Draft Senate Estimates opening statement – 3 March 2020

Thank you for the opportunity to make some opening remarks – I would like to briefly touch on:

- work my Office has being doing in resolving privacy complaints from members of the community
- how the Notifiable Data Breaches scheme is driving awareness of personal information security requirements and what to do after a breach
- our progress towards implementing the Consumer Data Right
- and our work to uphold and promote information access rights.

The Committee would be aware that in recent years there has been a significant increase in the volume of privacy complaints being made to my Office.

This reflects a heightened awareness of personal information issues in the community, as well as the increasing use of personal data as an input to business and government service delivery.

From 2015 to 2019, the number of incoming privacy complaints rose by 55 per cent.

Over this period, we sought to manage this increased workload through a range of strategies, including a greater focus on early resolution of matters.

However, while we did increase our throughput year on year, where matters could not be resolved through early resolution, the wait for allocation to an investigations officer had increased to more than 12 months.

This financial year we have been in a position to apply additional resources to this area and I'm pleased to report that our staff have made significant inroads into the backlog of cases, and we are continuing to reduce our average processing times. From July to December 2019, we closed 364 more privacy complaints than we received. This is the first time our closure rate has exceeded the rate of incoming complaints since the 2012-13 financial year.

We've focused on three key areas to achieve these results:

- streamlining processes and resetting timeframes for parties in managing incoming complaints, as part of our early resolution approach
- setting up specialist teams to target and conciliate older and more complex complaints

- establishing a new determinations team to progress matters to a Commissioner decision, where conciliation could not be achieved within the first eight weeks.

In the first three months of this project, from November to January, we closed more than 900 complaints, an increase of almost 50 per cent on the same time the previous year.

This included reducing the backlog of complaints awaiting an Early Resolution attempt down from more than 300 to zero.

A greater number of matters are also being resolved through conciliation — rising by 60% in the first half of the financial year compared to the previous year's results.

The improvements identified through these focused efforts are now being embedded in our BAU processes and will continue to help us manage privacy complaints in an effective and timely way.

In the Freedom of Information area, you would be aware that applications to my Office to review agencies' FOI decisions have also been on the rise — increasing 82 per cent in the four years to June 2019, as I noted in my last appearance before the Committee.

In the first half of the financial year we have seen this trend ease slightly, with 464 IC review applications received — 11 per cent less than the same period the previous year, but still a notable increase compared to previous years.

More than half the matters that have come to us over this period are classified as complex.

That means they may involve sensitive material, affect the rights and interests of affected third parties, or raise numerous exemptions.

We currently have almost 1,000 IC reviews under consideration, and of the IC reviews finalised, the average time taken is around 8 months.

We are continuing to increase the rate at which we finalise IC reviews — closing 13 per cent more reviews in the first half of the financial year than in the same timeframe the previous year. However, this is not keeping pace with the continuing rise in incoming work.

We continue to work to make our processes as efficient as possible within existing resources.

That includes attempting to resolve matters informally, for example, by:

- identifying matters that can be resolved early through agreement or negotiation

- providing agencies with the opportunity to make revised decisions

and by using the OAIC's regulatory powers under the FOI Act.

We continue to encourage agencies to deal with requests in a timely manner in order to meet their obligations under the FOI Act.

If an extension of time is needed, agencies should be seeking agreement from the FOI applicant first, applying early in the process, and providing evidence to my Office as to why it is necessary.

We would also like to see agencies analyse their FOI requests to identify areas where more information can be released proactively, to make the system work more efficiently for all involved.

Turning to other areas of focus, we are working towards the start date of July 2020 for the Consumer Data Right to commence in the banking sector.

Our primary role as co-regulators with the ACCC will be to regulate the privacy aspects of the scheme and handle consumer complaints from individuals and small businesses.

We recently published guidelines to help industry understand their obligations under the CDR Privacy Safeguards.

We are also establishing a new system for receiving and triaging all complaint and reports submitted under the CDR regime, to facilitate coordination of complaint and enforcement action by both regulators.

In relation to the Notifiable Data Breaches Scheme, I can also report to the Committee that we recently released a statistical report, covering the period from July to December 2019.

537 notifiable data breaches were reported, a 19 per cent increase in the number reported to the OAIC in the previous six months, providing accountability and transparency in the handling and protection of personal information.

Some key areas drawn out in the report include the risks associated with storing sensitive personal information in email accounts where it may be accessed when account credentials are compromised.

Generally, the trends remain consistent with previous reporting periods, with malicious or criminal attacks, including cyber-attacks, the cause of 64 per cent of all data breaches, and human error accounting for 32 per cent, with the remainder due to system faults.

Health and finance remain the top reporting sectors under the scheme, and so we are continuing to target these sectors for increased awareness and action on preventing and containing data breaches.

The NDB scheme is a key reform in recent times to improve accountability and transparency in the areas we regulate.

As we approach the tenth anniversary of the establishment of the OAIC, we are also preparing for changes to and a review of the Privacy Act.

Our work to support the review of the Privacy Act and reforms, and our ongoing focus to conciliate, investigate, review and determine issues raised with us by the community, reflect the commitment across the agency to increasing public trust and confidence in the areas we regulate.

Thank you, that concludes my opening remarks.

December 2019

PRIVACY – Complaints
(excluding 1783 DIBP matters)

	NOW	-3	-6	-9	-12
	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
ON HAND – at the end of the quarter	**1096**	1359	1451	1,431	1,394
ALLOCATION TIME (months) (not finalised through early resolution process)	**15.6**	12.6	10.8	9.1	9.0
AWAITING ALLOCATION (not finalised through early resolution process because not appropriate for the early resolution team due to complexity, or where early resolution has been ineffective)	**371**	340	316	371	408
RECEIVED – per quarter	**700**	771	759	817	785
Percentage changed compared to prior quarter	***-9%***	*+2%*	*-8%*	*+4%*	*-16%*
RESOLVED – per quarter	**965**	870	729	779	672
Percentage changed compared to prior quarter	***+11%***	*+19%*	*-6%*	*+16%*	*-9%*
AVERAGE TIME TO COMPLETE YTD (months)	**4.5**	5.3	4.4	4.2	4.2
Percentage changed compared to prior quarter	***-15%***	*+20%*	*+5%*	*0%*	*+14%*
Total received Q2 1 October – 31 December 2019	**700**	*763*			
Percentage changed compared to prior year (Oct – Dec 2018)	*-11%*	*-19%*			
Total completed Q2 1 October – 31 December 2019	**965**	870			
Percentage changed compared to prior year (Oct – Dec 2018)	*+43%*	*+18%*			
Total received 2019-20 YTD (Jul – Dec)	**1471**		3,305		
Percentage changed compared to prior year (Jul – Dec 2018)	*-15%*		*+13%*		
Total completed 2019-20 YTD (Jul-Dec)	**1835**		2,920		
Percentage changed compared to prior year (Jul – Dec 2018)	*+30%*		*+6%*		

KPI = 80% closed within 12 months:
As at 31 December 2019, 89% of privacy complaints have been closed within 12 months.

	NOW	-3	-6	-9	-12
PRIVACY - NDBs					
	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
ON HAND – at the end of the quarter *(includes secondary notifications)*	**350**	237	139	137	111
ALLOCATION TIME (months)	**4.2**	1.7	1.4	1	
AWAITING ALLOCATION		67		79	
RECEIVED – per quarter					
Percentage changed compared to prior quarter	**291** *+18%*	*246* *-0.4%*	*245* *+13%*	216 *-18%*	262 *+ 7%*
RESOLVED – per quarter					
Percentage changed compared to prior quarter	**171** *+14%*	150 *-36%*	*234* *+23%*	190 *-32%*	280 *+ 35%*
AVERAGE TIME TO COMPLETE YTD (months)					
Percentage changed compared to prior quarter	**2.1** *+5%*	*2* *+33%*	*1.5* *-12%*	1.7 *+13%*	1.5 *+7%*
Total received Q2 1 October – 31 December 2019					
Percentage changed compared to prior year (Oct – Dec 2018)	**291** *+14%*	246 *+2%*			
Total completed Q2 1 October – 31 December 2019					
Percentage changed compared to prior year (Oct – Dec 2018)	**171** *-39%*	*150* *-28%*			
Total received 2019-20 YTD (Jul – Dec)					
Percentage changed compared to prior year (Jul – Dec 2018)	**537** *+8%*		950 *9%*		
Total completed 2019-20 YTD (Jul-Dec)					
Percentage changed compared to prior year (Jul – Dec 2018)	**321** *-34%*		911 *61%*		

KPI = 80% closed within 60 days:

As at 31 December 2019, 57% of NDBs have been closed within 60 days.

