

OAIC with the Singaporean PDPC

- The OAIC and the PDPC have recently negotiated and signed an MOU to increase collaboration between our offices (Link to the signed MOU: D2020/005302 and D2020/005303).
- Potential areas of collaboration between the OAIC and PDPC include: Policy and information exchange in the areas of data portability, emerging technology, COVID-19 related matters; the promotion of the APEC CBPR system/Cross border data transfers;

policy, intelligence and enforcement of data breach notification schemes; and strategic issues of enforcement and intelligence.

Possible questions

- ***Does Australia need to obtain EU adequacy? What are the barriers, if any?*** This is a matter for the Attorney-General's Department. In 2001, the EU's Article 29 Working Party (WP29) issued an opinion on the level of protection offered by the Australian Privacy Amendment (Private Sector) Act 2000, which introduced the National Privacy Principles that applied to business before the 2014 Privacy Act reforms. WP29 noted 'with concern' that some exceptions to the NPPs, in particular the small business and employee records exceptions (link).

- ***Does the GDPR (or other international instrument) show that the Privacy Act requires amendments?*** The Australian Government recently announced a review of the Australian Privacy Act. As part of this review, the OAIC is committed to scrutinising other frameworks.

  My Office will advise Government to ensure that any requirements that are adopted fit within the Australian context, whilst ensuring that Australia's privacy framework is interoperable with other frameworks around the world.

  While the GDPR tends to be more prescriptive than the principles-based Australian Privacy Principles (APPs), many GDPR requirements would be expected of entities in their complying with relevant APPs or other Privacy Act obligations. For GDPR obligations that differ, as the GDPR only recently commenced, the OAIC is monitoring its implementation progress with interest, with a view to assessing whether any aspects of the GDPR could be replicated in the Australian context to secure better data protection outcomes for all Australians.

  Some of the underlying principles in the GDPR are incorporated into the ACCC's recommendations to Government from their *Digital Platforms Inquiry* , such as recommendations 16 to 18 which call to strengthen notification requirements, introduce certification schemes, strengthen consent requirements, and enable the erasure of personal information respectively. The OAIC worked with the ACCC throughout the course of the Digital Platforms Inquiry and continues to work with the Australian Government in considering these recommendations. Also of note is the right to data portability under article 20 of the GDPR, which is similar in effect to the proposed Consumer Data Right in Australia. A direct right of action to the courts for breaches of the GDPR under article 79 is similar in effect to a right of action under the Consumer Data Right for breaches of the CDR privacy safeguards.

- ***Will Australian businesses be impacted by the Schrems II decision?***
  The influence of this decision on international data transfers more generally is likely to be significant and we will be monitoring developments in this area and its impact for Australian businesses. The Court of Justice of the European Union (CJEU) decision found that EU and US companies could no longer use the EU-US Privacy Shield as a valid transfer mechanism due to the ability of US law enforcement and national security to access the transferred data.

  It also called into question the use of Standard Contractual Clauses as a transfer mechanism, calling on companies to undertake a case-by-case assessment of the surrounding environment to determine whether the data is adequately protected from acquisition by public authorities. Companies would need to make an assessment of the surrounding environment and legal frameworks and adopt supplementary measures to ensure its protection.

  This part of the decision has potential implications beyond the EU-US Transatlantic border transfers, and may have implications for Australian businesses, if EU companies or EU data protection authorities were to form the view that that data being transferred could be subject to an order by Australian public authorities. However, at this stage the implications are unclear, and further guidance is needed from the EU.

Regulatory developments

International regulatory developments related to surveillance

- In all jurisdictions (Europe, United Kingdom, United States, Canada, New Zealand) the use of surveillance devices is likely to collect personal information (or personal data) and is covered by privacy legislation and regulations.

- In Canada, the EU and the US, there are different regulatory and legislative frameworks in place to regulate surveillance conducted by government and official authorities, compared to surveillance conducted by private companies and organisations.

- Generally, in each jurisdiction there are exceptions relating to the use of surveillance for the purposes of law enforcement and national security.

- The use of surveillance for law enforcement and national security purposes is in some instances regulated by standalone legislative frameworks. For example, the UK has a standalone Surveillance Camera Commissioner to encourage compliance with the Surveillance Camera Code of Practice which applies to local authorities and the police operating surveillance camera systems.

New Zealand's Privacy Law reform of 2020

- In June 2020, New Zealand passed a bill that reformed New Zealand's privacy laws. The amendments include enhanced powers for the New Zealand Privacy Commissioner, stronger protections for cross-border data transfers, and new mechanisms that promote early intervention and risk management by entities, rather than relying on data subjects' complaints. The amendments will take effect on 1 December 2020.

Schrems II Landmark Ruling

- On 16 July 2020, the Court of Justice of the European Union (CJEU) released its judgment on the *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* C-311/18 case (Schrems II). The Schrems II decision concerns the transfer of personal data from the EU to the US, particularly the validity of Standard Contractual Clauses and the EU-US Privacy Shield Framework as transfer mechanisms.
- In its Judgment, the CJEU found that:
    - the EU-US Privacy Shield Framework is an invalid transfer mechanism, due to the ability of US law enforcement agencies to access data held by US companies.
    - Standard Contractual Clauses remain a valid transfer mechanism, but they must be assessed on a case-by-case basis as to the extent to which the receiving entity is subject to requirements to provide public authorities with access to that data.

Review of the GDPR

- The European Commission released its findings from a 2-year review of the General Data Protection Regulation (GDPR). The European Commission's report found that the GDPR has met most of its objectives, providing citizens with a strong set of enforceable rights and creating a new European system of government and enforcement. The report concluded that harmonisation across Member States is increasing, however, fragmentation of approaches must be continually monitored.

Developments in the EU on open data

- On 22 January 2019, the European Parliament, the Council of the EU and the EU Commission reached an agreement on revisions to Directive 2003/98/EC of the European Parliament and the Council on the re-use of public sector information ('PSI Directive') (link to revised text). Key aspects include:
    - public sector content that can be accessed under national access to documents rules will in principle be available for re-use, generally at no more than the marginal cost of providing it
    - in the case of 'high value' data sets (those with associated with important socio-economic benefits) the re-use must be at no cost

  - safeguards to prevent public sector information being 'locked in' through data deals with private companies, which would give those private companies exclusive use of the data
  - data will be available via Application Programming Interfaces (APIs), allowing it to be readily used in products and services (e.g. mobile apps).
- The revisions must next be formally adopted by the European Parliament and the Council of the EU, after which member states will have two years to implement the revised rules.

Japan's adequacy decision under the GDPR

- On 23 January 2019, the EU Commission adopted an adequacy decision on Japan, allowing personal data to be transferred from EU member states under the GDPR, to Japan without the need for other mechanisms such as contractual requirements to protect the information (although additional rules will apply around e.g. the on-disclosure of the information from Japan to third countries).
- This decision is reportedly part of an EU-Japan trade agreement that is in development (link).

UK ICO statement on use of Live Facial Recognition Technology by the Metropolitan Police Service

- On 24 January 2020, the ICO released a statement in response to the announcement by the Metropolitan Police Service (MPS) in its use of Live Facial Recognition (LFR) Technology. The ICO state that the MPS has incorporated the ICO's advice from an Opinion released on the use of LFR by police forces last October into its planning and preparation for future LFR use.
- The ICO have received assurances from the MPS that it is considering the impact of the technology and is taking steps to comply with requirements of data protection, and expects to receive further information from the MPS, shortly. The ICO reiterated its call for the Government to introduce a statutory and binding code of practice for the use of LFR as a matter of priority. (Link to ICO press release).

The Californian Consumer Privacy Act

- The Californian Consumer Privacy Act (CPPA) came into effect on 1 January 2020, with enforcement taking effect on 1 July 2020. The businesses affected include those that collect or participate in the processing of personal information in California, businesses whose gross revenue exceeds $25 million, businesses who process the personal information of at least 50,000 customers, households or devices every year, or businesses that derive 50% or more of its revenue from selling users' personal information.
- The main purpose of the CCPA is to give Californians more control over their personal information, by granting them a number of fundamental rights:
  - to know what personal information is being collected about them
  - to access this information
  - to know whether it is sold and to whom

- to ask that their personal data be deleted, and
- to refuse to allow their data from being sold.

CNIL decision against Google

- On 21 January 2019, CNIL imposed a €50 million penalty on Google, under the GDPR, arising from two complaints. CNIL found that Google was not meeting its obligations as:
    - information about its data handling practices was not sufficiently accessible to users and did not use sufficiently clear and plain language e.g., information about purposes of data processing (such as for geolocation and personalised advertising) and storage of data, were spread out across multiple documents, and was not expressed in clear or plain language (Articles 12 and 13)
    - Google relied on consent as the lawful basis for processing personal data for personalised advertising (Article 6). However, the consent was not sufficiently informed, and was not specific, or unambiguous (Articles 6 and 7).
- Google appealed this decision (link), however, France's top court for administrative law (the State Council) dismissed Google's appeal. In doing so, it confirmed that the CNIL's assessment that information relating to targeted advertising was not presented in a sufficiently clear and distinct manner for consent to be collected; and that the size of the fine was proportionate, given the severity and ongoing nature of the violations (link).

APEC CBPRs

- The APEC Joint Oversight Panel endorsed Australia's application to participate in the Cross-Border Privacy Rules (CBPRs) system in November 2018.
- The CBPRs were developed by participating APEC economies with the aim of building consumer, business and regulator trust in cross border flows of personal information.
- They require participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework. These are assessed against the minimum program requirements of the APEC CBPR system by an Accountability Agent, an independent APEC recognised private sector entity.
- It is intended that the OAIC will have oversight responsibilities once the system is implemented in Australia.
- The Attorney-General's Department will work with the OAIC and stakeholders to implement the system in Australia.
- Currently the 9 participating economies are USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei, and the Philippines.

Document history

Updated by	Reason	Approved by	Date
Renee Alchin	Estimates March 2020	Emi Christensen	04/02/2020
Alex The-Tjoean	Estimates October 2020	Emi Christensen	21/09/2020

Commissioner brief: Digital Identity

Key messages

- The OAIC welcomes the development of legislation for the Digital Identity scheme.[1]
- It is important that the legislation contains strong privacy protections to ensure that the identity information of Australians is protected, regardless of which type of entity is using that information.
- We consider that it is appropriate for the OAIC to regulate the additional privacy protections that are introduced through legislation, and that participants that are not currently covered by the Privacy Act or comparable privacy law must opt in to the Act to ensure that there is a consistent application of privacy protection.
- The Digital Transformation Authority (DTA) has also 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 will receive funding in the 2021-22 financial year to undertake two privacy assessments (audits) of the system and develop guidance materials.[2]
- We welcome the opportunity to engage with the DTA in its development of a privacy protective scheme 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 Federal Government agencies. It is proposed that the legislation will include additional privacy protections related to the scheme.
    - The DTA received funding in the 2020-21 Budget to expand the scheme over the next three years. This will include the rollout of the scheme to MyGov and a greater number of consumer-facing services integrated with the scheme.
- The OAIC is involved in both of these projects:

[1] The development of legislation and the OAIC's involvement in the expansion of the Digital Identity program are referred to in the DTA's 2020-21 PBS:
"As part of the 2020-21 Budget measure *JobMaker Plan – Digital Business Plan*, the Australian Government has provided the DTA with $50.2 million over two years from 2020-21. This funding is part of the broader commitment of $256.6 million to the DTA and partner agencies to deliver Digital Identity.
Digital Identity is all about making it easier and safer for people and businesses to get services and do business online. Expanding Digital Identity will see additional services connected to the system (including state and territory services). Improvements to privacy and security protections will be assured by the Office of the Australian Information Commissioner and the Australian Cyber Security Centre. A major component led by the DTA will be the development of legislation to expand the use of Digital Identity beyond Commonwealth entities. The legislation will embed the highest level of privacy, security protections and formalise ongoing governance arrangements for the system." (p137 of Social Services portfolio PBS)
https://www.dss.gov.au/about-the-department/publications-articles/corporate-publications/budget-and-additional-estimates-statements-budget-2020-21/portfolio-budget-statements-2020-21-budget-related-paper-no-112

[2] 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

  - The OAIC has consulted with the DTA since 2015 on the development of the Trusted Digital Identity Framework, which is the system of rules and protocols that underpin the Digital Identity scheme.
  - We are now engaging with the DTA on the development of legislation for the Digital Identity scheme, including as a member of the Steering Committee (OAIC Band 2), and as an observer on a IDC to develop the legislation for the scheme (OAIC EL2).
- The expansion of the Digital Identity scheme is intended to be used across many widely used consumer-facing Government services, including Centrelink, Medicare and the ATO. Legislation would also enable it to be rolled out to State/Territory and private sector services, and will therefore involve identity verification across jurisdictions. The privacy and security of the system will be critical issues.

Possible questions

What is the OAIC's role in relation to Digital Identity?

- The OAIC has worked with the DTA since the commencement of work on the Trusted Digital Identity Framework, providing advice on the privacy aspects of the framework. This role is continuing throughout the development of legislation for the Digital Identity scheme, and expansion of the scheme to a wider range of services across government. This work aligns with our strategic priority, set out in our Corporate Plan, to influence and uphold privacy frameworks, influencing policy and legislative change to ensure that these frameworks remain appropriate.

Do you think that the Digital Identity scheme adequately protects the privacy of individuals?

- The OAIC has been pleased with the amount of focus the DTA has had on privacy throughout the development of the TDIF and Digital Identity scheme.
- The OAIC will continue to undertake our monitoring, advice and guidance functions in relation to this work, to ensure that the DTA takes a best privacy practice approach to the development of the proposed legislation and expansion of the Digital Identity scheme.

The OAIC has received funding for Expanding Digital Identity commencing in 2021-22. Are you required to undertake any activities this financial year and what will you do with the funding next financial year?

- The OAIC is not receiving funding for activities in relation to this project in 2020-21, however we will continue to undertake our normal monitoring and guidance-related functions to help ensure that the expansion of the scheme includes appropriate privacy protections and aligns with the objects of the Privacy Act.
- The funding in 2021-22 will enable the OAIC to undertake two privacy assessments (audits) to proactively monitor the privacy protections built into the Digital Identity program, which will assist the Digital Transformation Authority to mitigate privacy risks

with the system. This funding also includes provision for the OAIC to develop guidance about the privacy aspects of the Digital Identity system.