	NOW	-3	-6	-9	-12
PRIVACY – Voluntary DBNs					
	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
ON HAND – at the end of the quarter	**39**	43	32	27	20
ALLOCATION TIME (months)	**4.3**	1.3	1.2		
AWAITING ALLOCATION		9			
RECEIVED – per quarter *Percentage changed compared to prior quarter*	**23** ***-44%***	41 *+14%*	*36* *+6%*	34 *-8%*	37 *-34%*
RESOLVED – per quarter *Percentage changed compared to prior quarter*	**18** ***-61%***	46 *+7%*	*43* *+59%*	27 *-48%*	52 *+21%*
AVERAGE TIME TO COMPLETE YTD (months) *Percentage changed compared to prior quarter*	**3.1** ***-3%***	3.2 *+60%*	*2.0* *-17%*	2.4 *+20%*	2.0 *+18%*
Total received Q2 1 October – 31 December 2019 *Percentage changed compared to prior year (Oct – Dec 2018)*	**23** ***-43%***	41 *-28%*			
Total completed Q2 1 October – 31 December 2019 *Percentage changed compared to prior year (Oct – Dec 2018)*	**18** ***-65%***	46 *+7%*			
Total received 2019-20 YTD (Jul – Dec) *Percentage changed compared to prior year (Jul – Dec 2018)*	**64** ***-34%***		175 *+1%*		
Total completed 2019-20 YTD (Jul-Dec) *Percentage changed compared to prior year (Jul – Dec 2018)*	**64** ***-33%***		165 *+4%*		

KPI = 80% closed within 60 days:
As at 31 December 2019, 41% of Voluntary DBNs have been closed within 60 days.

NOW -3 -6 -9 -12

PRIVACY – MHR DBNs

	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
ON HAND – at the end of the quarter	**1**	0	6	4	0
ALLOCATION TIME					
AWAITING ALLOCATION					
RECEIVED – per quarter					
Percentage changed compared to prior quarter	**1** -	0 -	7 -13%	8 0%	8 -33%
RESOLVED – per quarter					
Percentage changed compared to prior quarter	**0** -	*6* *+20%*	*5* *+25%*	4 *-64%*	14 *+56%*
AVERAGE TIME TO COMPLETE YTD (months)					
Percentage changed compared to prior quarter	**2.5** -	2.5 *+32%*	*1.9* *+90%*	1 -9%	1.1 *+38%*
Total received Q2 1 October – 31 December 2019					
Percentage changed compared to prior year (Oct – Dec 2018)	1 *-88%*	0 -			
Total completed Q2 1 October – 31 December 2019					
Percentage changed compared to prior year (Oct – Dec 2018)	0 -	6 *-33%*			
Total received 2019-20 YTD (Jul – Dec)					
Percentage changed compared to prior year (Jul – Dec 2018)	1 *-95%*		35 *+25%*		
Total completed 2019-20 YTD (Jul-Dec)					
Percentage changed compared to prior year (Jul – Dec 2018)	6 *-74%*		33 *+21%*		

KPI = 80% closed within 60 days:

As at 31 December 2019, 50% of MHR DBNs have been closed within 60 days.

	NOW	-3	-6	-9	-12
PRIVACY – CIIs					
	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
ON HAND – at the end of the quarter	**20**	25	21	21	20
ALLOCATION TIME (months)					
AWAITING ALLOCATION					
OPENED – per quarter	***2*** ***-78%***	*9* *+350%*	*2* *-50%*	4 *+100%*	2 *-71%*
RESOLVED – per quarter	***6*** ***+20%***	*5* *+150%*	*2* *-33%*	3 *+300%*	Nil *-100%*
AVERAGE TIME TO COMPLETE YTD (months)	***10.8*** ***-30%***	*8.3* *+48%*	*5.6* *+17%*	4.8 *N/A*	N/A *N/A*
Total received Q2 1 October – 31 December 2019 *Percentage changed compared to prior year (Oct – Dec 2018)*	***2*** ***0%***	*9* *+29%*			
Total completed Q2 1 October – 31 December 2019 *Percentage changed compared to prior year (Oct – Dec 2018)*	6 -	5 *+150%*	15 *-29%*		

KPI = 80% closed within 8 months:

As at 31 December 2019, 36% of CIIs have been closed within 8 months.

	NOW	-3	-6	-9	-12
FOI – IC Reviews					
	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
ON HAND – at the end of the quarter	**955**	851	847	860	786
ALLOCATION TIME (months)	**20**	18.0	14.6	11.9	11
AWAITING ALLOCATION	**400**	330	291	243	296
RECEIVED – per quarter					
Percentage changed compared to prior quarter	**251**	210	190	210	241
	+20%	*+11%*	*-10%*	*-13%*	*-15%*
RESOLVED – per quarter					
Percentage changed compared to prior quarter	**149**	210	205	136	136
	-29%	*+2%*	*+51%*	*0%*	*-25%*
AVERAGE TIME TO COMPLETE YTD (months)					
Percentage changed compared to prior quarter	**8.3**	8.2	9.3	7.7	7.7
	+1%	*-12%*	*+21%*	*0%*	*+18%*
Total received Q2 1 October – 31 December 2019					
Percentage changed compared to prior year (Oct – Dec 2018)	**251**	210			
	+6%	*-27%*			
Total completed Q2 1 October – 31 December 2019					
Percentage changed compared to prior year (Oct – Dec 2018)	**149**	210			
	+10%	*+15%*			
Total received 2019-20 YTD (Jul – Dec)					
Percentage changed compared to prior year (Jul – Dec 2018)	**461**		928		
	-12%		*+16%*		
Total completed 2019-20 YTD (Jul-Dec)					
Percentage changed compared to prior year (Jul – Dec 2018)	**359**		659		
	+13%		*8%*		

KPI = 80% closed within 12 months:

As at 31 December 2019, 69% of IC Reviews have been closed within 12 months.

	NOW	-3	-6	-9	-12
FOI - Complaints					
	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
ON HAND – at the end of the quarter	**118**	109	91	85	75
ALLOCATION TIME (months)	**24.9**	22.2	26.7	24.7	N/A
AWAITING ALLOCATION	**82**	8	25	35	
RECEIVED – per quarter *Percentage changed compared to prior quarter*	***24*** ***+33%***	*18* *+100%*	*9* *-36%*	14 *-26%*	19 *+6%*
RESOLVED – per quarter *Percentage changed compared to prior quarter*	***14*** -	*0* -	*5* *+67%*	3 *-63%*	8 *+14%*
AVERAGE TIME TO COMPLETE YTD (months) *Percentage changed compared to prior quarter*	**16.5**	n/a	*3.6* *-49%*	7 *-39%*	11.5 *+121%*
Total received Q2 1 October – 31 December 2019 *Percentage changed compared to prior year (Oct – Dec 2018)*	**24** ***+26%***	17 *-6%*			
Total completed Q2 1 October – 31 December 2019 *Percentage changed compared to prior year (Oct – Dec 2018)*	**14** ***+7%***	0 -			
Total received 2019-20 YTD (Jul – Dec) *Percentage changed compared to prior year (Jul – Dec 2018)*	**42** ***+14%***		61 *-2%*		
Total completed 2019-20 YTD (Jul-Dec) *Percentage changed compared to prior year (Jul – Dec 2018)*	**14** ***0%***		22 *-24%*		

KPI = 80% closed within 12 months:

As at 31 December 2019, 43% of FOI complaints have been closed within 12 months.

	NOW	-3	-6	-9	-12
FOI – Vexatious Applications (s 89K and s 89M(2))					
	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
ON HAND – at the end of the quarter	**2**	1	1	6	5
ALLOCATION TIME (months)					
AWAITING ALLOCATION					
RECEIVED – per quarter	**1**	0	2	4	2
Percentage changed compared to prior quarter	**-**	-	*-50%*	*+100%*	*-75%*
RESOLVED – per quarter	**0**	0	7	3	1
Percentage changed compared to prior quarter	**-**	-	*+133%*	*+200%*	*-86%*
AVERAGE TIME TO COMPLETE YTD (months)			5.4	2.7	3.4
Percentage changed compared to prior quarter	**N/A**	N/A	*+100%*	*-21%*	*+127%*
Total received Q2 1 October – 31 December 2019	**1**	0			
Percentage changed compared to prior year (Oct – Dec 2018)	***-50%***	-			
Total received 2019-20 YTD (Jul – Dec)	**1**		7		
Percentage changed compared to prior year (Jul – Dec 2018)	***-90%***		*-36%*		

No KPI in PBS for Vexatious Application requests

	NOW	-3	-6	-9	-12
FOI – Extension of Time Requests					
	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
ON HAND – at the end of the quarter	**169**	14	49	19	27
ALLOCATION TIME (months)					
AWAITING ALLOCATION					
RECEIVED – per quarter					
Percentage changed compared to prior quarter	**1,096**	798	820	943	1,000
	+37%	*-3%*	*-13%*	*-6%*	*-2%*
RESOLVED – per quarter					
Percentage changed compared to prior quarter	**941**	833	941	948	1,101
	+13%	*-11%*	*-1%*	*-14%*	*+17%*
AVERAGE TIME TO COMPLETE YTD (**DAYS**)	**2.7**	2.7	3.6	3.5	4.1
	0%	*-25%*	*+3%*	*-15%*	*+173%*
Total received Q2 1 October – 31 December 2019					
Percentage changed compared to prior year (Oct – Dec 2018)	**1,096**	797			
	+10%	*-22%*			
Total received 2019-20 YTD (Jul – Dec)					
Percentage changed compared to prior year (Jul – Dec 2018)	**1,894**		3785		
	-6%		*+12%*		