Key dates

- 2014: The Financial Systems Inquiry (FSI) recommended a 'national strategy for a federated-style model of trusted digital identities'.
- 2015: DTA commenced work on the FSI recommendation, with the development of the Trusted Digital Identity Framework (TDIF).
- 2019: DTA receives funding to develop legislation to underpin the Digital Identity scheme, which will incorporate many of the TDIF requirements into law and enable the scheme to be used by State and Territory governments and the private sector, in addition to Federal Government agencies.
- 2020: DTA receives approval for funding to expand the Digital Identity scheme to a larger range of Commonwealth Government services, including many consumer-facing services such as MyGov. OAIC receives funding as part of the budget measure (JobMaker Plan – Digital Business Plan) to undertake two assessments and produce guidance.

Key Facts

- The Digital Identity Scheme will act as a single, secure way to use government and private sector services online. It intends to replace the 100-point identification check and remove the need to visit government offices with identity documents. The DTA have stated that it will be voluntary to use the scheme.
- The scheme is currently in limited use, primarily for businesses and their representatives through the MyGovID portal, which is operated by the ATO. The scheme is also being piloted for some community-facing services, including the Unique Student Identifiers scheme.
- The scheme is underpinned by the Trusted Digital Identity Framework (TDIF), which is a set of rules and standards that accredited members must follow to take part in the Digital Identity scheme.
- The framework aims to increase safety, security, consistency and reliability when accessing government services online. Collectively, the TDIF documents sets the standards for:
    - How personal information is handled by participating agencies and organisations
    - The useability and accessibility of identity services
    - Identity system security and fraud protection
    - Identity system management and maintenance
    - Framework governance.
- The DTA was recently provided with funding to develop the Digital Identity Bill (the Bill) which will underlie the scheme and incorporate many of the TDIF requirements into

legislation. It is proposed that the legislation will include additional privacy protections related to the scheme.

The remainder of this brief is not public and should be taken as background only

s 47E(d)

[redacted]

s 47E(d)

[redacted]

Document history

Updated by	Reason	Approved by	Date
Sarah Croxall	October 2020 Senate Estimates		29/09/2020

Commissioner brief: FOI IC reviews

Key messages

- The number of IC review applications received and finalised by the Information Commissioner has increased each year for the past five years.
  - increase in IC review applications *received* from 2015-16 to 2019-20 was 109%
    - 2019-20 – received 1,066 applications (15% increase on 18-19; 33% increase on 17-18)
    - 2018-19 – received 928 applications
    - 2017-18 – received 801 applications
    - Q1 2020-21 – received 297 (increase of 41% on Q1 19-20)
  - increase in IC review applications *finalised* from 2015-16 to 2019-20 was 83%.
    - 2019-20 – finalised 829 applications (26% increase on 18-19; 36% increase on 17-18)
    - 2018-19 – finalised 659 applications
    - 2017-18 – finalised 610 applications
    - Q1 2020-21 – finalised 261 (increase of 24% on Q1 19-20)
- The numbers of IC reviews on hand has steadily increased with the increase in IC review applications.
  - on 30 June 2019 - 850 IC reviews on hand
  - on 30 June 2020 – 1,088 IC reviews on hand
  - on 30 September 2020 - 1,124 IC reviews on hand.
- Agencies and ministers may apply to the Information Commissioner for an extension of time (EOT) during the processing of FOI requests.
  - In 2019-20 - 12% increase in EOT applications compared with 2018-19.[1]
  - In Q4 2019-20 – 21% increase in EOT applications and notifications (992) during COVID compared with 2018-19 (819)
  - In Q1 2020-21 – received 1,100 EOT applications and notifications (increase of 38% on Q1 2019-20, when 798 were received).
- In 2019-20 the increase in IC review applications and our focus on reducing the number of cases over 12 months old prevented us from reaching our target of finalising 80% of IC reviews within 12 months. In 2019-20, with a continued focus on reducing the oldest cases in the IC review case load, we finalised 72% (592) of IC reviews within 12 months.

[1] Where an agency or minister does not make a decision within the statutory timeframe or extended timeframe for processing, a decision refusing access is deemed to have been made under s 15AC of the FOI Act. An applicant may apply for IC review of a 'deemed decision'. The OAIC prioritises the processing of applications for IC review of 'deemed' decisions.

- In accordance with the scheme envisaged by the FOI Act, the OAIC seeks to resolve IC reviews informally using alternate dispute resolution in appropriate cases (that is, without them progressing to a formal decision by the Information Commissioner) and we continue to review our processes and procedures to ensure IC reviews are progressed in the most efficient and cost effective way. We used various approaches to help resolve an IC review such as:
    - narrowing the scope of a review
    - providing an appraisal or preliminary view
    - trying to reach agreement between the parties.
    - In 2019-20 we finalised:
        - 779 IC reviews without a formal decision being made (94%). This is an increase compared with 90.9% in 2018-19.
        - 334 IC reviews where the applicant withdrew their application (40%).
        - 29 IC reviews by written agreement between the parties under s 55F of the FOI Act.
        - 50 decisions of the Commissioner under s 55K of the FOI Act.
- The OAIC's IC review jurisdiction is complex. 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). There are often affected third parties whose interests and rights need to be considered. 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.
- Each IC review application received is assessed for complexity during the triage process. Cases are categorised accordingly to complexity and issue. Case categories assist with efficient case management and developing strategies to address the increasing numbers of IC review applications on hand. On 25 September 2020, of the 1006 IC reviews that had been categorised for complexity, 516 IC reviews (51%) had been identified as less complex and 490 were more complex (49%). Of these 1006 IC reviews, 325 had been identified as involving significant and systemic issues (32%).[2]

[2] Less Complex IC reviews include the following issues or exemptions: charges, searches, practical refusals, single exemptions; More Complex include the following issues or exemptions: various (more than one) exemptions and searches and/ or a large volume of material. Significant and systemic issues include: applications including MPs, national security and cabinet exemptions, requests that relate to highly publicised investigations or ongoing public debate.

Critical facts

- During the FOI Bill Senate Committee hearing, questions were asked about the time it takes to finalise IC reviews. A copy of the response provided to Questions on Notice is at **Attachment 1**.

Possible questions

- ***What is the average time to finalise IC reviews?***
  - In 2016-17 it was 190 days (6.3 months)
  - In 2017-18 it was 204 days (6.8 months)
  - In 2018-19 it was 237 days (7.8 months)
  - In 2019-20 it was 246 days (8.1 months).
- ***Why does the Australian Information Commissioner take so long to make IC review decisions - other jurisdictions have a 30 day time limit?***
  There is no statutory timeframe in the FOI Act.

  To afford procedural fairness the OAIC needs to ensure parties have an adequate opportunity to consider all information (including the submissions of other parties) and to make their own submissions.

  Further, the OAIC encourages informal resolution of reviews, which includes the ability of the agency to make a revised decision under s 55G of the FOI Act giving more access. Sometimes informal resolution does not result in the matter settling and a formal decision is required.
- ***In 2018–19 there were 60 IC review decisions under s 55K of the FOI Act, but only 50 formal decisions were made in 2019-20. Why has the number of formal decisions declined?***

  50 IC review decisions were made under s 55K in 2019-20.

	2018-2019	2019-2020
Affirm	19	24
Vary	37	7
Set Aside	4	19
Total:	60	50

  The OAIC seeks to resolve matters informally in appropriate cases, without the need for a formal decision by the Information Commissioner. This is consistent with the focus on alternative dispute resolution under the FOI Act.

  94% of the 829 IC reviews closed were finalised other than by the Commissioner making a formal decision under s 55K of the FOI Act. This is a result of working to resolve reviews informally, in accordance with the objects of the FOI Act. Further, there is now a

significant body of IC review decisions which provide guidance to Australian Government agencies when making FOI decisions.

We have devoted additional resources to our early resolution team. The number of IC reviews finalised has increased from

- 515 in 2016-17 to
- 829 in 2019-20, a 61% increase.

In 2019-20, the OAIC finalised 170 more IC review (829) than in the same period in 2018-19 (659) (26% increase).

- ***What steps has the OAIC taken to improve the efficiency in the IC review process?***

  In November 2019, the structure of the FOI Group was realigned to further streamline the processing of IC reviews, enhancing the functions of the intake and early resolution area and focussing on the early identification of systemic issues. The new structure allows a focus on addressing the consistent and increasing number of IC reviews received without a corresponding increase in staffing levels.

  The realignment is designed to:

  - increase the capacity of the Intake and Early Resolution team to resolve incoming IC review applications, to address the increasing allocations times and to allow for more senior capacity to work on finalising reviews early.
  - increase the capacity of the Investigations/Compliance team to finalise FOI Complaints and progress CIIs, which inform the affected agencies' process: in certain circumstances, this may also reduce the number of IC review applications received by the OAIC.
  - allow flexibility in allocating resources across the extension of time, IC reviews – deemed access refusal matters and the FOI complaints functions based on priority and workload.
  - allow closer monitoring of issues relating to agencies' compliance with the statutory processing timeframes, which assists current and potential FOI investigations.

  As discussed at previous Estimates hearings, we engaged an external consultant, Synergy, to review IC review business processes in April 2019. Following the Synergy review, the FOI Group identified key objectives to focus on from July to September 2019. These included finalising 50% of allocated IC reviews that were 12 months or older within three months. As at 1 July 2019, there were 125 IC reviews on hand that were over 12 months old from receipt. The FOI Group finalised 48 IC reviews and progressed 14 IC reviews to Information Commissioner decision under s 55K during the period July to September 2019. This was 50% of the target of 125 IC reviews.

  In November 2019, the Group undertook a further three-month focus period in relation to the IC review case load. The FOI team has focussed on particular cohorts or types of matters to improve timeliness and efficiency in the IC review process.

The Group is currently implementing other initiatives to improve the efficiency of the IC review process, including:

- a conferencing pilot for a particular cohort of matters and a particular agency, focused on engagement with parties in relation to a cohort of complex matters with a view to refining the scope of review
- a complex IC reviews pilot. This project encompasses 151 IC reviews from the unallocated reviews queue that involve complex issues and considerations. The project will involve review of each IC review with a view to:
    - engaging with applicants to confirm the scope of the review and where appropriate, providing a verbal preliminary view
    - engaging with respondents and where appropriate, providing a verbal preliminary review and inviting a revised decision under s 55G
    - identifying reviews that are ready to proceed to Commissioner decision under s 55K of the FOI Act.

Other process improvements include:

- Development and promotion of 'smartforms' for agencies to lodge extension of time applications (to support the existing IC review and FOI complaint application forms for applicants). Use of smart forms reduces the time needed to enter data on Resolve and reduces the need for case officers to contact agencies to ask for the information because the forms require certain information to be provided before the form can be lodged.
- Resolve review – we are currently working with developers to improve Resolve workflows. This will assist case officers to more efficiency progress IC reviews, FOI complaints and extension of time applications.
- Developing a procedure direction for applicants – this will clarify the OAIC's procedures for applicants and provide them with guidance about what the OAIC may require during an IC review.
- Batching of decisions – it is more efficient for case officers to focus on particular types of cases (for example, searches or practical refusals) or to focus on particular exemptions (in particular IC reviews involving single exemptions).
- Case categorisation – we have developed a system of categorising IC reviews to assist with identifying complexity and the appropriate review paths, as well as ensuring that cases are appropriately allocated to case officers.

- ***Are the OAIC's resources sufficient to undertake IC reviews?***
  We are continuing to increase the rate at which we finalise IC reviews, building on the greater efficiencies achieved in this area in 2017-18 when we finalised 610, and completing 2018-19 with 659 reviews finalised. However, we acknowledge that this is not keeping pace with the continuing rise in incoming work (in the first half of 2019-20, 464 IC reviews were received and 359 were finalised).

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.

- ***How many matters are being declined to allow the applicant to go directly to the AAT? Please provide an example of when this has happened.***
  In 2019-20, 83 matters were declined under s 54W(b) of the FOI Act (10% of the 829 reviews finalised).

  Under s 54W(b) of the FOI Act, the Information Commissioner may decline to undertake an IC review where the Commissioner is satisfied that the interests of the administration of the FOI Act make it desirable that the IC reviewable be considered directly by the AAT, rather than by the Information Commissioner first. Guidelines issued the Australian Information Commissioner under s 93A (FOI Guidelines) at [10.88] - [10.89] provide that:

  > The Information Commissioner can decline to undertake a review if satisfied 'that the interests of the administration of the [FOI] Act make it desirable' that the AAT consider the review application (s 54W(b)). It is intended that the Commissioner will resolve most applications. Circumstances in which the Commissioner may decide that it is desirable for the AAT to consider a matter instead of the Commissioner continuing with the IC review include:
  >
  > - the IC review is linked to ongoing proceedings before the AAT or a court
  > - there is an apparent inconsistency between earlier IC review decisions and AAT decisions
  > - the IC review decision is likely to be taken on appeal to the AAT on a disputed issue of fact, and
  > - the FOI request under review is complex or voluminous, resolving the IC review matter would require substantial allocation of resources, and the matter could more appropriately be handled through procedures of the AAT.
  >
  > The OAIC will consult the parties involved in a matter before making a decision under s 54W(b) to conclude an IC review.

- ***How many matters are awaiting allocation to a case officer?***

  The phrase 'awaiting allocation to a case officer' has been previously used by the OAIC to explain matters that are 'ready to be allocated' to a case officer for substantial case management through to a Commissioner decision under s 55K of the FOI Act.

  As at 30 September 2020, of the 1124 IC reviews on hand, there were approximately 222 reviews 'awaiting allocation to a case officer'. Reviews for which the OAIC is awaiting information/documents from either of the parties, or where the OAIC is assisting the parties resolve the IC review, are case managed by the OAIC's FOI Intake & Early Resolution team and are not included in this figure.

For completeness, I note that the phrase 'awaiting allocation to a case officer' carries an implication that IC reviews do not progress until allocated to a case officer, which is not an accurate reflection of the IC review process.

The IC review process aims to achieve early triage, intervention and resolution. The process includes:

- triage of IC reviews for validity
- assessment of incoming IC reviews to identify issues relating to complexity, significance and sensitivity, including whether decisions form part of a cohort of matters which raise systemic or significant issues
- obtaining copies of information relevant to the IC review from the respondent agency, for example, copies of the material at issue and submissions
- steps taken to advise parties of any issues which may require further submissions by the parties, commonly known as preliminary views, case appraisals or procedural fairness steps
- Upon receipt of this material, IC reviews are allocated to the team responsible for progressing reviews, based on the complexity, significance and systemic issues raised in the case.