No KPI in PBS for Extension of Time Requests

	NOW	-3	-6	-9	-12
ENQUIRIES					
	Dec-19 Q2	Sep-19 Q1	Jun-19 Q4	Mar-19 Q3	Dec-18 Q2
Privacy enquiries (phone & written; **received** in quarter)	2630	2940	3700	3,012	2,928
FOI enquiries (phone & written; **received** in quarter)	635	658	651	785	715
Other (phone & written; **received** in quarter)	1461	1546	1135	1,139	1,162
Total	**4726**	**5144**	**5486**	**4,936**	**4,805**
Total received per Qtr *(Percentage changed compared to prior quarter)*					
Privacy	**2630** *-11%*	2940 *-21%*			
FOI	**635** *-3%*	658 *+1%*			
Other	**1461** *-5%*	1546 *+36%*			
Total	**4726** *-8%*	5,144 *-6%*			
Total received 2018-19 *(Percentage changed compared to previous year)*					
Privacy (including Other)			**17,445** *-10%*		
FOI			**2,881** *+49%*		
Total			**20,326**		

KPI = 90% of written enquiries closed within 10 working days:

As at 31 December 2019:

86% of Privacy written enquiries have been closed within 10 working days.

92% of FOI written enquiries have been closed within 10 working days.

96% of Other written enquiries have been closed within 10 working days.

OAIC Staffing figures

Total Staff: Overview

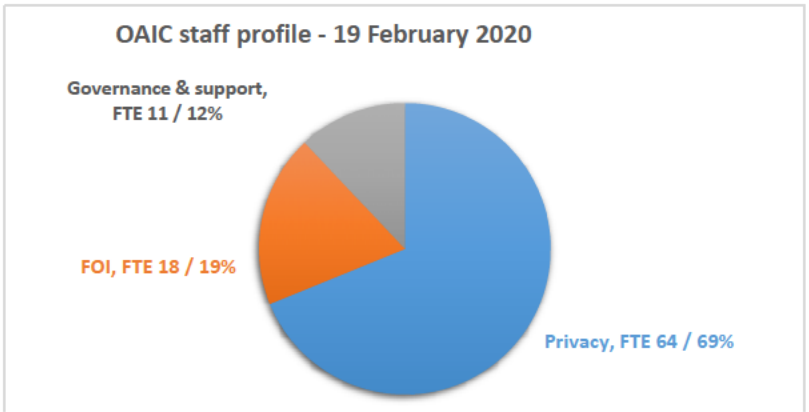
(As at)	19 February 2020	2 October 2019	February 2019	February 2018	February 2017	May 2014
FTE	94	99	85	75	69	83
ASL	92	90	86	74	70	77
Headcount	109	113	99	86	81	97

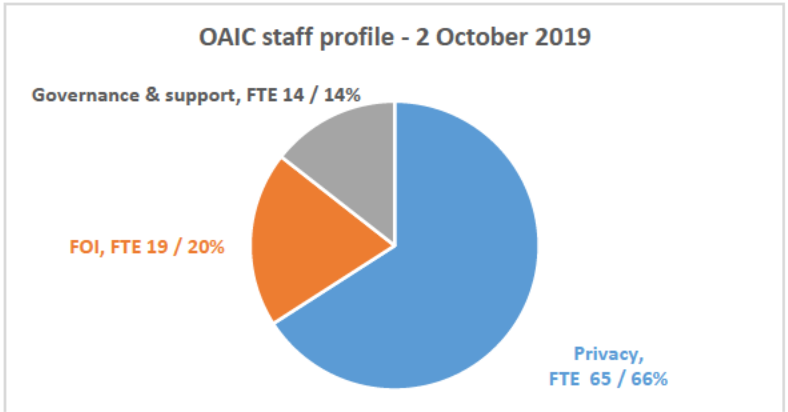
Funding: FTE

(As at)	19 February 2020	2 October 2019	February 2019	February 2018	February 2017	May 2014
Budget	94	99	76	62	56	67
ADHA MOU	Nil	Nil	10	12	13	16
Total	**94**	**99**	**85**	**75**	**69**	**83**

Staffing allocation

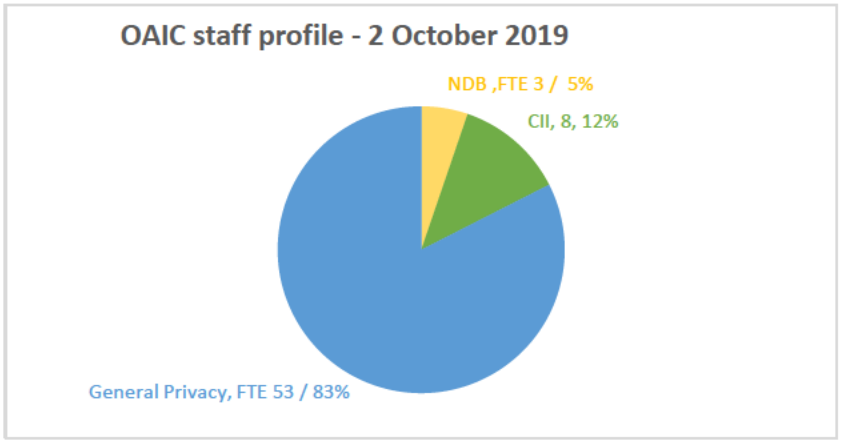
	As at 19 February 2020		As at 2 October 2019	
	FTE	%	FTE	%
Privacy	64	69%	65	65%
FOI	18	19%	19	20%
Governance & support	11	12%	14	14%
Total	**94**		**99**	

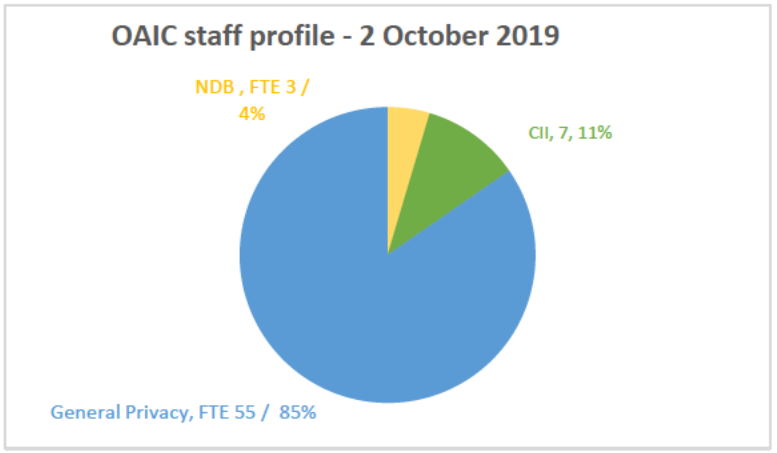




NDB allocation:

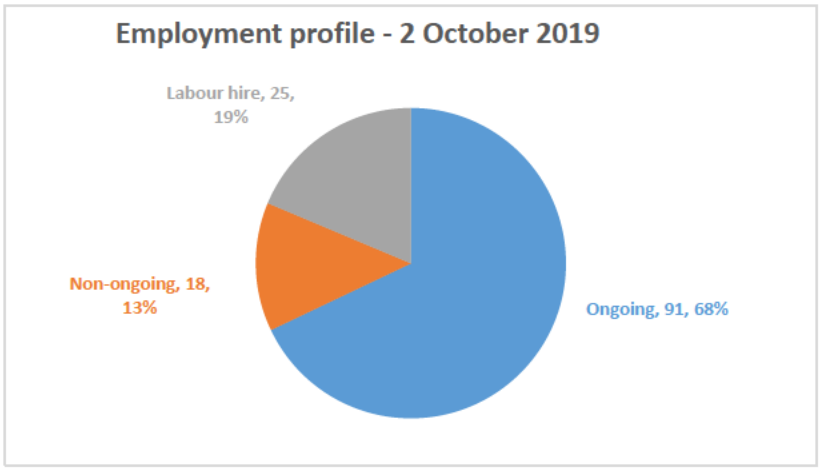
	As at 19 February 2020		As at 2 October 2019	
	FTE		FTE	%
NDB	3	5%	3	4%
CII	8	12%	7	11%
General Privacy	53	83%	55	85%
	64		**65**	