IC reviews may remain with the Intake & Early Resolution team if the review can be resolved by way of dispute resolution procedures, or if it is proposed that an IC review not be undertaken (under s 54W of the FOI Act). Alternatively, the review may be allocated to the IC reviews or the Significant & Systemic Teams, depending on the complexity or sensitivity of the issues.

Once allocated to the relevant team, the review is progressed including by obtaining and sharing submissions on the issues in dispute and by providing preliminary views to the parties that may result in the respondent agency making a revised decision (to release further documents within the scope of the request) or withdrawal of the IC review application.

- ***What's the average time from application to a case officer being assigned?***

The process and timeframe for each review varies depending on the nature of issues and documents under review and whether the review should be resolved by way of a formal decision by the Information Commissioner under s 55K of the FOI Act.

As discussed earlier, IC reviews progress through different stages and do so without being allocated to an individual case officer.

The allocation timeframe to a case officer can vary considerably.

As at 30 September 2020, the oldest unallocated IC review (post early resolution) was received by the OAIC on 9 May 2018. On 30 September 2020, there were 222 reviews 'awaiting allocation to a case officer'. However, it is important to note, as set out above, that there are many case management activities undertaken prior to formal

allocation and the timeframe between the last case management event to allocation to a case officer can vary considerably, from a few weeks to a number of months.

- ***What is the number of open IC reviews that are on hand for more than 12 months?***
  As at 30 September 2020, there were 479 open IC reviews that had been on hand for more than 12 months from receipt.

Key dates

- **N/A**

Document history

Updated by	Reason	Approved by	Date
Raewyn Harlock	October 2020 Senate Estimates	Raewyn Harlock Rocelle Ago	1.10.2020 1.10.2020

Senator PATRICK: What's the average time it takes to get from an application to a case officer being assigned?
Ms Falk: I'll have to take that on notice. It changes, depending on the circumstances. And can I just be clear that we're talking along the same terms. When the matter arrives at the OAIC, it will be assessed and contact will be made. It will be triaged. There might be initial information sought, so there are time periods for that. And there will be also attempts at early resolution. If the matter is more complex and early resolution doesn't seem viable in the situation then what we're experiencing at present is a delay in allocating to a case officer for that. Perhaps I would call it more complex work that needs to be handled on the case.
Senator PATRICK: That's my own personal experience, and it seems to be quite a long time before you get assigned a case officer. Is it three months?
Ms Falk: That period of time has increased.
Senator PATRICK: Can you provide that on notice? The 120 days, in my view, is probably mostly taken up just even getting to a case officer—which I find totally unacceptable, I might point out.
Ms Falk: In the 120 days, as I said, there is active work done on the matters as soon as they're received. In the early resolution process, where we're experiencing the greatest delays are those matters that then need to go to more formal submissions. I can come back to you on notice with time periods there.

The response to the honourable senator's question is as follows:

The time to progress each IC review and the time it is formally allocated to a case officer varies from case to case depending on the complexity of the matters involved and the outcome sought by the IC review applicant.

The OAIC generally acknowledges receipt and triages an IC review application within three days of receipt, makes preliminary inquiries within two weeks and commences an IC review between three to eight weeks of receipt.

The process and timeframe for each review varies depending on the circumstance. For example, where an FOI decision is not made within the statutory timeframes, a decision to refuse access to a document is 'deemed' to have been made by the agency or minister. The IC review process for 'deemed' decisions is separate to the process followed where an applicant seeks IC review of an FOI decision where a statement of reasons has been provided by an agency or minister. In IC review applications involving 'deemed' decisions, the OAIC will conduct preliminary inquiries and may also issue a notice to the agency or minister to produce a statement of reasons and key documents within a specified timeframe.

Where an applicant seeks IC review of an FOI decision where a statement of reasons has been provided by an agency or minister, various case management events will generally occur early in the process, including case assessment by a senior officer, preliminary inquiries with an agency or minister, or issuing a notice to the agency or minister that an IC review has been commenced and requesting submissions and key documents to be considered during the IC review. These events will generally have occurred prior to formal allocation to a review officer.

Once allocated, opportunities to facilitate further informal resolution will be explored. This may include inviting the agency or minister to finalise a matter by agreement with the applicant or to make a revised decision in the applicant's favour.

In the 2017-18 year, 39% of IC review applications finalised were closed within 120 days of receipt and a further 30% were closed within 9 months of receipt.

At 31 October 2018, the time from receipt to formal allocation for those matters not resolved in the early stages was approximately eight and a half months, noting, as set out above, there are many case management activities undertaken prior to formal allocation and the timeframe between the last case management event to allocation to a case officer can vary considerably from a few weeks to a number of months.

Commissioner brief: 2019-20 Australian Government agency and ministerial FOI statistics[1] D2020/017448

Key messages

- The number of FOI requests made to Australian Government agencies and ministers in 2019–20[2] increased by approximately 6% over the previous year to 41,333 (when there was a 13% increase in the number of requests compared with the previous year).
- The Department of Home Affairs, Services Australia (formerly the Department of Human Services) and the Department of Veterans' Affairs together continued to receive the majority of FOI requests received by Australian Government agencies (70% of the total). Of these, 95% are from individuals seeking access to personal information.
- Of all FOI requests made to agencies and ministers, 81% were for personal information (33,584) and 19% for non-personal (7,749). This trend has been consistent over the past 4 years.
- 13,727 FOI requests were granted in full in 2019-20 (47% of all requests decided). This represents a decline in the percentage of FOI requests granted in full compared with 2018-19, when 52% of all FOI requests decided were granted in full.
- 11,221 FOI requests were granted in part in 2019-20 (38% of all requests decided). This represents an increase in requests granted in part compared with 2018-19, when 35% of all requests decided were granted in part.
- 4,410 FOI requests were refused in 2019-20 (15% of all requests decided). This represents an increase in requests refused compared with 2018-19, when 13% of all requests were refused.
- 79% of all FOI requests decided in 2019-20 were decided within the statutory timeframe. This is a decline in timeliness compared with 2018-19 (83%) and 2017-18 (85%) and may be due to the impact of the COVID-19 pandemic on agencies and ministers' ability to process FOI requests.
- There was a 25% decline in the amount of charges notified in 2019–20 ($267,069) than in 2018–19. There was a 28% decline in the amount of charges collected in 2019-20 ($88,090) than in 2018-19.
- The total cost attributable to processing FOI requests in 2019–20 was $63.91 million, approximately 7% more than the previous financial year's total ($59.85 million).
- There was a 106% increase in the number of documents agencies and ministers made available for direct download from their disclosure logs in 2019-20 (1,438) compared with 2018-19 (719).

[1] Percentages in this brief have been rounded to the nearest full number.
[2] In 2019–20, 294 agencies reported FOI statistics to the OAIC (however due to MOG changes not all these agencies were in existence at the end of the financial year).

Statistics

Period	Number of requests to agencies	% personal vs non-personal	Granted in full[3]	Granted in part[4]	Refused[5]	% processed within statutory timeframe
2019-20	41,333 (+6%)	81% pers (33,584) (-2 percentage points) 19% non-personal (7,749) (+2 percentage points)	47% (13,727) (-5% percentage points)	38% (11,221) (+3 percentage points)	15% (4,410) (+2 percentage points)	79% (23,066) (-4 percentage points) 80% pers (19,002) 73% non-pers (4,064)
2018-19	38,879 (+13%)	83% personal (32,440) 17% non-personal (6,439)	52% (15,623) (+2 percentage points)	35% (10,541) (+1 percentage point)	13% (3,980) (-3 percentage points)	83% (24,893) (-2 percentage points) 83% personal (21,233) 80% non-personal (3,660)
2017-18	34,438 (-13%)	82% personal (28,199) 18% non-personal (6,239)	50% (15,778) (-2 percentage points)	34% (10,767) (-1 percentage point)	16% (3,087) (+6 percentage points)	85% (26,879) (+27 percentage points) 85% personal (21,952)

[3] Expressed as a percentage of all FOI requests decided during the year.
[4] Expressed as a percentage of all FOI requests decided during the year.
[5] Expressed as a percentage of all FOI requests decided during the year.

						86% non-personal (4,927
2016-17	39,519 (+4%)	82% personal (32,383) 18% non-personal (7,136)	55% (18,877)	35**%** **(**11,767)	10% (3,385)	58% (19,607) 54% personal (16,343) 84% non-personal (3,264)

- The increase in FOI requests in 2019–20 was principally driven by a substantial increase in FOI requests made to Services Australia (+43%). Services Australia states that during the second half of 2019–20, they experienced a surge in FOI requests from 'a specific cohort of applicants who were seeking access to very similar document types.'

Table 2: Charges – notified and collected 2016-17 to 2019-20

Period	Number of requests notified	Amount notified	% change from previous	Amount collected	% change from previous
2019-20	716	$267,069	-25%	$88,090	-28%
2018-19	822	$357,039	-7%	$122,774	+6%
2017-18	1,029	$383,531	-24%	$115,863	-21%
2016-17	1,317	$505,394	+1%	$147,043	—

Practical refusals

- Agencies and ministers sent 71% more notices of an intention to refuse an FOI request for a practical refusal reason in 2019–20 than in 2018–19 (3,803 in 2019–20, compared with 2,225 in 2018–19). The reason for this increase was a substantial increase in the number of practical refusal notices issued by the Department of Home Affairs (which issued 792 notices in 2018–19 and 2,713 in 2019–20). The Department of Home Affairs issued practical refusal notices for 15.45% of all the FOI requests it received during 2019–20. In 2017–18, 4,128 notices were issued (86% more than in 2018–19).

s 47E(d) [redacted]

Exemptions

- The personal privacy exemption (s 47F) remains the most claimed exemption. It was applied in 38% of all FOI requests in which exemptions were claimed in 2019–20; the same percentage as in 2018–19. The use of s 47F has declined over the past two years – it comprised 43% of the exemptions applied in 2017–18.
- The next most claimed exemptions were s 47E (certain operations of agencies), s 37 (documents affecting enforcement of law and protection of public safety), s 47C (deliberative processes), and s 38 (documents to which secrecy provisions apply). This is similar to previous years.
- There was a 7% increase in amendment applications in 2019–20, with seven agencies receiving 717 amendment applications (no applications were received by ministers). In 2018–19, 673 applications were received.
- See Com brief - Trends in use of exemptions in FOI Act D2020/017449.

Disclosure logs

Australian Government agencies reported publishing 1,949 new entries in disclosure logs during 2019–20; including documents available for download directly from the agency or minister's website in relation to 1,468 requests, documents available from another

website in relation to 56 requests, and 425 entries in which the documents are available by another means (usually upon request). This is approximately **62% higher than 2018–19, when 1,200 entries were added**Costs

- The total cost attributable to processing FOI requests was $63.91 million, almost 7% more than 2018-19, when the total cost was $59.85 million. The reason for the increase in the overall cost of FOI activity is a 6% increase in the total staff hours devoted to FOI in 2019–20.
- General legal advice costs ($719,718) decreased 53% compared with 2018–19 ($1,517,125). Litigation costs ($911,551) increased approximately 120% from 2018–19 ($414,635). General administrative costs ($136,634) decreased approximately 5% from 2018–19 ($144,140). Training expenses ($168,339) decreased 56% over 2018–19 ($385,745). 'Other' non-labour costs ($242,585) decreased 8% from 2018–19 ($263,206).
- The average cost per FOI request determined (granted in full, in part or refused) was $1,546 in 2019–20 (a fraction of a percentage more than in 2018–19).

Possible questions

- ***How has the COVID-19 pandemic affected access to government documents through FOI?***

  While some agencies have attributed increases in the number of FOI requests received during 2019–20 to the impact of the COVID-19 pandemic, the increase in total FOI requests (2,454 more than in 2019–20) is the direct result of a substantial increase in FOI requests made to Services Australia (2,672 more requests than in 2018–19).

  The COVID-19 pandemic affected the ability of some Australian Government agencies to respond to FOI requests within the statutory timeframes in the FOI Act. In some agencies, FOI staff were redeployed to work in frontline customer service roles while the internal redeployment of other staff to meet service delivery needs made it difficult to obtain documents to satisfy FOI requests and to engage with decision makers, many of whom assumed additional responsibilities as part of their agency's response to the pandemic. Interagency consultation was more difficult, particularly with agencies heavily involved in delivering Australia's response to the pandemic.

  For agencies with staff working remotely, some aspects of FOI processing was more difficult, for example, manipulating large files and using redaction software can be slower on domestic internet servers. In some cases the necessary IT infrastructure was not in place to allow staff to work from home, resulting in delays that affected productivity. Posting and receiving hard copy documents, particularly for staff living in locations subject to movement restrictions was difficult. For some agencies, the impact of COVID-19 was more significant because they were in the early stages of integrating functions following machinery of government changes that came into effect on 1 February 2020.

  Because of the issues outlined above, some agencies and ministers found it difficult to meet the statutory timeframes in the FOI Act. This resulted in a significant increase in

the number of applications from agencies and ministers to extend the time to process FOI requests.

- ***What action is the OAIC proposing to take to address poor compliance with statutory timeframes?***

  The OAIC continues to monitor agency compliance with statutory timeframes and we are working directly with some agencies to address this issue. Work undertaken by my office in promoting compliance with statutory timeframes includes:

  - making decisions extension of time applications
  - using our formal powers to require provision of a statement of reasons when a person seeks review of a deemed refusal
  - investigating complaints about delay
  - providing assistance through our enquiries phone line
  - publishing regular e-newsletters for FOI practitioners
  - publishing resources on our website, including checklists to streamline the FOI request process.

- ***Many agencies do not make documents available for direct download from their disclosure logs; they provide contact details only. What is the OAIC doing to address this?***

  The FOI Guidelines [14.32] say that publishing documents directly on the disclosure log, rather than describing the documents and how they can be obtained on request, is consistent with the FOI Act object of facilitating public access to government information. We are reviewing the Guidelines to place more emphasis on direct publication, with reference to *the Explanatory Memorandum to the Freedom of Information Amendment (Reform) Bill 2009* which provides that information is to be published on a website and a description and contact details, only if the information cannot readily be published in that way.

  In October 2019, the OAIC commenced a desktop review of agency compliance with disclosure log obligations. The review assessed 38 Australian Government agencies, including departments. s 47E(d) [redacted]

  We anticipate the desktop review will be published shortly.

- ***Some agencies received significant increases in the number of FOI requests last year; what assistance does the OAIC provide to support agencies discharge their functions and powers under the FOI Act?***

  The OAIC publishes a range of resources to assist agencies discharge their functions and powers under the FOI Act. These include:

- agency resources, FAQs and the FOI Guidelines
- regular e-newsletters for FOI practitioners which provide practical guidance and processing tips
- the publication of IC review decisions provides guidance to agencies in the use of FOI Act provisions and the OAIC holds twice yearly information sessions for FOI practitioners (although our ability to do this has been impacted by COVID-19 restrictions)
- the OAIC also operates an enquiry line that agencies can call for advice and guidance.

- ***Why don't more agencies make documents available to the public without requiring an FOI request to be made?***

  The OAIC's Corporate Plan identifies proactive disclosure of government held information, including the establishment of administrative access schemes, as a key focus for the coming year. We have suggested these items be included in the next Open Government National Action Plan and we promote these through our Information Contact Officers Network e-newsletters and information sessions.

Key dates (mandatory section / heading – not to be removed)

- N/A

Document history

Updated by	Reason	Approved by	Date
Nikki Edwards	Senate Estimates October 2020	Raewyn Harlock	29.9.2020

Commissioner brief: Trends in use of FOI Act exemptions[1]

D2020/017449

Key messages

- The percentage of cases in which no exemptions were claimed has varied over the past 9 years[2]:
    - In 2011-12, no exemptions claimed in **58%** of all FOI requests decided (12,844 requests)
    - In 2012-13, no exemptions claimed in **44%** of all FOI requests decided (9,766 requests)
    - In 2013-14, no exemptions claimed in **49%** of all FOI requests decided (11,255 requests)
    - In 2014–15, no exemptions claimed in **19%** of all requests decided (5,747 requests)
    - In 2015-16, no exemptions claimed in **18%** of all FOI requests decided (5,954 requests)
    - In 2016-17, no exemptions claimed in **19%** of all FOI requests decided (6,554 requests)
    - In 2017-18, no exemptions claimed in **23%** of all FOI requests decided (7,312 requests)
    - In 2018-19, no exemptions claimed in **22%** of all FOI requests decided (6,718 requests)
    - In 2019–20, no exemptions claimed in **64%** of all requests decided (18,823 requests).
- The type of exemptions applied are generally consistent from year-to-year.
- The most commonly claimed exemption is the personal privacy conditional exemption (s 47F).
    - In 2019–20, it was applied in approximately **38%** of all requests in which an exemption was applied.
- The use of the certain operations of agencies conditional exemption (s 47E) has increased over the past nine years:
    - 2011-12 - approximately **8%** of all requests in which an exemption was applied
    - 2019-20 - approximately **20%** of all requests in which an exemption was applied.
- The exemptions applied by agencies may change on review.

1 All percentages have been rounded to whole numbers in this brief.
2 As reported by agencies

Critical facts

- 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 which are included in the OAIC's annual report. This information includes the number of FOI requests and amendment applications received and the outcomes, charges collected during the year, the number of internal reviews etc. Agencies enter their FOI statistics into an online portal each quarter. The statistics in this brief are based on the data reported by agencies and ministers.
- The percentage of requests granted in full has gradually declined since 2011–12.
    - In 2011–12**, 59%** of all requests were **granted in full**, 29% were granted in part and approximately 12% were refused.[3]
    - In 2014–15, approximately **57%** of all requests were **granted in full**, 33% were granted in part and approximately 10% were refused.
    - In 2018-19, approximately **52%** of all requests were **granted in full**, 35% were granted in part and approximately 13% were refused.
    - In 2019–20, approximately **47%** of all requests were **granted in full**, 38% were granted in part and approximately 15% were refused.
- Table – Top 5 exemptions (and their percentages) in 2019-20 (in order):

Exemption	**Percentage of matters in which exemption applied**
Personal privacy (s 47F)	38%
Certain operations of agencies (s 47E)	20%
Documents affecting enforcement of law and protection of public safety (s 37)	10%
Deliberative processes (s 47C)	8%
Secrecy provisions of enactments (s 38)	7%

- The personal privacy conditional exemption (s 47F) of the FOI Act has been the most used exemption every year since 2011–12:

[3] These figures are taken from the 2011–12 annual report, which says that no exemptions were applied in 57.8% of all requests decided. The annual report also says that in 36.1% of all requests decided exemptions were applied. This leaves 6.1% of all requests unaccounted for.

  - In 2011–12 - applied in **48%** of all FOI requests in which exemptions were applied
  - In 2015–16 – applied in **48%** of all FOI requests in which exemptions were applied
  - In 2019-20 – applied in **38%** of all FOI requests in which exemptions were applied.
- The use of the certain operations of agencies conditional exemption in s 47E has increased since 2011–12:
  - In 2011-12 – applied in **8%** of all FOI requests in which exemptions were applied (the 3rd most used exemption behind ss 47F and 37)
  - In 2014-15 – applied in **14%** of all FOI requests in which exemptions were applied (2nd most used)
  - In 2019-20 – applied in **21%** of all FOI requests in which exemptions were applied (2nd most used).
- The documents affecting enforcement of law and protection of public safety exemption (s 37) has decreased, however it remains one of the most used exemptions:
  - In 2011–12 – applied in **12%** of all exemptions in which exemptions were applied (2nd most used)
  - In 2014–15 – applied in **12%** of all FOI requests in which exemptions were applied (3rd most used)
  - In 2019–20 – applied in **10%** of all FOI requests in which exemptions were applied (3rd]).
- The secrecy exemption (s 38) was applied:
  - In 2011-12 – applied in **6%** of all FOI requests in which exemptions were applied (the 4th most used)
  - In 2014–15 - applied in **5%** of all FOI requests in which exemptions were applied
  - In 2018–19 – applied in **7%** of all FOI requests in which exemptions were applied
  - In 2019–2020 – applied in **7%** of all FOI requests in which exemptions were applied (5th most used).
- The **deliberative processes** conditional exemption (**s 47C)** was applied:
  - In 2011-12 – applied in **4%** of all FOI requests in which an exemption was applied (the 6th most used)
  - In 2014–15 – applied in **5%** of all FOI requests in which an exemption was applied (5th most used)
  - In 2019–20 – applied in **8%** of all FOI requests in which an exemption was applied (4th most used).

- The documents affecting national security, defence or international relations exemption (s 33):
    - In 2011–12 – applied in 2% of all FOI requests in which exemptions were applied XXXX (10th most used)
    - In 2014-15 – applied in 5% of all FOI requests in which exemptions were applied (6thmost used)
    - In 2019-20 – applied in 4% of all FOI requests in which exemptions were applied (6th most used).
- The least used exemptions, consistent from year-to-year, are:
    - ss 45A (Parliamentary budget office documents)
    - 47A (electoral rolls)
    - 47H (research)
    - 47J (the economy) – each of which comprise less than 0.2% of all exemptions applied.

Possible questions

- ***Why is personal privacy the most used exemption when 81% of all requests are for personal information?***

  Agencies and ministers report to the OAIC whether FOI requests are for 'predominantly personal' or 'other' information. A request for access to the personal information of another person is categorised as a 'predominantly personal' FOI request. As a result, it is not correct to say that 81% of all requests are for a person's own personal information, although a large number are.

  The Australian Government holds a large amount of personal information. Personal privacy is taken very seriously. While giving a person access to their own personal information is a public interest factor that strongly favours access to documents, any negative impacts on the personal privacy of other individuals is a factor that the FOI Guidelines specify favours non-disclosure.

  The FOI Act recognises the significant impacts that disclosing personal information can have on individuals and requires agencies and ministers to consult affected third parties before making a decision on access if it appears to the agency or minister that the affected third party might reasonably wish to make a contention that a document is conditionally exempt under s 47F and that giving access to the document would, on balance, be contrary to the public interest for the purposes of s 11A(5) of the FOI Act.

  The FOI Act allows personal information to be removed from documents before being released and in many cases removal of a name or telephone number protects the privacy of a third party but allows the FOI applicant to access the substance of the requested document, consistent with the objects of the FOI Act.

While it is the most used exemption, use of the personal privacy conditional exemption has decreased over time. In 2019–20, it was applied in approximately 38% of all requests in which an exemption was applied (it was applied in approximately 48% of requests in 2011–12). This may reflect the increasing use of administrative access schemes to provide individuals with access to their own personal information.

- ***Has the use of s 47E (certain operations of agencies) increased?***

  The certain operations of agencies conditional exemption has four subsections:

  - prejudice the effectiveness of procedures or methods for the conduct of tests, examinations, or audits by an agency
  - prejudice the attainment of the objects of particular tests, examinations or audits conducted or to be conducted by an agency
  - substantial adverse effect on management of staff
  - substantial adverse effect on agency operations.

  Section 47E has a wide scope.

  The largest increase in the use of s 47E has been over the past five years. This may reflect the view of the Information Commissioner, as expressed in IC review decisions, that some of the impacts that disclosing the names and contact details of staff may have are more appropriately addressed under s 47E, rather than s 47F (personal privacy).

- ***What are your thoughts on the recommendation made by the Thodey review of the APS that material prepared to inform the deliberative processes of government should be exempt from release under the FOI Act?***

  The deliberative processes conditional exemption in s 47C of the FOI Act protects information which relates to the opinions, advice or recommendations obtained, prepared or recorded, or consultation or deliberations that have taken place for the deliberative processes of an agency or a minister or the government. It does not apply to 'purely factual material'. This exemption, which is subject to a public interest test, protects the ability of government officials to develop policy, debate issues, and to brief ministers and government where appropriate.

  The rights and interests of the Australian public could be significantly impacted if the deliberative processes of government are not subject to an overriding public interest test. The objects of the FOI Act, include that Australia's representative democracy is enhanced by increasing public participation in government processes with a view to promoting better informed decision making and increasing scrutiny, discussion, comment and review of the government's activities.

Key dates

- 1 November 2010 – the *Freedom of Information Amendment (Reform) Act 2010* came into effect. This resulted in some exemptions which were previously non conditional becoming subject to a public interest test (e.g., personal privacy).
- The data used in this brief has been sourced from the OAIC's FOI annual reports from 2011–12 to 2019–20.

Document history

Updated by	Reason	Approved by	Date
Nikki Edwards	Senate Estimates October 2020	Raewyn Harlock	29.9.2020

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:
    - 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.
- The OAIC requires agencies and ministers to provide supporting documentation during the consideration of an extension of time application. The application 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.
- In 2019–20, 79% of all FOI requests determined were processed within the applicable statutory time period:
    - 80% of all personal information requests and
    - 73% of non-personal requests.

  This represents a slight decrease in timeliness of decision-making from 2018–19 (when 83% were decided within time).
- In 2019–20, there was an increase in the number of FOI requests decided more than 90 days after the expiry of the statutory time period (including any applicable extension of time provisions) when compared with 2018–19 (10% in 2019–20, up from 2% in 2018–19).

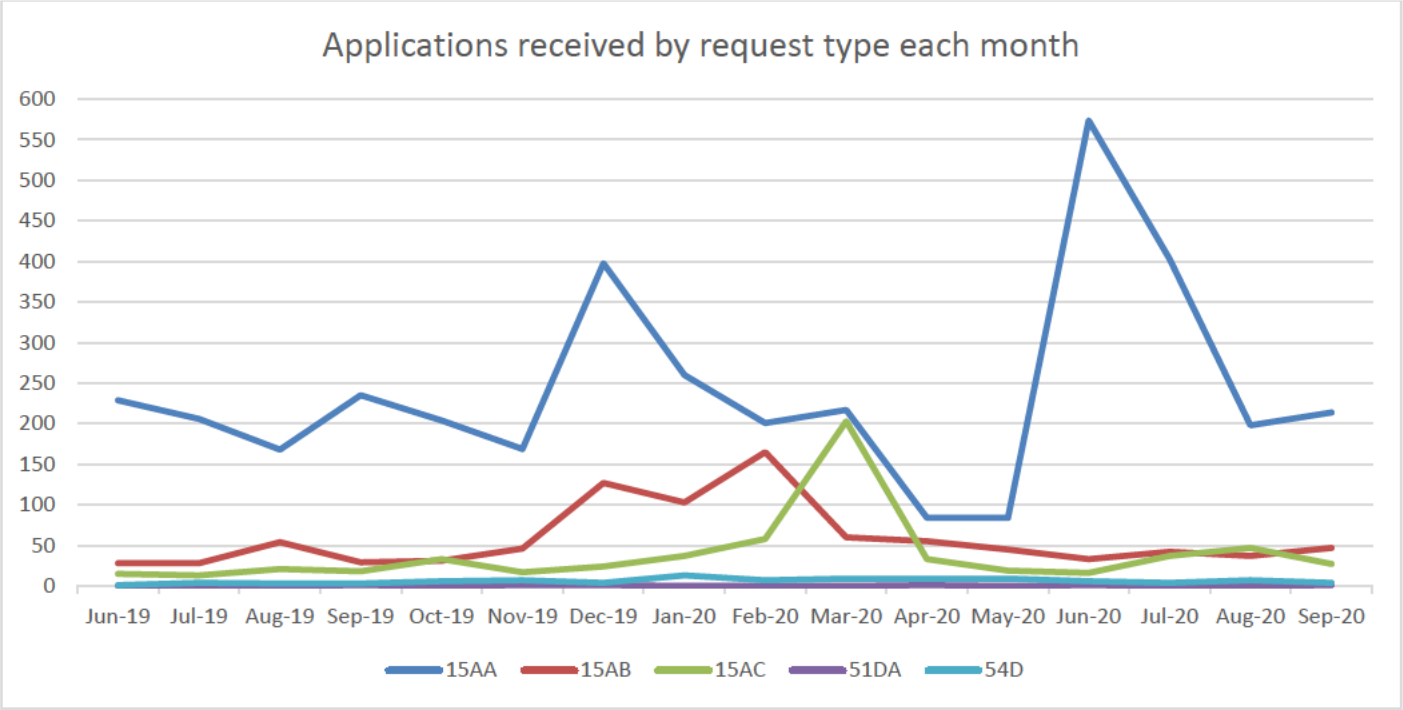
Critical facts

- In 2017-18, 2018-19 and 2019-20 the OAIC finalised:

Request Type	2017-18	2018-19	2019-20
Section 15AA (agreement between agency and applicant)	2,762	2,959	2,393 (-19%)
Section 15AB (extension based on complexity or voluminous)	370	562	786 (+48%)
Section 15AC (deemed access refusal decision made)	122	178	492 (+176%)
Section 51DA (extension to deal with an amendment or annotation request)	1	1	5 (+400%)
Section 54D (deemed affirmation of primary decision)	38	41	80 (+95%)
Total	**3,293**	**3,741**	**3,756**

EOT Applications received by request type

- The following graph sets out the number of extension of time applications received by the OAIC since June 2019.