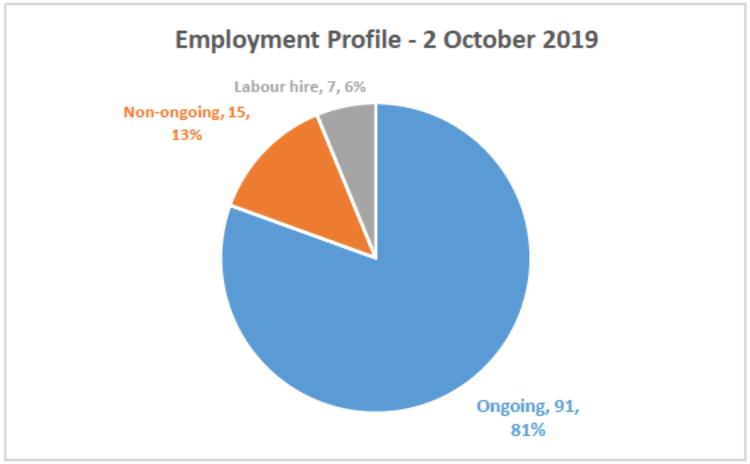




Employment type:

	As at 19 February 2020		As at 2 October 2019	
	Headcount		Headcount	%
Ongoing	91	68%	91	81%
Non-ongoing	18	13%	15	13%
Labour hire	25	19%	7	6%
	134		**113**	





General staffing details:

(Financial year)	2019/20 (as at 19/02/20)	2018/19	2017/18	2016/17	2015/16	2014/15
Positions advertised	6	15	14	15	17	10
Engagements permanent	20	20	10	14	24	7
Engagements temporary	18	8	11	6	1	2
Internal Promotions	16	16	9	12	12	5
Total	**54**	**44**	**30**	**32**	**37**	**14**

Turnover: Terminations (APS staff only)

	2019/20 (as at 19/02/20)	2018/19	2017/18	2016/17	2015/16	2014/15
Permanent	13	19	14	11	15	28
Temporary	10	5	3	2	1	3
Total	**23**	**24**	**17**	**13**	**16**	**31**
Turnover % (based on permanent staff and positions)	**14%**	**24%**	**21%**	**13%**	**20%**	**48%**

Leave: Unplanned sick leave per FTE

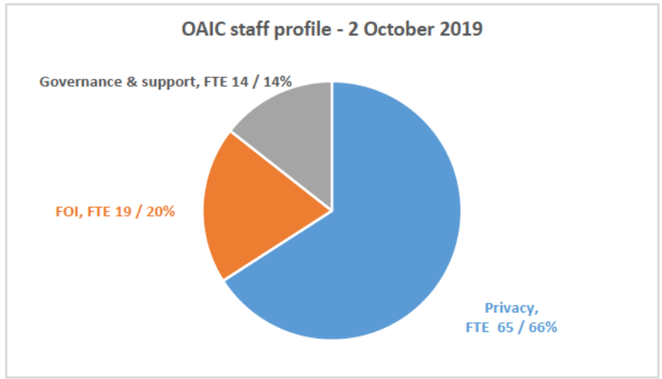
(Financial year)	2019/20 (as at 19/02/20)	2018/19	2017/18	2016/17	2015/16	2014/15

Hours	76.35	87.58	77.22	83.23	83.38	80.71
Days	10.18	11.68	10.33	11.52	11.12	10.76

Leave: Deemed annual leave days

(As at)	2019/20 (as at 19/02/20)	2018/19	30/06/2018	30 June 2017	30 June 2016	30 June 2015
Dispute resolution	4	3	4	6	0	0
Regulation and Strategy	2	1	2	3	3	1
Operations	2	2				
Executive	2	2	1	1	2	2
Total	**10**	**8**	**7**	**10**	**5**	**3**

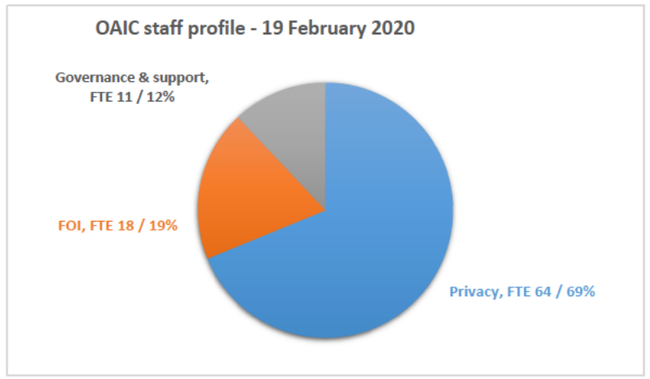
Staffing and workload comparison



Staff profile:
- Total FTE is 99
- 66% assigned to privacy
- 20% assigned to FOI
- 14% assigned to governance & support

Note:
- Staffing is point in time (2 October 19)
- Small changes in staff movements shift allocation % significantly

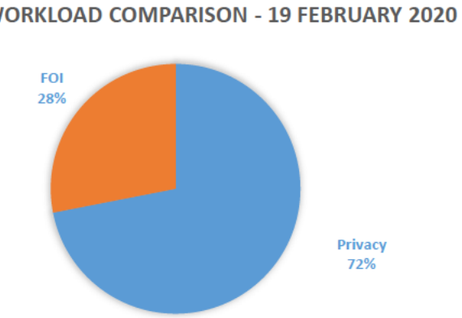
Privacy staff include:
- Dispute Resolution, privacy
- Regulation & Strategy (almost all)
- Privacy support by Executive, Legals and SCaC



Staff profile:
- Total FTE is 94
- 69% assigned to privacy
- 19% assigned to FOI
- 11% assigned to governance & support

Note:
- Staffing is point in time (19 February 20)
- Small changes in staff movements shift allocation % significantly

Privacy staff include:
- Dispute Resolution, privacy
- Regulation & Strategy (almost all)
- Privacy support by Executive, Legals and SCaC



Workload includes:
- Privacy enquiries: 9782
- Privacy complaints: 1665
- Privacy NDBs: 551
- Privacy DBN: 121
- Privacy Health DBN: 1
- Privacy submissions: 10
- Privacy assessments 11
- Privacy advice and consultation 173
- Privacy CII 11
- Privacy Bill scrutiny 29
- FOI enquiries: 1534
- FOI IC: 551
- FOI complaints: 57
- FOI EOT: 2311
- FOI Consultation: 12
- FOI policy advice: 343
- FOI Bill scutiny: 18
- FOI submissions: 2

Governance & support staff include:
- remaining areas of work that are not privacy or FOI, and
- all of Corporate Support team (e.g. EO / Office manager / Records manager & officer etc)
- notable portion of the Legal and SCaC teams

Commissioner brief: Budget and resourcing

Key messages

- The OAIC incurred a $1.195million financial loss in 2018-19
- Total revenue, including MOUs, for 2019-20 is $23.234million
- The 2019-20 base appropriation budget represents a 51% increase in funding compared to the 2018-19 Budget
- 2019-20 ASL cap is 124 – actual ASL at 2 October 2019 is 90.

Critical facts

- OAIC incurred a total (unapproved) financial loss of $1.195million in 2018-19.
    - 2018-19 total revenue was $15.854million — $13.825million is appropriation (increased by $329,000 in 2019-20 Budget for Medicare data matching) & $2.2029million is MOU
- 2019-20 Budget allocated $25.121million over three years undertake regulatory functions, including regulating the handling of personal information and taking enforcement action.
    - 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.
    - 2019-20 total revenue is $23.264million. $13.825million is appropriation (increased by $329,000 in 2019-20 Budget for Medicare data matching) & $2.2029million is MOU
- OAIC has not receive any additional resourcing for the Notifiable Data Scheme.
- Received $12.911million over forward estimates for Consumer Data Right Scheme (CDR) in 2018-19 Budget (including a once-off capital injection for new office space of $860,000)
- s74 External revenue (MOU) increase from $2.029m in 2018-19 to $2.323m in 2019-20. The overarching increase relates to the ADHA cost recovery MOU (actual amount charged vs value).

  In the forward estimates, MOU value is $252,500 in 2020-21 and nil after that. This is due to several MOUs (including ADHA at $2.070million) terminating at 30 June 2020 and yet to be renewed.
- Funding concluded at 30 June 2019 for the **terminating measure** *Enhanced Welfare Payment Integrity – non-employment income data matching (commenced MYEFO 2015-16), $1.326million.*

Possible questions

Why did the OAIC incur a financial loss?

- Total loss is $1.195million, including depreciation and amortisation
    - The OAIC is permitted to have a loss up to the total the value of depreciation and amortisation, which in 2018-19 was $464,000
- In May 2019 the Department of Finance issued the OAIC with an invoice for $531,000 for an unexpected additional superannuation contribution
- The balance of $200,000 can be attributed to a number of factors, including: OAIC's enhanced regulatory and legal position, additional accommodation & recruitment agency exit fees.

What caused the additional unexpected superannuation payment?

s 47F

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

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

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

The Office 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. Since 1 July 2019 and following recruitment, the OAIC's FTE has increased from to 90 to 99. The additional staff are primarily allocated to privacy case management and the Regulation and Strategy Branch.

Does this funding include an allocation for freedom of information?

The funding specifically does not apply to freedom of information and staffing levels for the management of FOI matters have not increased. While the office continues to look for and implement opportunities to increase productivity in relation to its freedom of information functions, it remains the case that demonstrated significant efficiencies have been found and applied the function has not kept pace with incoming complaints and decision reviews. There has been an increase in Information Commissioner reviews of 82% between 2015 – 16 and 2018 – 19.