- On 25 October 2019, the IC commenced an Information Commissioner Investigation into the Department of Home Affairs' compliance with the timeframes set out under the FOI Act for requests relating to non-personal information. The increase of EOT applications received may be a result of the announcement of this investigation.
- During January – March 2020, the OAIC received 655 applications for extension of time under ss 15AB, 15AC, 51DA and 54D of the FOI Act. This represented an increase of 352% in extension of time applications for the same period in January - March 2019. The increase in applications generally related to COVID-19, staffing affected by agency shutdown over the Christmas period, effects of the bushfires and s 47E(d) [redacted] information not publicly available). Please see **Attachment A**.
- During March to June 2020, many of the 1,889 extension of time requests made by agencies referred to COVID-19 related reasons why the agency has been unable to process the FOI request within the statutory processing period. Agencies referred to a reduction in staffing due to reassignment of FOI processing officers to other areas of the agency as the main reason for seeking the extension. Other reasons included a lack of available decision makers or subject matter experts to retrieve and advise of the documents within the scope of a FOI request.
- In June 2020, 574 notifications of an agreement to extend the processing period under s 15AA of the FOI Act was received by the OAIC. The Department of Home Affairs accounted for 397, Australian Taxation Office 57 and Services Australia 53.

Possible questions

- ***What was the effect of COVID on extension of time applications received by the OAIC?***

During the 1st quarter of 2020-2021, we have seen a significant reduction in the number of agencies applying for extensions of time with COVID being provided as a reason for seeking that extension.

In March 2020, the OAIC experienced a significant increase of extension of time applications and notifications (489 total). Between March and June 2020, the OAIC received 1,889 extension of time applications and notifications (ss 15AA, 15AB, 15AC, 51DA and 54D), that is an increase of 55% for the same period in 2019 (with 1,219 received in 2019).

- ***What action is the OAIC proposing to take to address poor compliance with statutory timeframes?*** The OAIC continues to monitor agency compliance with statutory timeframes and works directly with some agencies to address this issue. We are pleased to see overall improvements in timeliness since 2016-17 (where 58% of requests were processed within the statutory timeframe). For 2019-20 79% were processed within the statutory timeframe. Work undertaken by my office in promoting compliance with statutory timeframes includes:
    - making decisions extension of time applications
    - using our formal powers to require provision of a statement of reasons when a person seeks review of a deemed refusal
    - investigating complaints about delay
    - providing assistance through our enquiries phone line
    - publishing regular e-newsletters for FOI practitioners and
    - publishing resources on our website, including checklists to streamline the FOI request process.
- ***What information does the OAIC require from agencies and ministers prior to making an extension of time decision?*** The OAIC requires:
    - the name and contact details of the FOI applicant
    - the scope of the FOI request
    - the reasons for the delay
    - an explanation of why the statutory timeframe is not able to be met.

  Inadequate explanatory information to support the application for an extension may cause the application to be declined. Further information is set out on our website: see 'Extension of time provisions under the FOI Act'.[1]
- ***What factors does the OAIC take into consideration when considering an extension of time application?*** Factors considered include:
    - whether the FOI request is complex and/or voluminous

[1] https://www.oaic.gov.au/freedom-of-information/guidance-and-advice/extension-of-time-for-processing-requests/.

- the length of time that has been requested by the agency or minister
- whether other extension provisions have been applied
- whether adequate explanatory information has been provided to support the application for an extension
- what work has already been undertaken to process the FOI request, and
- what work will be undertaken if the extension of time is granted.

In some circumstances, the OAIC may consult with the FOI applicant. Any comments the FOI applicant makes will be taken into consideration.

- ***How long can the OAIC grant an extension of time for?*** The Information Commissioner may grant an extension of time for 30 days, or such other period as the delegate of the Information Commissioner considers appropriate. The time period requested by the agency or minister is based on the facts and circumstances of each application.
- ***Do you always grant an extension of time?*** No. Each application is considered on its merits. Applicants may be consulted for their comments on the application, and those comments will be considered by the decision maker.
- ***How many extensions of time applications were received from agencies and Ministers in the1st quarter of this financial year?***

  In the first quarter of this financial year the OAIC received 253 ss 15AB, 15AC, 51DA and 54D applications from agencies and Ministers. The OAIC was also notified by agencies and ministers of a further 815 s 15AA agreements.
- ***How many extensions of time applications were received from agencies and Ministers in the last financial year?***

  In the 2019-20 financial year the OAIC received 1353 ss 15AB, 15AC, 51DA and 54D applications from agencies and Ministers. The OAIC was also notified by agencies and ministers of a further 2,800 s 15AA agreements.
- ***How many extension of time applications does the OAIC grant?***

In the 1st quarter of FY2020-2021, the OAIC granted 82% of all extension of time applications received that require an Information Commissioner decision.

In 2019-20, the OAIC granted 69% of all extension of time applications received that require an Information Commissioner decision. The OAIC 'granted varied' 10% and refused 15%. Four percent of the applications received by the OAIC were subsequently withdrawn.

- ***Have you issued any guidance about what FOI applicants can do if they have not received a decision within time?***

  The OAIC has published information about an individual's review rights and the availability of Information Commissioner review where a decision has not been made

within time.[2] If an agency or minister doesn't make a decision on the FOI request within the required time, the FOI request is taken to have been refused. Any charge the agency or minister asked to pay is no longer due, and any deposit must be refunded. In these circumstances, the FOI applicant has the right to ask for Information Commissioner review of this decision (internal review does not apply to this kind of decision).

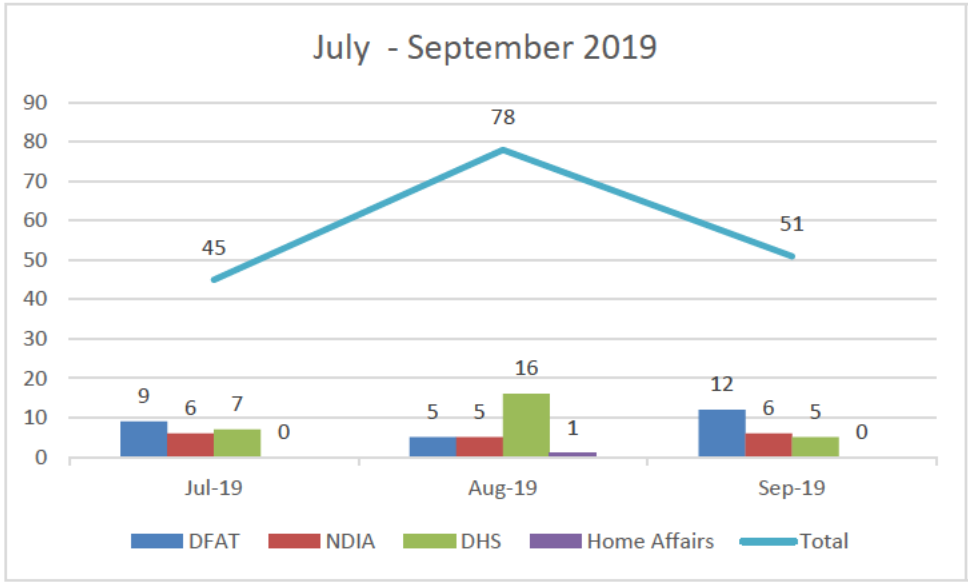
Document history

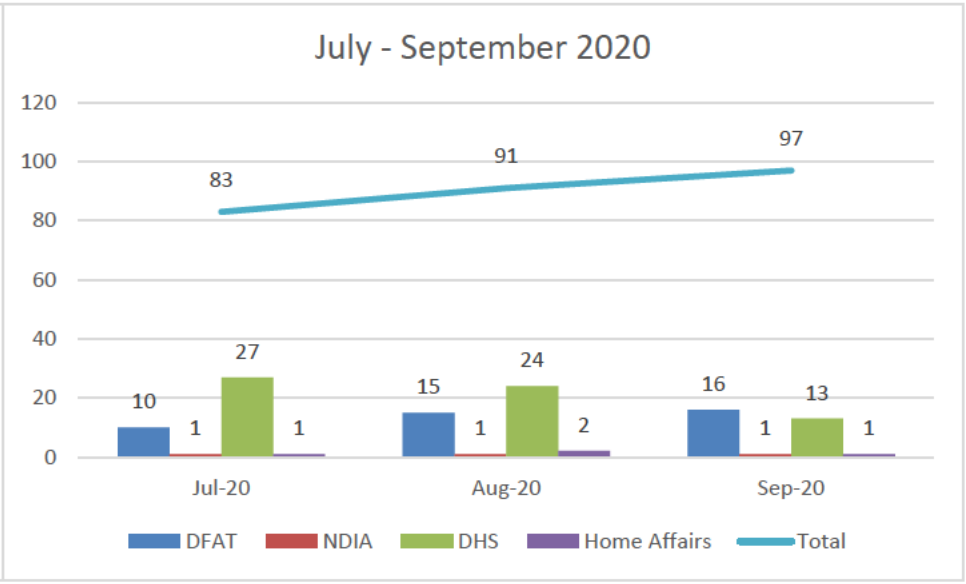
Written by	Reason	Approved by	Date
Shelley Napper	October 2020 Senate estimates	Angelene Falk	October 2020

[2] OAIC website: https://www.oaic.gov.au/freedom-of-information/how-to-make-an-foi-request/when-to-expect-a-decision/ and https://www.oaic.gov.au/freedom-of-information/reviews-andcomplaints/information-commissioner-review/.

Extension of time application received under ss 15AB, 15AC, 51DA and 54D

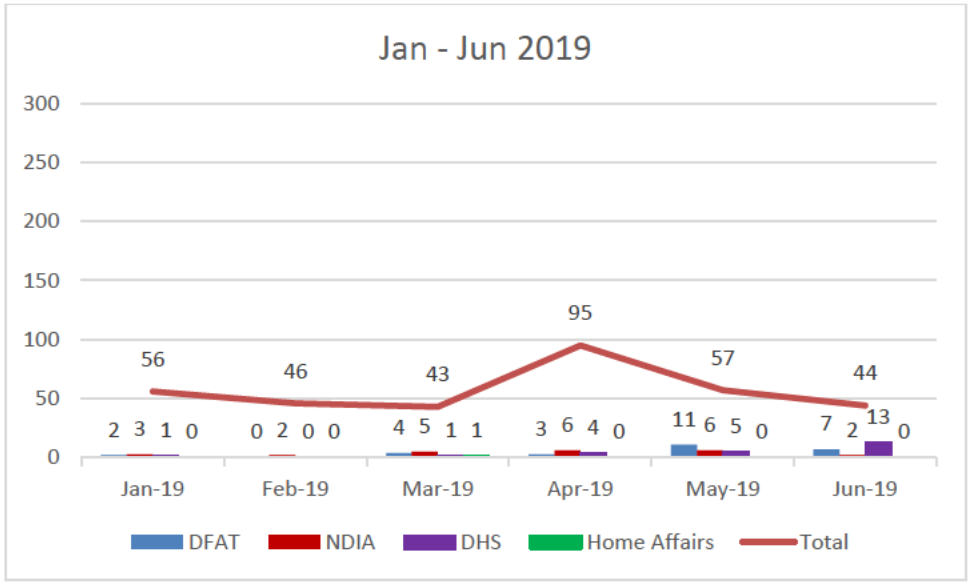
During the 1st quarter of this financial year, the OAIC received an increase of 56% in extension of time applications for the same period in July - September 2019.[3]

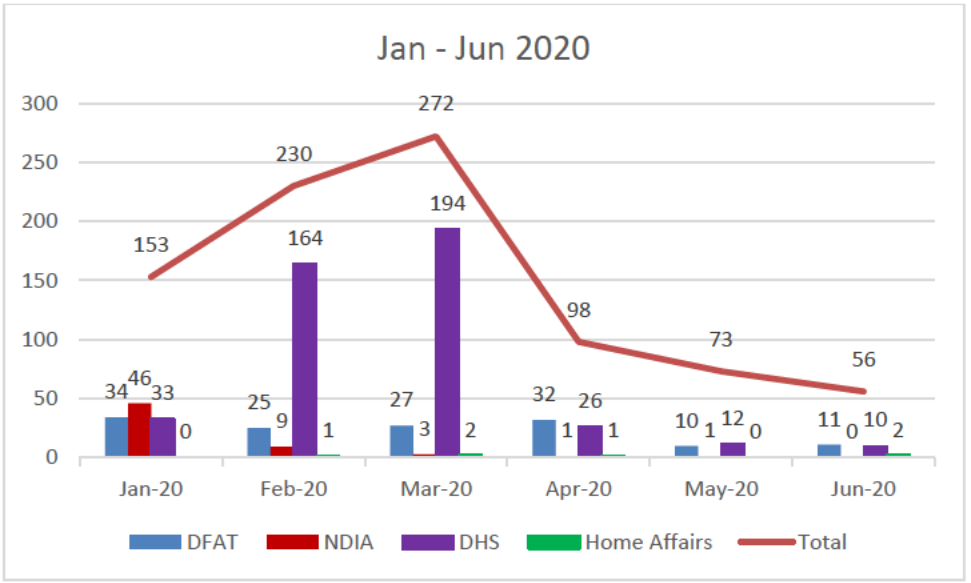




During January – June 2020, the OAIC received an increase of 159% in extension of time applications for the same period in January - June 2019.

3 Statistics taken from Resolve report accessed on 8 October 2020.


Jan - Jun 2019
300
250
200
150
100
50
0
56
46
43
95
57
44
2 3 1 0
0 2 0 0
4 5 1 1
3 6 4 0
11 6 5 0
7 2 13 0
Jan-19
Feb-19
Mar-19
Apr-19
May-19
Jun-19
DFAT
NDIA
DHS
Home Affairs
Total


Jan - Jun 2020
300
250
200
150
100
50
0
153
230
272
98
73
56
34 46 33 0
25 9 164 1
27 3 194 2
32 1 26 1
10 1 12 0
11 0 10 2
Jan-20
Feb-20
Mar-20
Apr-20
May-20
Jun-20
DFAT
NDIA
DHS
Home Affairs
Total

Commissioner brief: FOI Complaint issues

Key messages

- 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
    - poor communication/failure to update
    - failure of decision maker to provide name
    - poor record keeping (leading to an inability to find requested documents)
    - the Information Publication Scheme
    - deletion of public servants' personal information from documents before release.
- I am of the view that making a complaint is not an appropriate mechanism where IC review is available, unless there is a special reason to undertake an investigation and the matter can be dealt with more appropriately and effectively as a complaint. IC review will ordinarily be the more appropriate avenue for a person to seek review of the merits of an FOI decision, particularly an access refusal or access grant decision.
- The OAIC will soon publish a summary of the de-identified outcomes of finalised FOI investigations on the OAIC website.

Statistics

Period	Number received	Number finalised	Finalisation timeframe	S 86 notices – with and without recommendations

2019-20	**109** (increase of 79% on previous year)	**71** (increase 223% on previous year)	48% > 12 months 52% <12 months	46 issued: • 27 with recommendations • 19 without recommendations
2018-19	**61** (decrease of 2% on previous year)	**22** (decrease of 24% on previous year)	18% > 12 months 82% <12 months	Nil s 86 issued
2017-18	62 (72% increase on previous year)	29 (61% increase on previous year)	17% > 12 months 83% <12 months	5 issued: • 4 with recommendations • 1 without recommendation

- Number of complaints on hand at 30 September 2020: 136
- Percentage of complaints on hand are more than 12 months old: 47%
- For an overview of the status of finalised FOI complaints please see **Attachment A** to this brief.

Possible questions

- ***Your evidence is that delay is the most complained about issue. What action is the OAIC taking to address this?***

  The OAIC oversees the extension of time provisions in the FOI Act which provides valuable insight into the issues that affect agencies' ability to comply with decision making timeframes. The OAIC is currently reviewing its guidance material to focus on the need for agencies to take action early in the processing cycle and to routinely engage with applicants when processing FOI requests. The OAIC is currently monitoring agencies' compliance with statutory decision making timeframes.

- ***What department or agency is the most complained about and what kinds of complaints are people making?***

s 47E(d)

[redacted]

s 47E(d) [redacted]

- ***What recommendations have you made to improve FOI processing within agencies?***

  I have made a number of recommendations for agencies 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.

- ***Are agencies implementing your recommendations?***

  Yes. Agencies have not raised any objections and have taken steps to implement my recommendations.

- ***What happens if agencies do not implement your recommendations?***

  Under s 89 of the FOI Act I have the discretion to issue a notice of implementation requiring an agency to provide particulars of steps the agency has taken to implement a recommendation. Where an agency does not comply with the implementation notice I can provide a report to the responsible minister.

Document history

Updated by	Reason	Approved by	Date
Irene Nicolaou	Estimates October 2020	Angelene Falk	October 2020

Attachment A – Summary of outcomes of FOI investigations

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Respondent	Issues	Type of FOI request	Date of Notice on completion	Outcome	Recommendations	Respondent's response received	Status
s 47E(d)							

Commissioner brief: FOI Disclosure Logs D2020/017452

Key messages

- In October 2019, the OAIC began work on a desktop review of agency compliance with disclosure log obligations. A key focus of the review is whether agencies make documents directly available for download to members of the public.
- Our report is near finalisation and will be published soon.

Critical facts

- Section 11C of the FOI Act requires agencies to publish information released in response to FOI requests within 10 days of release to the FOI applicant, unless the documents contain personal or business information that it would be unreasonable to publish. Subsection 11C(3) provides three options for publication:
  1. directly on the agency's website
  2. linking to another website from which the information can be downloaded
  3. publishing details of how the information can be obtained on the agency's website.
- The FOI Guidelines state that publication of documents directly on an agency's website, rather than describing the documents and how they can be obtained on request, is consistent with the FOI Act object of facilitating access to government information. Further, the Explanatory Memorandum to the *Freedom of Information Amendment (Reform) Bill 2009* states that information is to be published to the public generally on a website, and it is only if the information cannot readily be published in that way that the website should give details of how the information can be obtained.
- In December 2018 and January 2019 an individual made FOI requests through the 'Right to Know' website to 12 Departments that do not make documents directly available through their disclosure logs, but which instead require an email to be sent requesting access. The individual sought access to all documents not directly available for download. Many Departments treated this as a formal request for access when a decision had already been made on access, imposed with charges and applied a 30-day processing period (in one case the agency asked for a 30-day extension to process the 'request'). Several Departments issued practical refusal notices.
- This issue was brought to our attention via social media and the 'Right to Know' website.
- The OAIC's desktop audit assessed all Australian Government departments (those subject to the FOI Act), as well as the 20 agencies that receive the largest number of FOI requests for non-personal information that result in release of documents.
- The desktop review assessed:
  - the form in which access is provided (directly on the website, linked to another website or on request)

  - the adequacy of the description of the documents
  - how documents are removed and archived on their disclosure log.
- While the report based on the desktop review is currently being finalised, the review found that most agencies are largely compliant with their disclosure log obligations. The report identifies the following issues:
  - almost 40% of reviewed agencies require members of the public to contact them for access to documents on their disclosure log. This places an unnecessary barrier to accessing government information.
  - all reviewed agencies include some information identifying the subject matter or content of documents on their disclosure logs. However, descriptions vary in the amount of detail provided which can make it difficult for members of the public to identify what the documents contain and whether to seek access.
  - almost 70% of the reviewed agencies do not publish a timeframe for the removal of documents from their disclosure log making it difficult for members of the public to know how long documents will remain on a disclosure log.
- The review will recommend that agencies work towards making documents available for download directly from their website, improving the description of documents on their disclosure log and provide clearer details about when documents will be removed from their active disclosure log.
- A report detailing the findings of the review is near finalisation and should be published soon.

Possible questions

- ***If the OAIC was aware of non-compliance with disclosure log obligations in January 2018, why is it only now that action is being taken?***

  The OAIC has a number of regulatory functions and we need to ensure we are able to discharge all of these functions in an efficient and cost-effective way. During the last financial year (2019-20) the OAIC assigned specific resources to undertake the review, as well as working on other projects that promote proactive publication of information by Australian Government agencies.

- ***What agencies are the worst offenders?***

s 47E(d) [redacted]

  The report is near finalisation and will be published soon. The report will identify trends in agency disclosure log compliance but will not identify individual agencies.

- ***What action will you take in relation to agencies who are non-compliant with their statutory obligations?***

  The OAIC will publish a report that includes trends and outcomes. We are using the information obtained during the review to update Part 14 of the FOI Guidelines

(Disclosure Log) to provide more guidance to agencies which will enable them to better meet their disclosure log obligations (for more information see Commissioner Brief - Changes to Disclosure Log Guidelines D2020/017619). We will take regulatory action if required. Further, we will work directly with agencies to ensure more government held information is made available to the Australian public.

Key dates

- December 2018/January 2019 – 12 FOI requests made to Australian Government Departments for access to documents not directly available for download from agency disclosure logs.
- October 2019 to December 2019 – desktop review conducted.

Document history

Updated by	Reason	Approved by	Date
Nikki Edwards	Senate Estimates October 2020	Raewyn Harlock	20.9.2020

Commissioner brief: Changes to Disclosure Log Guidelines D2020/017619

Key messages

- The OAIC is in the process of updating Part 14 of the FOI Guidelines (Disclosure Log).
- In October 2019, the OAIC began work on a desktop review of agency compliance with disclosure log obligations. Our report is near finalisation and will be published soon. (For more information see Commissioner brief: FOI Disclosure Logs D2020/017452).
- We are using the information obtained during the disclosure log review to inform our update of Part 14 of the FOI Guidelines (Disclosure Log) to provide more guidance to agencies to enable them to better meet their disclosure log obligations, as well as to improve readability and update cross references to supporting material.

Critical Issues

- The desktop review of agency compliance with disclosure log obligations found that almost 40% of reviewed agencies require members of the public to contact them for access to documents on their disclosure log. This places an unnecessary barrier to accessing government information.
- In the updated Guidelines, we will emphasise the Explanatory Memorandum to the Freedom of Information Amendment (Reform) Bill 2009, which states that it is only if 'information cannot readily be published on a website' that 'the website should give details of how the information may be obtained'.
- The revised Guidelines will note the Information Commissioner's view that documents should be made directly available for download from an agency's website (see ss 11C(3)(a) and 11C(3)(b) of the FOI Act) unless it is not possible to upload documents, for example, due to file size, the requirement for specialist software to view the information, or for any other reason of this nature. This approach is consistent with the objects of the FOI Act.
- Previously the Guidelines suggested that it may be appropriate that information attached to a disclosure log listing is removed after 12 months unless the information has enduring public value. The revised Guidelines will suggest that it may be appropriate to retain information and documents on the disclosure log for a longer period of at least three years.
- We will also update the section on Facilitating Access to emphasise that agencies and ministers are encouraged to release information on the disclosure log as a machine readable or searchable PDF, or in HTML format to ensure readability and accessibility of information.

Possible questions

- ***Will you seek input from the community or agencies on content for the revised Part 14?***

  My office will publish a draft version of Part 14 of the FOI Guidelines for public consultation. We will consider the consultation responses and further revise the draft, as appropriate, before it is issued.

- ***When will a new version of Part 14 be ready for publication?***

  I anticipate Part 14 will be ready for publication before the end of the year.

Key dates

- October 2019 to December 2019 – desktop review conducted.

Document history

Updated by	Reason	Approved by	Date
Nikki Edwards	October 2020 Senate Estimates	Raewyn Harlock	29.9.2020

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.
- 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.

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 (see **Attachment A**).
- The APSC made a detailed submission after consulting agencies on a draft. The majority of agencies who made submissions expressed

support for the APSC's position. (The APSC submission is at **Attachment B**.)

- Many agency submissions highlighted work health and safety concerns with disclosure of public servants' names and contact details, in the context of a digital environment where members of the public can publish this information online. Examples of harassment and abuse were provided, some of which were not the result of disclosure in response to an FOI request.
- Other submissions include:
  - it is not reasonable to disclose the names and contact details of APS staff below SES level and this does not further the objects of the FOI Act
  - disclosure can impact on agency operations because members of the public to circumvent existing contact channels (e.g., enquiry lines).
  - more guidance is needed about what 'special circumstances' will make disclosure unreasonable when considering the personal privacy exemption in s 47F.
- Three agencies said they include public servants' names and contact details when releasing documents in response to FOI requests and this has not caused any work health and safety issues for them.
- Generally, members of the public support greater disclosure of government held information, including public servants' personal information.
- The OAIC published a position paper on 20 August 2020 that recognises the need to balance the changes resulting from the development of the online environment with accountability and safety of public servants in the context of disclosures required by the FOI Act (see **Attachment C**).
- The paper identified the following principles that will inform updates to Parts 3 and 6 of the FOI Guidelines:
  - Public servants are accountable for their decisions, their advice and their actions. Agencies and ministers must ensure this is made clear in staff induction programs and ongoing training.
  - Agencies and ministers should start from the position that including the full names of staff in documents released in response to FOI requests increases transparency and accountability and is consistent with the objects of the FOI Act.

- Agencies and ministers who have not identified work health and safety risks associated with disclosure of staff names and contact details should generally continue to provide full access to this information on request.
- Agencies and ministers who have identified work health and safety risks associated with disclosing staff names and contact details can consider asking the FOI applicant whether they seek access to this information.
- In general, it will only be appropriate to delete public servants' names and contact details as irrelevant under s 22 of the FOI Act if the FOI applicant states, clearly and explicitly, that they do not require this information.
- If disclosure of names and contact information poses a risk to the health and safety of staff – because of the nature of the work performed or because of the nature of the client base – agencies and ministers may consider whether the conditional exemption in s 47E(c) applies.
- The OAIC is currently in the process of updating Parts 3 and 6 of the FOI Guidelines to reflect this position. Agencies and members of the public will soon have an opportunity to provide comment on draft versions of these parts before they are finalised and issued under section 93A of the FOI Act.

Possible questions

- ***Do you support the view of the APSC that there is a distinction between SES and APS staff?***

  The conditional exemption in s 47E(c) of the FOI Act is applicable when disclosure of a document would have a substantial adverse effect on the management of staff. For a document to be exempt from disclosure under this provision, it must also be contrary to the public interest to disclose it.

  In assessing whether disclosure will have a substantial adverse effect on the health and safety of their staff, whether the name and contact details of the public servant are already publicly available, including Senior Executive Service details available on the Government Online Directory, will be a relevant factor.

- ***It is apparent from agency submissions that disclosure of public servants' names and contact details is an issue with wider***

significance for the public sector than simply FOI requests. Have you discussed this issue with the Australian Public Service Commissioner?

I have engaged with the Australian Public Service Commissioner in relation to the issues arising from the consultation.

Key dates

- **1 July 2019** – discussion paper published
- **26 July 2019** – original closure date for submissions
- **9 August 2019** – extended closure date
- **20 August 2019** – date last submission received
- **16 September 2019** – submissions published on OAIC website
- **20 August 2020** – position paper published on OAIC website

Document history

Updated by	Reason	Approved by	Date
Nikki Edwards	Senate Estimates October 2020	Raewyn Harlock	17.9.2020

Attachment A

Disclosure of public servants' names and contact details

Discussion paper

July 2019

Summary

The Office of the Australian Information Commissioner (OAIC) is aware of agency concerns about the disclosure of public servants' names and contact details in the context of FOI requests, both in response to FOI requests and when requests are being processed.

The purpose of this discussion paper is twofold; firstly to provide greater awareness of the relevant guidance and decisions regarding the disclosure of public servants' names and contact details, including the circumstances in which public servants' names and contact details may be released or published in response to an FOI request and when they may be exempt from disclosure. Secondly, this discussion paper also seeks to explore agency concerns and practices in relation to this issue.

It is not the intention of this discussion paper to explore the legal requirements for the name and designation of a decision maker to be stated in a notice of decision (ss 26(1)(b) and 29(9)) or the name and contact details in a request consultation notice (s 24AB(2)(c) and (d)).

Rather, this paper focusses on the circumstances in which public servants' names and contact details are included in the documents at issue, and the FOI Act provisions that agencies have relied on to withhold this information from disclosure — namely ss 22 (relevance), 47E(c) (substantial adverse effect on the management or assessment of personnel), 47E(d) (substantial adverse effect on agency operations) and 47F (personal privacy).