What activities will you undertake with increase of funding for Medicare data matching?

The OAIC is the complaint handling body for the regime and offers 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 also 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.

Will the growing workload result in greater backlogs?

The OAIC continues to implement efficiencies in the way that work is completed. For example, the OAIC recently reviewed its workflow processes for the Dispute Resolution Branch which, once implemented, will streamline the complaint handling process. It is anticipated the new process will assist in maintaining and

then reducing the backlog. Additionally, the enhanced budget will enable additional resources to be allocated to clear the backlog.

Key dates

- 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.
- 1 July 2019: MOU funding with ADHA secured at $2.070million for one year. The MOU no longer operates on a cost recovery basis. The value of this MOU is not included in the PBS as was negotiated after publication of the 19/20 federal Budget.
- 30 June 2019: *Enhanced Welfare Payment Integrity – non-employment income data matching (commenced MYEFO 2015-16)* measure valued at $1.326million terminates.
- 1 July 2018: 2018-19 Budget provides $12.91million over the forward estimates for CDR
- 22 February 2018: NDB Scheme commenced, no funding received.
- 1 July 2023: reduction in revenue due to terminating measure (statutory obligations and social media).

Forward estimates

	2018-19	2019-20	2020-21	2021-22	2022-23
Appropriation	$13,825,000	$20,941,000	$21,000,000	$20,685,000	$13,271,000
MOUs	$2,029,523	$2,322,500	$178,000	—	—
Total	**$15,854,523**	**$23,263,500**	**$21,178,000**	**$20,685,000**	**$13,271,000**
Difference from prior year		+$7,408,977	-$2,085,500	-$493,000	-$7,414,000

MOU detail

MOU	2018-19	2019-20	2020-21	2021-22	2022-23
ADHA	$1,626,023	$2,070,000	—	—	
ACT Government	$177,500	$177,500	$177,500	concluded	—
USI	$100,000	Concluded	—	—	—
DHA – NFBMC	—	$75,000	$75,000	—	
Ticket sales	$73,000	—	—	—	—
Total	$2,029,523	$2,322,500	$252,500	—	—

Statutory obligations and social media detail

	2018-19	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**	**$3,036,000**	**$3,058,00**	**—**

Medicare data matching

	2018-19	2019-20	2020-21	2021-22	2022-23
Appropriation	$329,000	$571,000	$565,000	$560,000	$560,000
Capital	—	–	—	—	—
Total	**$329,000**	**$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**	

2019-20 Funding

- 2019-20 total revenue is $23.263million, of this:
  - $20.941million is appropriation (including 7.734million for social media & $3.178 million CDR)
  - $2.322million is MOU based.

2018-19 operational loss

Item	Amount	Note
Depreciation & amortisation	$464,000	Permitted loss amount
Superannuation contribution	$531,000	Mandatory, unforeseen and issued in May 2019
Unforeseen	$200,000	Number of factors: additional accommodation / legal expenditure / recruitment agency exit fees
Total	**$1,195,000**	

2019-20 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 20 February 2020

- Year-to-date ASL at 20 February 2020 is 92
- Year-to-date FTE at 20 February 2020 is 94 (detailed below)
- Current recruitment agency staff at 20 February is 23

- Full-time-equivalent (FTE) at 2 October 2019 is 94. That FTE is allocated to:

	20 February 2020	**2 October 2019**	**20 March 2019**	**6 February 2019**
OAIC	94 FTE	99 FTE	86 FTE	85 FTE
Privacy (including NDB)	64 / 69%	65 / 66%	59 / 68 %	57 / 67%
NDB	3 / 5%	4 / 11%	7 / 8%	10 / 12%
FOI	18 / 19%	20 / 20%	20 / 24 %	21 / 25%
Governance & support	11 / 12%	14 / 14%	7 / 9%	7 / 8%

- 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**
Brenton Attard	March 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. It was announced that in consultation with the Privacy Commissioner, legislation will be introduced to support improved compliance.

As part of the measure, the Department of Health intends to review the arrangements relevant to section 135AA of the *National Health Act 1953*. Section 135AA of the *National Health Act 1953* provides for the Australian Information Commissioner to make privacy rules that specify the requirements for storage and linkage of Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Schedule (PBS) information.

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

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	

Commissioner brief: Performance against MoUs

MOU: ACT Government Provision of Privacy Services

MOU value:

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

Deliverables under MoU			OAIC Performance		
2017-18	2018-19	2019-20	2017-18	2018-19	2019-20 (1 Jul – 31 Jan 2020)
Reporting One annual report on the operation of this MOU in a form that can be tabled in the Legislative Assembly (s 54 report)	**Reporting** One annual report for each year of the Term of the MOU about its operation in a form that can be tabled in the Legislative Assembly (s 54 report)	**Reporting** One annual report for each year of the Term of the MOU about its operation in a form that can be tabled in the Legislative Assembly (s 54 report)	**Reporting** 2017–18 Annual Report made under ACT MoU deliverable met, and published on OAIC website	**Reporting** 2018-19 Annual Report made under ACT MoU provided but not tabled	**Reporting** Due to be tabled by 22 October 2020
Complaints and Enquiries Respond to complaints or enquiries.	**Complaints and Enquiries** Respond to complaints or enquiries.	**Complaints and Enquiries** Respond to complaints or enquiries.	**Complaints** • 11 received • 17 closed **Enquiries** • 19 received by phone • 4 received in writing	**Complaints** • 10 received • 8 closed **Enquiries** • 21 enquiries (written and phone)	**Complaints** • 6 received • 8 closed **Enquiries** • 16 enquiries (written and phone)
Assessments One assessment per year.	**Assessments** One assessment per year for the term of the MoU.	**Assessments** One assessment per year for the term of the MoU.	**Assessments** • 1 finalised • 1 ongoing as at 30 June 18	**Assessments** • 1 commenced • 1 ongoing as at 30 June 19	**Assessments** • 1 commenced • 1 finalised
Privacy Professional Network Access to Privacy Professional Network meetings.	**Privacy Professional Network** Access to Privacy Professional Network meetings.	**Privacy Professional Network** Access to Privacy Professional Network meetings.	**Privacy Professional Network** • 4 meetings	**Privacy Professional Network** • 0 meeting	**Privacy Professional Network** • 0 meetings
	Guidance The Commissioner will review and update the Commissioner's	**Guidance** The Commissioner will review and update the Commissioner'	**Guidance Materials** • 1 material updated	**Guidance Materials** • 0 materials reviewed/ updated	**Guidance Materials** • 0 material reviewed/ updated

	website content and guidance material in relation to the Information Privacy Act.	s website content and guidance material in relation to the Information Privacy Act.			
Data Breach Notifications Where ACT agencies notify the Commissioner of a data breach, the Commissioner will register the breach and provide further advice. Provision of advice or further services will be at the Commissioner's discretion.	**Data Breach Notifications** Where ACT agencies notify the Commissioner of a data breach, the Commissioner will register the breach and provide further advice. Provision of advice or further services will be at the Commissioner's discretion.	**Data Breach Notifications** Where ACT agencies notify the Commissioner of a data breach, the Commissioner will register the breach and provide further advice. Provision of advice or further services will be at the Commissioner' s discretion.	**Data Breach Notifications** • 10 received	**Data Breach Notifications** • 4 received	**Data Breach Notifications** • 9 received
Policy and Legislation Advice Includes limited advice to agencies, scrutiny of Bills, appearances before the ACT Legislative Assembly at Estimates Committees and advice to Members of the ACT Legislative Assembly.	**Policy and Legislation Advice** Includes limited advice to agencies, scrutiny of Bills, appearances before the ACT Legislative Assembly at Estimates Committees and advice to Members of the ACT Legislative Assembly.	**Policy and Legislation Advice** Includes limited advice to agencies, scrutiny of Bills, appearances before the ACT Legislative Assembly at Estimates Committees and advice to Members of the ACT Legislative Assembly.	**Policy Advices** • 1 policy advice requests received	**Policy Advices** • 2 policy advice requests received	**Policy Advices** • 0 policy advice requests received

MOU: Australian Digital Health Agency Privacy, Healthcare Identifiers & My Health Records

MOU value:

- 2017-18: $1,688,343.83 (actual based on cost recovery)
- 2018-19: $1,626,023.40 (actual based on cost recovery)
- 2019-20: $2,070,00.00 (fixed fee for service)