In seeking to further explore this issue, we invite you to comment on your experience as an FOI practitioner, or as someone who has sought access to information from an Australian Government agency or minister. To assist you to do this, at the end of this paper we have posed a series of questions to explore the issues and have provided information about how you can submit your comments.

The information gathered as part of this consultation will be used to consider whether the FOI Guidelines provide sufficient and appropriate guidance for agencies and ministers in relation to the disclosure of the names and contact details of public servants in the current information access landscape.

Background

Public servants' names and contact details may be in a wide range of documents generated and held by Australian government agencies. Usually this is because the public servant was involved, to some degree or extent, with the work which is the subject of the documents.[1]

It has long been considered that in general, disclosure of public servants' names in response to an FOI request would not be unreasonable. Such disclosure forms part of the system of accountability and transparency of government actions and decision making.

Freedom of Information Memorandum No. 94 (dated June 1994)[2] states:

> 12 … It was not Parliament's intention to provide anonymity for public officials each time one of them is mentioned in a file. That would be contrary to the stated aims of the FOI Act and would not assist in promoting openness or accountability.

Further, in relation to consultation, Memorandum No. 94 states [emphasis added]:

> 21. One major example of circumstances which would be relevant [to the need to consult under s 27A] is where the name of an official appears in a document in the normal course of the official's duties. *There is no personal privacy interest in that information, and there is no need to consult with officials in such circumstances.* The situation would be different, however, where the information related to something in which there may be some real privacy concern, such as work performance information concerning an individual official, or information relating to alleged disciplinary offences or sexual harassment. Other information relating to an official may be entirely private in nature, such as information relating to the official's entitlement to bereavement leave because of the death of a close relative…

The OAIC's view, as expressed in the FOI Guidelines, is that it would not be unreasonable to disclose public servants' personal information unless special circumstances exist:

> 6.153 Where public servants' personal information is included in a document because of their usual duties or responsibilities, it would not be unreasonable to disclose unless special circumstances existed. This is because the information would reveal only that the public servant was performing their public duties. Such information may often also be publicly available, such as on an agency website.

The FOI Guidelines recognise that in some circumstances disclosure of public servants' personal information, including their names, may be unreasonable:

> 6.154 When considering whether it would be unreasonable to disclose the names of public servants, there is no basis under the FOI Act for agencies to start from the position that the classification level of a departmental officer determines whether his or her name would be unreasonable to disclose. *In seeking to claim the exemption an agency needs to identify the special circumstances which exist rather than start from the assumption that such information is exempt.* [Emphasis added]

[1] Part 6.157 of the FOI Guidelines distinguishes between this kind of personal information and personal information that *does not* relate to the public servant's usual duties and responsibilities. For example, if a document contains information about an individual's disposition or private characteristics, such as the reasons a public servant has applied for personal leave, information about their performance management or whether they were unsuccessful in a recruitment process. This kind of personal information is not the subject of this issues paper.

[2] Freedom of Information Memorandums were issued by the Attorney-General's Department and provided guidance to Australian government agencies in exercising powers and discharging functions under the FOI Act.

6.155 In *Maurice Blackburn Lawyers and Department of Immigration and Border Protection* [2015] AICmr 85, where the agency raised the concern that disclosure would affect the personal safety of its officers, the Information Commissioner said that there is no apparent logical basis for distinguishing between the disclosure of SES officers and other officers' names, particularly where the purported concern is that disclosure could affect personal safety.

6.156 A document may, however be exempt for another reason, for example, where disclosure would, or could reasonably be expected to, endanger the life or physical safety of any person (s 37(1)(c)). In addition, where an individual has a propensity to pursue matters obsessively and there is no need for them to contact a particular public servant in the future, disclosure of the public servant's name may be unreasonable.

Decisions: Commonwealth and other jurisdictions

There have been various decisions made by the Administrative Appeals Tribunal (AAT) and former and current Information, FOI and Privacy Commissioners regarding the disclosure of the names and contact details of public servants. These decisions discuss the relevant legislative tests and the submissions provided by agencies to demonstrate why such information should exempt. In cases where agencies have claimed that names and contact details are conditionally exempt, this requires first, consideration as to whether the relevant exemption has been made out, and second, whether disclosure would be contrary to the public interest.

In the context of Information Commissioner (IC) reviews, s 55D of the FOI Act provides that the agency or Minister bears the onus of establishing that an FOI decision is justified or that the Information Commissioner should give a decision adverse to the IC review applicant. When making an IC review decision, the Information Commissioner relies on agencies making submissions[3] and providing evidence to establish that special circumstances exist (such that it would be unreasonable to disclose public servants' personal information), or that disclosure would have a substantial adverse effect on the proper and efficient conduct of agency operations or on the management or assessment of personnel by the Commonwealth or by an agency, and that disclosure would be contrary to the public interest.

The table at **Attachment A** to this paper highlights the approach taken by the AAT and the Information Commissioners when considering whether it would be unreasonable to disclose public servants' personal information.

The table at **Attachment B** summarises decisions from other relevant jurisdictions regarding the disclosure of public servants' names. Although caution is required when considering cases from other jurisdictions, the principles articulated are consistent with the approach adopted by the OAIC despite these legislative differences.

Consultation Questions

The OAIC seeks comment on the issues raised in this paper.

Please provide examples of the situations or circumstances you describe in your submissions. To assist you frame your response, you may wish to consider the following questions.

[3] See Part 10 of the FOI Guidelines and 'Direction as to certain procedures to be followed in IC reviews'.

For agencies:

1. Does your agency have concerns about releasing the names and contact details of staff in response to FOI requests? If so, what are your concerns? Has your agency experienced any specific work health and safety issues as a result of a person's name or contact details being released in response to an FOI request?

2. Have your agency's views on this issue changed over time? If so, please describe any factors that have affected your agency's approach, including technological, environmental or legal factors.

3. Does your agency advise staff, including contractors undertaking functions on behalf of the agency, that names and contact details may be released in response to an FOI request as part of your agency's training and induction programs?

4. How do you balance work health and safety considerations with the objects of the FOI Act, which include increasing public participation in Government processes with a view to promoting better-informed decision making and increasing scrutiny, discussion, comment and review of the Government's activities?

5. If your agency considers that disclosure of a public servant's name or contact details will negatively impact their health or safety, what evidence do you require before deciding that their name or contact details are exempt from disclosure?

6. Do you consider the FOI Guidelines provide enough guidance for agencies when considering these issues?

7. In what circumstances do you consider that a public servant's personal information (name and contact details) are irrelevant to the FOI request?

8. Where you have withheld the names and contact details of public servants, what impact does deleting this information from documents have on the time it takes to process FOI requests?

For members of the public:

9. As a person who has requested access to documents from an Australian Government agency, have you been denied access to the names of agency staff? Did you consider this decision was justified? If no, why not?

10. What are your views on deletion of the names of public servants and their contact details before documents are released in response to an FOI request? What are the reasons for your view?

How to provide comments

Submissions can be made by:

Email	foidr@oaic.gov.au
Post	GPO Box 5218 Sydney NSW 2001

The closing date for comments is Friday 26 July 2019.

The OAIC intends to make all submissions publicly available. Please indicate when making your submission if it contains confidential information you do not want made public and the reasons why it should not be published. Requests for access to confidential comments will be determined in accordance with the FOI Act.

Although you may lodge submissions electronically or by post, electronic lodgement is preferred. To help the OAIC meet its accessibility obligations, we would appreciate you providing your submission in a web accessible format or alternatively, in a format that will allow the OAIC to easily convert it to HTML code, for example Rich Text Format (.rtf) or Microsoft Word (.doc or .docx) format.

Privacy collection statement

The OAIC will only use the personal information it collects during this consultation for the purpose of considering the issues associated with the disclosure of public servants' names and contact details in response to an FOI request.

Decisions: Commonwealth jurisdiction

Administrative Appeals Tribunal

Decision	Case	Key messages
Unreasonable to disclose any personal information of Departmental staff but not unreasonable to disclose names of staff (but not contact details) of staff engaged by the Commissioner for Complaints (Section 41(1))[4]	*Bartucciotto and Commissioner for Complaints* [2006] AATA 36 (17 January 2006) [19]–[27]	▪ The relevant personal information relates exclusively to public servants in the context of their performance of their public duties. As a general rule, disclosure of such personal information will not be unreasonable. ▪ There was evidence before the Tribunal that the applicant had engaged in intimidating and aggressive behaviour, both by telephone and in person, against staff of the Department of Health and Ageing and had made threats against officers. In these circumstances disclosure of any personal information would be unreasonable. ▪ However in relation to staff employed by the Commissioner of Complaints, while there was evidence that the applicant had communicated aggressively by telephone and in letters on numerous occasions, there was no evidence of any threatening or intimidating behaviour towards particular officers. Further, there was no evidence that any officer specifically objected to their personal information being disclosed to the applicant. As a result, the Tribunal considered it would not be unreasonable to disclose the names of officers contained in the relevant documents, but that it would be unreasonable to disclose contact details — namely, email addresses, direct work telephone and fax number.
Not unreasonable to disclose names of public servants who attended meetings as contained in the Attorney-General's diary (Section 47F)	*Dreyfus and Attorney-General (Commonwealth of Australia) Freedom of information) [2015] AATA 995 (22 December 2015) (Justice Jagot)* [50]	▪ There is no basis upon which the personal privacy exemption can apply insofar as the names of public servants are disclosed as having attended meetings with the Attorney-General.

[4] Section 41 of the FOI Act is the equivalent provision to s 47F in the current FOI Act.

Decision	Case	Key messages
Not unreasonable to disclose messages to which FOI applicant is a party Disclosing internal investigation reports would have a substantial adverse impact on the management of personnel (Sections 47E(c) and 4F)	*De Tarle and Australian Securities and Investments Commission (Freedom of information)* [2016] AATA 230 (8 April 2016) [24]–[26], [42]	▪ There can be no proper claim under s 47F where the applicant is a party to the communication; even when documents include derogatory comments about others, information about performance reviews and supervision, or personal information unrelated to the individual's duties as a public servant (personal email addresses, mobile numbers, feelings and health issues). ▪ Candour is essential when an agency investigates complaints, especially those of bullying and harassment. Staff may be reluctant to provide information and cooperate with investigators if the subject matter of those discussions is disclosed and made public.
Not unreasonable to disclose names of people interviewed as part of criminal investigation (Section 47F)	*Leigh and Australian Federal Police (Freedom of information)* [2016] AATA 330 (20 May 2016) [40]–[55]	▪ Although in the circumstances of this matter it would not be unreasonable to disclose the names of people interviewed as part of a criminal investigation, because this information appears in the documents because of their usual duties and responsibilities, it will not the case that it will never be unreasonable to disclose this information. ▪ The relevant report was more than 12 years old and related to events that occurred 17 months before its creation. The level of detriment following disclosure would be low or non-existent. which mitigated against finding that disclosure
Contrary to the public interest to disclose email addresses, surnames, signatures (Section 47F)	*Price and Attorney General's Department (Freedom of information)* [2016] AATA 1044 (20 December 2016) [37]–[45]	▪ Disclosing the surnames, signatures, email addresses and user IDs of officers, other than particular executive officers would be contrary to the public interest. ▪ The potential for harm was a real given the nature of agency's role (harassment from complainants and other inappropriate contact).
Not unreasonable to disclose names (Section 47F)	*Lever and Australian Federal Police (Freedom of information)* [2017] AATA 1407 (22 August 2017) [53]–[56]	▪ The exempt material identifies staff on duty at Australia's Nuclear Science and Technology Organisation on a particular day. ▪ The Respondent submits that the zeal with which the applicant pursued his application indicates he may press these staff for more information. ▪ The Tribunal was not satisfied the Respondent had established that the applicant has a tendency to pursue matters obsessively, or that there is no need for him to contact the relevant persons in the future. The factual background to the FOI request was not relevant to the issues for

Decision	Case	Key messages
		determination in this review and although the Tribunal accepted the applicant had pursued his application with unusual vigour, whether this amounted being obsessive depends on underlying facts not within the scope of the review. Similarly, whether there was any need for him to contact relevant staff depends on the same questions, as well as his intentions as to other litigation, which would be speculative to consider on the evidence before the Tribunal. ▪ The fact that the applicant sought to call the named individuals to give evidence was not relevant to the decision whether the documents were exempt (see s 11(2) of the FOI Act).

Australian Information Commissioner

Decision	Case	Key messages
Unreasonable to disclose unsubstantiated allegations (Section 47F)	*Besser and Attorney-General's Department* [2013] AICmr 12 (25 February 2013) [25] and [30]	▪ Disclosing the names and personal details of AFP officers against whom unsubstantiated allegations were made would involve a serious and significant invasion of their privacy and cause unnecessary harm and detriment to them and their families.
Not unreasonable to disclose outcome of Code of Conduct investigation Unreasonable to disclose information not related to officer's usual functions (Section 47F)	*'AF' and Department of Immigration and Citizenship* [2013] AICmr 54 (26 April 2013) [54]–[56]	▪ It would not be unreasonable to disclose personal information relating to the sanction imposed following an internal investigation because this demonstrates that allegations are taken seriously, that the agency does not tolerate behaviour that is inconsistent with the APS Code of Conduct and that the appropriate sanction was imposed. ▪ Disclosing a statement that the officer changed their name on a specific date would be unreasonable because it is unrelated to their usual duties and responsibilities.
Not unreasonable to disclose names where applicant is aware of them (Section 47F)	*'AH' and Australian Federal Police* [2013] AICmr 59 (6 June 2013) [21]	▪ When the applicant is aware of the identity of the officers investigated and the nature of the sanction imposed, it will not be unreasonable to disclose information about when and how those officers were notified of the sanction and what further action was considered.

Decision	Case	Key messages
		▪ In terms of public interest, disclosure demonstrates the agency takes allegations seriously and does not tolerate behaviour inconsistent with the Code of Conduct.
Unreasonable to disclose information which might identify individual under investigation Personal information can be edited from documents for publication on disclosure log (Section 47F)	*Besser and Department of Families, Housing, Community Services and Indigenous Affairs* [2013] AICmr 65 (21 August 2013) [31] and [33]–[34]	▪ If disclosing dates would identify an individual under investigation it would be unreasonable to release this information (for example, commencement date or periods of absence from work would likely be sufficient for one of their co-workers to identify them). ▪ A person's signature can be edited from the document before being published on the agency's disclosure log
Unreasonable to disclose date and place of birth, mobile telephone number (Section 47F)	*Hunt and Australian Federal Police* [2013] AICmr 66 (23 August 2013) [72]–[74]	▪ It is not unreasonable to release personal information such as names, work email addresses, positions or titles, work contact details and decisions or opinions because this information appears in documents because of the person's usual duties or responsibilities. ▪ It would be unreasonable to release personal details such as dates and places of birth and personal mobile telephone numbers.
Unreasonable to disclose names of officers interviewed during investigation (Section 47F)	*'AO' and Department of Veterans' Affairs* [2013] AICmr 77 (21 October 2013) [63]	▪ When information is given confidentially by public servants during an internal investigation it would be unreasonable to disclose their identity or any record of their statements.