Deliverables under MoU			**OAIC Performance**		
2017-18	2018-19	2019-20	2017-18	2018-19	2019-20 (1 Jul – 31 Jan)
Complaints Receive and respond to complaints relating to all privacy aspects of the My Health Records system and the HI service	**Complaints** Receive and respond to complaints relating to all privacy aspects of the My Health Records system and the HI service	**Complaints** Receive and respond to complaints relating to all privacy aspects of the My Health Records system and the HI service	**Complaints** • 8 MHR received • 5 MHR closed • Nil HI received • Nil HI closed	**Complaints** • 62 received • 42 closed (Both MHR & HI)	**Complaints** • 6 Received • 20 closed (Both MHR & HI)
Commissioner Initiated Investigations The OAIC will investigate, where appropriate, acts and practices that may be a misuse of Healthcare Identifiers or a contravention of the My Health Records Act, on the Commissioner's own initiative.	**Commissioner Initiated Investigations** The OAIC will investigate, where appropriate, acts and practices that may be a misuse of Healthcare Identifiers or a contravention of the My Health Records Act, on the Commissioner's own initiative.	**Commissioner Initiated Investigations** The OAIC will investigate, where appropriate, acts and practices that may be a misuse of Healthcare Identifiers or a contravention of the My Health Records Act, on the Commissioner's own initiative.	**Commissioner Initiated Investigations** • Nil MHR commenced • Nil MHR finalised • Nil HI commenced • Nil HI finalised	**Commissioner Initiated Investigations** • Nil MHR commenced • Nil MHR finalised • Nil HI commenced • Nil HI finalised	**Commissioner Initiated Investigations** • 5 MHR commenced
Data Breach Notifications Deal with DBNs received relating to the MHR system and the HI service. Investigate failures to notify data breaches.	**Data Breach Notifications** Deal with DBNs received relating to the MHR system and the HI service. Investigate failures to notify data breaches.	**Data Breach Notifications** Deal with DBNs received relating to the MHR system and the HI service. Investigate failures to notify data breaches.	**Data Breach Notifications** • 28 received	**Data Breach Notifications** • 35 received	**Data Breach Notifications** • 1 received
Assessments Conduct a minimum of 4 and up to 6	**Assessments** Conduct a minimum of 4 and up to 6	**Assessments** Conduct a minimum of 4 and up to 6	**Assessments** • 1 commenced • 1 finalised	**Assessments** • 4 commenced • 0 finalised	**Assessments** • 0 commenced • 4 finalised

assessments in relation to the MHR system and the HI service. This will be subject to a work plan developed by the OAIC in consultation with the ADHA.	assessments in relation to the MHR system and the HI service. This will be subject to a work plan developed by the OAIC in consultation with the ADHA.	assessments in relation to the MHR system and the HI service. This will be subject to a work plan developed by the OAIC in consultation with the ADHA.			
Enquiries Respond to privacy related enquiries about the handling of MHR information and the HI service	**Enquiries** Respond to privacy related enquiries about the handling of MHR information and the HI service	**Enquiries** Respond to privacy related enquiries about the handling of MHR information and the HI service	**Enquiries** • 17 MHR received • 2 HI received	**Enquiries** • 155 (both MHR & HI)	**Enquiries** • 5 (both MHR & HI)
Guidance Materials Prepare and/or update written guidance materials for individuals and entities on the MHR system, MHR information, the HI service, and handling HI information	**Guidance Materials** Prepare and/or update written guidance materials for individuals and entities on the MHR system, MHR information, the HI service, and handling HI information	**Guidance Materials** Prepare and/or update written guidance materials for individuals and entities on the MHR system, MHR information, the HI service, and handling HI information	**Guidance Materials** • 19 materials reviewed/updated	**Guidance Materials** • 11 materials reviewed/updated	**Guidance Materials** • 4 materials reviewed/updated
Speeches, articles and media OAIC will prepare HI and MHR speeches, articles and media comments on privacy matters.	**Speeches, articles and media** OAIC will prepare HI and MHR speeches, articles and media comments on privacy matters.	**Speeches, articles and media** OAIC will prepare HI and MHR speeches, articles and media comments on privacy matters.	**Speeches** • 5 delivered **Media Enquiries** • 1 received	**Speeches** • 3 delivered **Media Enquiries** • 25 received	**Speeches** • 1 delivered **Media Enquiries** • 2 received
Consultations The OAIC will participate in consultations and comment on digital health developments that relate to the HI service and My Health Record system, including	**Consultations** The OAIC will participate in consultations and comment on digital health developments that relate to the HI service and My Health Record system, including	**Consultations** The OAIC will participate in consultations and comment on digital health developments that relate to the HI service and My Health Record system, including	**Consultations** 7 consultations provided	**Consultations** 17 consultations provided	**Consultations** 14 consultations provided

commenting on draft legislation that may interact with the HI Act and the My Health Records Act.	commenting on draft legislation that may interact with the HI Act and the My Health Records Act.	commenting on draft legislation that may interact with the HI Act and the My Health Records Act.			

MOU: Department of Home Affairs National Facial Biometric Matching Capability

MOU value:

- 2019-20: $75,000
- 2020-21: $75,000

Deliverables under MoU		**OAIC Performance**	
2019-20	2020-21	2019-20	2020-21 (1 Jul – 31 Jan)
Assessments Conduct a privacy assessment of Home Affair's management of the Hub	**Assessments** Conduct privacy assessments of Affair's management of the NDLFRS	**Assessments** • Nil	**Assessments** • n/a

Document history

Updated by	**Date**	**Reason**	**Approved by**	**Date**
Brenton Attard	22/02/20	March 2020 Estimates		

Commissioner brief: APS Census results

Key messages

- The OAIC actively engaged with its staff to understand what they perceived to be the most important things we must retain and strengthen and where there was room for improvement.
- All staff were invited to attend small workshops in September to explore some of the issues raised through the Census with a view to gaining a deeper understanding of staff perceptions and identifying suggestions to improve our environment.
- A working group has been formed and will implement a range of activities in response to the Census results.
- The results reflect that OAIC has a committed workforce. There is a positive culture with high levels of acceptance, respect and ethical behaviour.
- Results are also reflective of the significant change and growth the organisation is experiencing and continued increases to work volumes. Staff are identifying a need for increased focus of the organisation, and of the SES in particular, on improving communication, valuing staff contributions and on the health and wellbeing of staff. There is also an appetite for clearer prioritisation of work, support for innovation and risk taking and reducing inefficiencies.
- The OAIC's results were made public along with other participating agencies, in November.

Critical facts

- Results were made public in November
- Some of the positive results are:
  - 85% believe strongly in the agency purpose;
  - 93% happy to go the extra mile
  - 95% believe staff are accepting of diverse backgrounds
  - 85% support an inclusive workplace culture (up 10%)
- Some of the more challenging aspects are:
  - 60% recommend the agency as a good place to work (down 14%);
  - 47% believe agency does a good job promoting health and well-being.
  - 48% believe SES manager effectively leads change.
  - 12% drop in SES manager is of high quality – but 69% positive remains a good result
  - 29 % believe Internal comms is effective (down 24%, 44% negative)
  - 18% are positive about mobility outside the agency
- OAIC is below the APS index score in relation to:
  - Engagement: OAIC (71%) APS index score (72%) (83 of 97 agencies)
  - Wellbeing: OAIC (64%) APS index score (67%) (77 of 97 agencies)
  - Innovation: OAIC (59%) APS index score (66%) (91 of 97 agencies)

Possible questions

- ***Are you happy with the OAICs results in the 2019 APS Employee Census?***

  The OAIC Census results are mixed. There are certainly some very positive results around staff willingness to go the extra mile and belief in the agency purpose. There is also a very positive culture. However the agency is under pressure and the Census results reflect that. There is a need to focus on a range of areas including internal communication, innovation, recognising staff commitment and looking after their well-being.

- ***What are you doing with the Census results?***

The OAIC has undertaken a significant process of engaging with staff to better understand the results and to identify practical strategies in relation to the things that are of greatest concern to staff. We will be implementing a change program with a focus on staff inclusion.

Key dates

- Results were made public on 25 November when they were tabled in Parliament.

Other background

- The OAIC 2019 APS Employee Census result can be found at: D2019/009649

Document history

Updated by	Reason	Approved by	Date
Ruth Mackay	March 2020 - Reflect the passage of time since the original Estimates briefs. The only new information is that a working group has been formed and will implement a range of activities.		

HOT TOPIC BRIEF OAIC–01
OAIC Facebook Investigation

Related backpocket: Nil

- On 5 April 2018 the OAIC opened an investigation into whether Facebook has breached the *Privacy Act 1988* (the Privacy Act) following confirmation from Facebook that the personal information of up to 311,127 individuals in Australia was collected by the 'This Is Your Digital Life' app, including personal information of installers of the app and their Facebook friends.[1] The OAIC has also accepted a representative complaint about the matter.
- The OAIC does not generally publicly comment on ongoing investigations.

- Between 2013 and 2015, a Cambridge University researcher published a personality quiz app 'This Is Your Digital Life' (the app) on Facebook, which Facebook confirmed was installed by approximately 270,000 Facebook users.

- Media reports stated that because of Facebook's app developer policies at the time, the app was also able to collect profile information from these individuals' friend lists, where their privacy settings permitted this. In total, the app collected personal information of up to 87 million Facebook users globally.