Decision	Case	Key messages
May be unreasonable to disclose mobile phone numbers Not unreasonable to disclose mobile phone numbers if included in work signature block (Section 47)	*Thomson and Australian Federal Police* [2013] AICmr 83 (22 November 2013) [13]	▪ Work mobile phone numbers can be personal information. ▪ It would not be unreasonable to disclose a mobile phone number if included in an email signature and sent outside the organisation, where the phone number has been included in a document because of the employee's usual duties or responsibilities. ▪ Agencies need to carefully consider their policies and practices when including mobile phone numbers in email signatures for external emails.
Not unreasonable to disclose names when applicant aware of them No substantial adverse effect on agency operations (Sections 47E(d) and 47F)	*Rudd and Civil Aviation Safety Authority* [2013] AICmr 87 (11 December 2013) [24] and [34]	▪ It would not be unreasonable to disclose the names of public servants against whom the applicant has complained. ▪ Information about other employees only reveals they are performing their public duties. ▪ It will not be unreasonable to disclose an investigator's findings because these provide only a general summary of issues and recommendations for future action and does not disclose any personal information.
Unreasonable to disclose recruitment information (Section 47F)	'*BA' and Merit Protection Commissioner* [2014] AICmr 9 (30 January 2014) [92]–[93] and [95]	▪ Even if documents contain positive information about an individual which is unlikely to embarrass them, recruitment information is highly personal because it shows how the individual performed at interview and their rating. ▪ It will be unreasonable to disclose a person's job application and submissions. These documents contain distinctly personal information about the individual's career and their perceived strengths. The documents were also prepared for a specific purpose, with a particular audience in mind, and with the expectation they would be treated confidentially.
No substantial adverse effect on agency operations established (Section 47E(d))	*'BB' and Department of Human Services* [2014] AICmr 11 (6 February 2014) [15]–[27]	▪ Clause in Enterprise Agreement which says the Department will 'work toward ensuring' that employees have a choice about whether to provide their full name or only a first name in response to public enquiries does not unconditionally assure staff that their identity will be protected. ▪ Clause in Enterprise Agreement does not permit staff to deal with members of the public anonymously.

Decision	Case	Key messages
		▪ No evidence that disclosure of names in response to an FOI request would divert contact on a scale that is substantial and adverse.
Not unreasonable to disclose names, signatures and investigator identification numbers (Section 47F)	*Stephen Waller and Department of Environment* [2014] AICmr 133 (25 November 2014) [50]–[52]	▪ The Departmental officers identified in the documents are acting in their professional capacity as public servants. None of the information in the document relates to the individuals in their private capacity. ▪ The Departmental officers are known by the occupier, but not by the applicant or the third party, to have been associated with the matters dealt with in the documents
Substantial adverse impact on management of staff to disclose details of complainants Not unreasonable to disclose staff signatures and initials Unreasonable to disclose names of individuals subject to internal investigation (Sections 47E(C) and 47F)	'*HJ' and Australian Federal Police [2015] AICmr 71* (6 November 2015) [20]–[22], [31]–[34] and [38]–[40]	▪ Exempting all staff signatures and initials would require the Information Commissioner to find that being employed by an agency is a 'special circumstance'. ▪ Disclosure would be unreasonable where a named individual is associated with the subject matter of the documents (completed investigations).
Not unreasonable to disclose names of staff at all levels (Section 47F)	*Maurice Blackburn Lawyers and Department of Immigration and Border Protection* [2015] AICmr 85 (18 December 2015) [3], [14]–[17], [21] and [25]–[27]	▪ Agencies should not start from the position that an officer's classification will determine whether it would be unreasonable to disclose their name. ▪ Whether the applicant intends disseminating the names of departmental officers may be a relevant consideration in deciding that disclosure would be unreasonable. ▪ Increasing scrutiny, discussion, comment and review of the government's activities are some of the stated objects of the FOI Act which need to be balanced with disclosure of public servants' personal information.
Unreasonable to disclose names of departmental officers (Section 47F)	*Australian Associated Press Pty Ltd and Department of Immigration and Border Protection* [2016] AICmr 25 (22 April 2016) [50]–[53]	▪ Where public servants have been appointed to investigate and report on the conduct of other officers, with potentially significant consequences for the personnel concerned, it is unreasonable to release their names. ▪ Facts in this case distinguished from Maurice Blackburn Lawyers and Department of Immigration and Border Protection [2015] AICmr 85, where

Decision	Case	Key messages
		disclosure would reveal only that the departmental officers were carrying their usual duties or responsibilities.
Not unreasonable to disclose signature (Section 47F)	*'JN' and Commonwealth Ombudsman* [2016] AICmr 62 (19 September 2016) [36]–[38]	▪ The Ombudsman did not present any special circumstances justifying the exemption of the signature, beyond the individual acting in their official capacity as an officer of the AFP.
No special circumstances - disclosure of names and titles not unreasonable No substantial adverse impact on agency operations established (Sections 47E(d) and 47F)	*John Mullen and Australian Aged Care Quality Agency (Freedom of information)* [2017] AICmr 11 (1 February 2017) [27]–[29] and [35]–[37]	▪ The Tribunal was not satisfied that the nature and extent of previous contact between the applicant with Agency staff amounted to special circumstances that would make disclosure of officers' names and titles unreasonable (two telephone conversations, two missed calls on a staff member's work mobile telephone and one voicemail message requesting a hard copy of the redacted documents). ▪ Disclosure of names and titles would not be unreasonable. ▪ Merely asserting that disclosure would have a substantial adverse impact on agency operations is not sufficient to discharge an agency's onus under s 55 of the FOI Act. Evidence is needed to establish that the centralised complaints management process would be affected by the applicant directly contacting staff. This was especially so because the evidence was that many of the relevant staff no longer worked for the Agency.
Substantial adverse impact on operation of media section not established Not unreasonable to disclose names of staff working in media operations section Unreasonable to disclose names of former staff members (Sections 47E(d) and 47F)	*The Australian and Department of Immigration and Border Protection (Freedom of information)* [2017] AICmr 62 (27 June 2017) [16] and [24]–[28]	▪ The Department did not provide particulars of how the predicted adverse effects could reasonably be expected to occur on a scale that would or could have a substantial adverse effect on the proper and efficient operations of its media operations section. ▪ Although Department provided examples relating to the personal safety of staff, the Information Commissioner was not satisfied this established that disclosure would, or could reasonably be expected to, result in staff in the *media operations section* being exposed to online stalking or harassment, or would affect their personal safety.

Decision	Case	Key messages
Not unreasonable to disclose names and contact details Section 47F	*'MA' and Department of Veterans' Affairs (Freedom of information)* [2017] AICmr 72 (26 July 2017) [105]–[112]	▪ Names and contact information of staff included in documents due to their usual duties and responsibilities. ▪ The applicant was a party to the correspondence and the details would already be known to them.
Unreasonable to disclose name (Section 47F)	*Julian Knight and Attorney-General's Department (Freedom of information)* [2017] AICmr 79 (31 August 2017) [26]–[31]	▪ Disclosing the name of non-Executive officer unreasonable because of reasonable expectation that this could subject officer to harassment from complainants and other inappropriate contact.
Substantial adverse impact on agency operations not established (Section 47E(d))	*Maria Jockel and Department of Immigration and Border Protection (Freedom of information)* [2017] AICmr 101 (9 October 2017) [20]–[21]	▪ The Department did not discharge its onus to establish that it would be unreasonable to disclose the names of current staff in an organisational chart. ▪ It was not established that disclosure of contact details to one migration agent could reasonably be expected to occur on a scale that would or could have a substantial adverse effect on the proper and efficient operations of the Department. ▪ Further, contact details had previously been made available to the applicant as part of the Department's stakeholder engagement.
Not unreasonable to disclose name and signature (Section 47F)	*'PF' and Department of Human Services (Freedom of information)* [2018] AICmr 59 (11 July 2018) [43]–[47]	▪ The Department did not establish special circumstances. In particular, the Department did not explain why disclosure would be unreasonable when the applicant was to be given access to the remainder of the document through a qualified person and the officer had met the applicant during the course of their duties as a departmental officer. ▪ The Department had already given the applicant access to the signatures of other public servants in other documents and did not explain why a different approach had been taken to the signature at issue.
No substantial adverse impact on agency operations Not unreasonable to disclose opinions of public servants (Sections 47E(d) and 47F)	*Reece Walters and Great Barrier Reef Marine Park Authority (Freedom of information)* [2019] AICmr 9 (1 March 2019) [105]–[106], [109] and [124]–[125]	▪ Not established that disclosure of names would, or could reasonably be expected to, have a substantial adverse effect on the proper and efficient conduct of the operations of the agency. ▪ Where comments are made, or opinions expressed, as a result of public servants discharging their usual duties or responsibilities, it will not be unreasonable to disclose those comments/opinions.

Decision	Case	Key messages
Irrelevance Section 22	*'FM' and Department of Foreign Affairs and Trade* [2015] AICmr 31 (24 April 2015) [14]–[15]	▪ There is no logical basis for treating the names of SES officials as being within the scope of a request, but the names of other officials as being irrelevant.
Irrelevance Section 22	*'PO' and Australian Federal Police (Freedom of information)* [2018] AICmr 72 (19 December 2018) [16]–[17]	▪ Whether the names and contact details of public servants will be irrelevant to the request and able to be deleted under s 22 requires consideration of the scope of the request. When an applicant specifically seeks documents pertaining to a particular officer it is unlikely that the name of that officer can be irrelevant to the request.

Decisions: Other jurisdictions

Note: Please note that other jurisdictions operate under different legislative schemes and the relevant legislative tests may differ from those in the Commonwealth jurisdiction.

Decision	Case	Key messages
Not reasonable to disclose names when physical safety of individual at risk	*Re 'M' and WA Country Health Service – South West* [2012] WAICmr 8 Decision of Information Commissioner (Western Australia)	▪ Where fears for safety are reasonably based and established by evidence disclosure of public servants' names and other identifying details will be unreasonable.
Unreasonable to disclose signatures, initials and contact telephone numbers	*Mond v Department of Justice (General)* [2005] VCAT 2817 (22 December 2005) [45]–[52]	▪ It would not be reasonable to disclose the signatures, hand-written initials or contact telephone numbers of CAV [Consumer Affairs Victoria] officers. ▪ Disclosure under the FOI Act is disclosure to the world and it is possible that signatures may be misused and telephone numbers used to approach officers who are not usually available to speak to members of the public. The applicant seeks access to substantive information, not personal details of officers. ▪ In the circumstances, it would be unreasonable to disclose signatures, initials or telephone numbers.
Unreasonable to disclose name and signature of junior officer	*Roy Costa Planning & Development v Mildura CC (Review and Regulation)* [2014] VCAT 1360 (25 September 2014) [41]	▪ It would be unreasonable in circumstances where the applicant said they did not seek access to the name and signature of a junior rank officer to disclose this information.

Decision	Case	Key messages
Unreasonable to disclose name and signature	*Coulson v Department of Premier and Cabinet (Review and Regulation)* [2018] VCAT 229 (20 February 2018) [110]–[119]	▪ Those circumstances involve litigation against two former Premiers by a former Ministerial Adviser. ▪ It would be unreasonable to disclose the names, initials, signatures and email addresses of non-executive Victorian Public Service officers' and subject them potential public criticism in circumstances where they were implementing directions for which they were not the decision-makers and cannot respond publicly to any personal attacks in relation to those directions. ▪ If names disclosed, this would have the potential to inhibit the candour and frankness of the advice provided and the willingness of officers to perform directions where they may personally face public criticism.
Not unreasonable to disclose routine personal work information	*Australian Broadcasting Corporation and Psychologists Board of Australia* (3 January 2012) Decision of Assistant Information Commissioner (Queensland)	▪ Routine personal work information can be distinguished from other personal information. ▪ The potential harm from disclosing routine personal work information is in most circumstances minimal or non-existent because public service officers are employed in the business of government to deliver services to the public. The public is generally entitled to know the identity of service deliverers, advice givers and decision makers. ▪ A reasonable public service officer would expect that information which is solely their routine personal work information will be made available to the public.
Names of junior public servants	*Dun v Information Commissioner and National Audit Office* (UK) (18 January 2011) EA/2010/0060	▪ There is no blanket level at which all junior public servants' names will be exempt from disclosure. This needs to be decided on a case by case basis, through consideration of the role and responsibilities of the individual and the information itself.
Names of junior public servants	*Freedom of Information Act 2000 Decision Notice – Information Commissioner's Office* (UK) (6 February 2012) FS50401773	▪ Evidence was provided that in the past correspondence from Home Office officials had been published on the internet which led to officials being targeted. The Commissioner accepted that the nature of the information could lead to individuals being targeted and the distress this would cause was a factor which made disclosure of the names of junior home office officials unfair.

Decision	Case	Key messages
Public servants' names	*Joe McGonagle v Information Commissioner and Ministry of Defence* (UK) (4 November 2011)	▪ It will not be unreasonable to disclose the names of officials who speak to the media or who represent the Department at outside functions.
Names of senior staff in relevant authority	*Freedom of Information Act 2000 Decision Notice – Information Commissioner's Office* (UK) 16 June 2009 (FS50125350)	▪ Decision to disclose the names of senior staff. ▪ The Information Commissioner was satisfied there was a legitimate public interest in knowing who was responsible for important decisions involving significant sums of public money.
Not unreasonable to disclose names of public servants	*Ombudsman's opinion under the Official Information Act* Opinion of New Zealand Ombudsman Ref: 320402 (14 December 2012) [4]–[21]	▪ The Ombudsman did not accept an argument that 'less senior' staff without decision making responsibility have privacy interests that need protecting. ▪ 'The names of officials should, in principle, be made available when requested. All such information normally discloses is the fact of an individual's employment and what they are doing in that role. Anonymity may be justified if a real likelihood of harm can be identified but it is normally reserved for special circumstances such as where safety concerns arise.'