- Facebook has since confirmed in public statements that it was made aware that the researcher, Dr Kogan, disclosed the Facebook profile information he had collected to Cambridge Analytica, a data analytics firm.

- Facebook's public statement of 16 March 2018 advised that in 2015, once Facebook became aware of the disclosure to Cambridge Analytica, it removed the app's access to Facebook data and requested confirmation from Cambridge Analytica that it had destroyed the data. Facebook claims that it received this confirmation from Dr Kogan and Cambridge Analytica.[2]

- Facebook's public statement of 4 April 2018 confirmed that the personal information of up to about 311,127 individuals in Australia may have been collected by the app.[3]

---

[1] https://newsroom.fb.com/news/2018/04/restricting-data-access/
[2] https://about.fb.com/news/2018/03/suspending-cambridge-analytica/
[3] https://newsroom.fb.com/news/2018/04/restricting-data-access/

- On 31 July 2018 Facebook announced that it was cutting off Application Programming Interface[4] (API) access for hundreds of thousands of inactive apps that had not submitted to an app review process.[5]

- Facebook has been investigated by several international data protection authorities in relation to this incident.

- On 24 July 2019 the US Federal Trade Commission settled its investigation into Facebook, which considered whether Facebook had violated a 2012 FTC Order. The settlement terms include a US$5 billion penalty and changes to Facebook's privacy and governance practices. To be given the force of law, the settlement must be signed by a US District Court Judge. This has not yet occurred.[6]

- On 25 April 2019, a joint investigation by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia found Facebook contravened Canadian privacy laws. Facebook declined to implement the changes to its privacy practices recommended in the joint investigation report.[7] On 6 February 2020, the Privacy Commissioner of Canada filed a Notice of Application in Canada's Federal Court seeking a declaration that Facebook has contravened Canadian privacy laws, as well as binding orders requiring Facebook to change its practices and comply with the law.

- On 24 October 2018, the UK Information Commissioner's Office fined Facebook a maximum of £500,000 for breaches of the UK *Data Protection Act 1988* in relation to the incident. This was part of the Information Commissioner's investigation, commenced in May 2017, into the *Use of Data Analytics for Political Purposes*.[8] While Facebook initially appealed the fine in a UK court, the parties reached a settlement on 30 October 2019,

[4] Application Programming interfaces are a set of functions and procedures allowing the creation of applications that access the features or data of an operating system.
[5] https://newsroom.fb.com/news/2018/07/update-on-app-review/
[6] https://www.courtlistener.com/docket/15959672/united-states-v-facebook-inc/
[7] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200206/
[8] https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/

under which the appeal was withdrawn and Facebook agreed, without admitting liability, to pay the £500,000 fine.

Regulatory options

Following an investigation, the Commissioner may decide to take enforcement action against an entity.

Powers available to the Commissioner include:

- accepting an enforceable undertaking from the respondent under s 114 of the *Regulatory Powers (Standard Provisions) Act 2014.*
- making a determination under s 52 of the Privacy Act, with declarations that the respondent must take specified steps, or that individuals affected by an act or practice are entitled to a specified amount of compensation.
- applying to the court for a civil penalty order under s 82 of the *Regulatory Powers (Standard Provisions) Act 2014*, where a civil penalty provision, such as s 13G of the Privacy Act (a serious and/or repeated interference with privacy) has been contravened.

In each case, the Commissioner considers all of the powers available and proceeds on the basis of exercising powers which will most effectively and efficiently achieve a suitable regulatory outcome, in accordance with the OAIC's Privacy regulatory action policy[9] and Guide to privacy regulatory action.[10]

Note: Brief may require revision prior to Estimates hearing pending any further regulatory developments.

Version: 7	Cleared by: Brenton Attard	Action officer: Brenton Attard
Current at: 13/2/2020	Phone number: 02 9284 9710	Action officer number: 02 9284 9710

[9] Para 38, www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/.

Related backpocket: Nil

HOT TOPIC BRIEF OAIC–02
Consumer Data Right

OAIC

The Consumer Data Right (CDR) seeks to give consumers greater control over how their data is used and disclosed. It will apply in sectors of the Australian economy designated by the Treasurer, allowing consumers to access particular data in a readily usable form and to direct a business to securely transfer that data to an accredited data recipient.

The Office of the Australian Information Commissioner (OAIC) and Australian Competition and Consumer Commission (ACCC) will co-regulate the CDR scheme. The OAIC will be the primary complaint-handler and will have responsibility for overseeing the privacy aspects of the scheme.

- The CDR will allow consumers to access particular data in a usable form, and to direct a business to securely transfer that data to an accredited data recipient. The CDR is not limited to individuals. Businesses will also be able to access and transfer their data under the CDR.
- On 1 August 2019, the *Treasury Laws Amendment (Consumer Data Right) Act 2019* was passed to insert a new Part IVD into the *Competition and Consumer Act 2010* (Competition and Consumer Act) to enact the CDR. The OAIC was consulted throughout the development of the legislation.
- The OAIC has since been working with the ACCC on the implementation of the CDR regime, including by supporting the ACCC in its development of the *Competition and Consumer (Consumer Data Right) Rules 2020* (Rules). The Rules complement Part IVD of the Competition and Consumer Act, including by defining the elements for consent, outlining the accreditation framework, and elaborating on the privacy safeguards.
- The ACCC have formally made the CDR Rules for the banking sector which entered into force on 6 February 2020.
- The OAIC has prepared guidelines on the privacy safeguards to assist industry in interpreting their privacy obligations under the CDR. The OAIC finalised these guidelines following consultation with industry, the ACCC and other key stakeholders. The OAIC published the final version on 24 February, following completion of the consultation with the Treasurer.

- The CDR Data Standards Body, Data61, is developing technical standards to support data sharing under the legislation and the Rules. The OAIC is an observer on the Data Standards Advisory Committee.

Timeline

- The CDR will be rolled out across one sector of the Australian economy at a time. Banking is the first sector to which the CDR applies, where it is called 'Open Banking'.
- The Treasurer formally designated the banking sector on 4 September 2019. The next sector to be designated is the energy sector. Telecommunications is proposed to follow.
- The CDR has a phased implementation in the banking sector. From 1 July 2020, major banks will commence sharing consumer data regarding credit and debit card, deposit account and transaction account data. Consumer data relating to mortgage and personal loan data will be able to be shared after 1 November 2020.
- This timetable was announced by the ACCC on 20 December 2019. Prior to this, major banks were due to commence sharing consumer data in February 2020.

Privacy

- A strong privacy and security framework to protect consumers' information is necessary to maintain the integrity of, and public confidence in, the CDR scheme.
- The Competition and Consumer Act sets out 13 Privacy Safeguards based on the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Privacy Act). The OAIC provided advice to the Treasury on the development of these safeguards.
- Consent is the primary basis upon which CDR data may be handled. The Rules seek to ensure that consent is 'voluntary, express, informed, specific as to purpose, time limited and easily withdrawn'. In addition, consent must not be 'bundled'.
- Small business operators (not normally covered by the Privacy Act) who are accredited to receive data under the CDR scheme will be covered by the Privacy Act in relation to their handling of personal information outside of the CDR regime.

- Treasury undertook a Privacy Impact Assessment (PIA) on the draft legislation between late 2018 and 1 March 2019. An external consultant undertook a second PIA for the full CDR scheme (the legislation, Rules and standards), published 11 December 2019.
- The CDR scheme does not limit the credit reporting provisions in Part IIIA of the Privacy Act.

Regulatory model

- The OAIC will co-regulate the CDR scheme with the ACCC. The responsibilities of each regulator are outlined in the Competition and Consumer Act and the OAIC and ACCC have an MOU to support their working relationship.
- The OAIC will advise and coordinate with the ACCC on privacy aspects of the CDR. In particular, the OAIC will have primary responsibility for the handling of consumer complaints using a 'no wrong-door' approach.
- The OAIC will also have a role in dealing with systemic or serious privacy breaches of the CDR framework, sector designation, the rule-making process, consumer education and reviewing technical standards.
- The OAIC and the ACCC are currently working together on implementation matters, including the development of a system to receive and process CDR matters.

Governance

- In January 2020, Treasury established the CDR Board and the CDR Operational Committee to strengthen accountability for program delivery of the CDR. The Australian Information Commissioner and Deputy Commissioner are members.
- Internally, the OAIC has an internal 'CDR Governance Board' which meets monthly to actively manage a CDR project plan which sets out key deliverables and deadlines. The OAIC also participates in a range of other cross-agency governance fora, including a fortnightly ACCC-OAIC Coordination Committee meeting.

s 47E(d)

s 47E(d)

s 47E(d)

Commissioner brief: NDB overview

Key messages

- The OAIC has moved to publishing six monthly reports – replacing quarterly reports – on the NDB Scheme and published its most recent NDB report on 28 February 2020.
- There has been an increase in the number of NDB notifications received by the OAIC over previous reporting period, but trends across all notifications have been broadly consistent.
- Breaches resulting from malicious or criminal attacks (including cyber attacks) remain the largest source of data breaches (64 percent), with data breaches resulting from human error accounting for 32 percent of all breaches notified to the OAIC.
- The health sector is again the highest reporting sector, accounting for 22 percent of all breaches. The Finance sector is the second highest reporting sector, at 14 percent.

Critical facts

- The OAIC publishes regular statistics on the operation of the scheme. In mid-2019, the OAIC took the decision to move from published quarterly statistics reports to publishing reports every six months. The latest report was published on 28 February 2019.
- From the commencement of the NDB Scheme on 22 February 2018 to 31 December 2019, the Office of the Australian Information Commissioner (OAIC) received a total of 1809 primary notifications of eligible data breaches across all industries.
- Noting that the NDB Scheme only commenced on 22 February, the OAIC received 812 notifications in 2018 and 997 NDB notifications in 2019.[1] Across 2019, there has been a broad increase of NDB Notifications, with an increase of 19 percent in notifications for the period 1 July – 31 December 2019 (537) over the number received for the period 1 January – 30 June 2019 (460). Notifications made under the NDB Scheme remain significantly higher than those made under the earlier voluntary notification scheme, which resulted in 114 notifications for the full 2016-17 financial year.
- During the period 1 July – 31 December 2019, 64 percent of data eligible data breaches reported to the OAIC resulted from malicious or criminal attacks, with 32 percent attributed to human error, and a further 4 percent attributed to system faults.
    - These percentages are broadly consistent with previous periods, but there has been a slight increase in the number of eligible data breaches attributed to malicious or criminal attacks.
- **Further breakdown of NDB notifications during reporting period is outlined on page #**
- For 2019, the OAIC finalised approximately 65% of NDB notifications within 60 days, below the OAIC's KPI of 80% within 60 days.
    - A number of long-standing NDBs were closed during the second-half of 2019, which has impacted on the OAIC's performance against this KPI.
- The OAIC generally finalises notifications on the basis that the entity has complied with the requirements of the NDB scheme and has taken reasonable steps to prevent reoccurrence of the incident. The OAIC may also finalise notifications on the basis that the matter has been escalated to consider as a potential Commissioner initiated investigation.
- Analysis of data breaches conducted by DLA Piper (Global Law Firm) indicate that there have been approximately 161,000 data breaches reported to European data protection authorities from the

[1] This is the number of primary notifications. It does not include secondary notices where more than one entity reports about the same data breach incident. Taken from statistics published in Annual Report.

commencement of the General Data Protection Regulation (GDPR) on 25 May 2018 until 27 January 2020.[2] The Netherlands, Germany and the UK topped the EU member countries in the report with approximately 40,600, 37,600, and 22,200 reported breaches respectively. The UK has also separately reported receiving 2795 reports of data security incidents in the July to September 2019 quarter.[3]

- In comparison to EU member countries and data breach notifications in 2019, Australia ranks 23rd. Australia has had 3.9 notifiable data breaches per 100,000 people in the period from 1 January 2019 to 31 December 2019. This is calculated using Australian Bureau of Statistics data on Australia's population.[4] In comparison, for approximately the same period (28 January 2019 to 27 January 2020) the UK had 17.8 data breaches per 100,000 people, ranking 13th of EU member countries.
- However, this should take into account the exemptions to the OAIC's jurisdiction (such as small business operators, state government), as well as the higher threshold of 'serious harm' in the NDB scheme compared to the requirements for notification under GDPR.
    - Under the GDPR (article 33), a data controller must notify the relevant supervisory authority of a personal data breach within 72 hours unless the personal data breach is *unlikely to result in a risk to the rights and freedoms of natural persons*.
    - Under article 34, the controller must also notify the individual, without undue delay, where a personal data breach is *likely to result in a high risk to the rights and freedoms of natural persons*.
- The OAIC has worked to assist businesses and agencies to comply with the NDB scheme, and to educate the Australian public about the scheme, by:
    - publishing a consolidated data breach preparation and response guide
    - hosting webinars on the requirements of the NDB scheme, and an overview of the first 12 months of the scheme
    - developing information systems to support the scheme, including an online breach reporting tool
    - conducting a number of communications activities and campaigns with a particular focus on the health sector.
    - engaging with stakeholders, including peak industry bodies, members of OAIC's privacy professionals' network and community privacy network, and government agencies.
- The OAIC's priority is ensuring an entity has met the notification requirements of the NDB scheme. If appropriate, the Commissioner also has the power to direct the entity to notify individuals and the OAIC. Additionally, if the Commissioner identifies an interference with privacy as a result of a notification, there are a number of regulatory and enforcement powers available to the Commissioner. Individuals may also complain to the OAIC about an interference with their privacy as a result of a data breach.
    - Where the OAIC becomes aware of additional incidents that may indicate a systemic issue, we will consider appropriate regulatory action in line with the OAIC's *Privacy regulatory action policy*.
- The My Health Record system is subject to different data breach reporting requirements (see D2019/000840).

[2] https://www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020/
[3] ICO 2018, 'Data Security Trends', available at https://ico.org.uk/action-weve-taken/data-security-incident-trends/.
[4] https://www.abs.gov.au/ausstats/abs@.nsf/0/D56C4A3E41586764CA2581A70015893E?Opendocument

Possible questions

Have entities made repeat data breach notifications, and what is the OAIC doing about them?

- Some entities have made more than one data breach notification to the OAIC. During the 2019 calendar year:
  - 80 entities made more than one notification
  - of these, 10 entities make five or more notifications.
- The OAIC reviews the notifications it receives to identify any patterns that may indicate a systemic issue with an entity's privacy practices. This includes consideration of any previous notifications made.
- Depending on the kinds of data breaches an entity notifies, the OAIC may take further action, such as providing targeted advice on personal information security practices or making further inquiries to establish whether to open a Commissioner initiated investigation (CII).
- Across 2019 through to the end of January 2020, the OAIC has opened two Commissioner-initiated investigations into entities from the finance sector. One of these related to an entity that had made several notifications under the NDB scheme, potentially indicating a systemic issue with the entity's personal information handling and security practices. The Commissioner has also made preliminary inquiries with several other entities from across a range of sectors regarding repeat data breach notifications.

What is the OAIC doing about the notifications that it has received from the top reporting sectors?

- The OAIC is working with peak bodies in the health and financial services sector to inform them of the types of matters being notified to the OAIC. For example, the OAIC has jointly developed an action plan with the Australian Digital Health Agency, Australian Cyber Security Centre and Services Australia to help the health sector contain and manage data breaches and implement continued improvement.

How does the OAIC ensure it has been notified of eligible data breaches?

- The OAIC may become aware of data breaches through a number of different channels, including referrals from members of the public, privacy complaints, media reports or social media commentary, or from other regulators.
- Where the OAIC becomes aware of a potentially eligible data breach that has not been notified to it, the OAIC may make enquiries with the entity about whether it is completing, or has completed, an assessment of whether the data breach is likely to result in serious harm to affected individuals. In some instances, the entity may commence notification following contact from the OAIC, or may otherwise advise they are still completing an assessment of the data breach.
- In instances where the OAIC disagrees with the entity about its assessment of whether the data breach is notifiable, the Commissioner has the power to direct the entity to notify individuals and the OAIC. The Commissioner has issued one direction to notify to a data base operator.

Should the data breach scheme be reviewed for the kinds of breaches that are required to be reported or the timeframe in which entities are required to notify?

- The OAIC considers it good practice to periodically review the implementation of legislative schemes to ensure they meet their intended objective.
- Now that the NDB scheme has been operating for two years, we are in a better position to identify and analyse patters and trends in notifications, including across industries and in relation to sources of breaches.

- The Australian law came into operation before the GDPR and has some important differences. One is that the threshold for reporting to the regulator under the GDPR is lower, and the time frame for reporting is 72 hours.
- Under the GDPR (article 33), a controller must notify the relevant supervisory authority of a personal data breach within 72 hours unless the personal data breach is ***unlikely to result in a risk*** *to the rights and freedoms of natural persons.*
- Under article 34, the controller must also notify the individual, without undue delay, where a personal data breach is ***likely to result in a high risk*** *to the rights and freedoms of natural persons.*
- In Australia, notification must occur to both the OAIC and affected individuals where a breach occurs and a reasonable person would conclude it is ***likely to result in serious harm*** to any of the individuals whose personal information was involved in the data breach, and the ***entity has not been able to prevent the likelihood of serious harm through remedial action***.
- Also the Australian law allows entities to assess whether a suspected breach has in fact occurred and whether it meets the test.
- If an entity suspects that an eligible data breach has occurred, they must undertake an assessment into the relevant circumstances. The entity must take all reasonable steps to complete this within 30 calendar days (s 26WH (2)(b)).
- The Australian law was drafted to allow this assessment time, and to expressly provide that if remedial action prevents the likelihood of serious harm, it is not notifiable. The advantage is that the law seeks to address more serious matters, and the risk of notification fatigue by individuals is reduced. It does however mean that there are different tests for global entities to comply with.
- Where there is proposed or draft legislation that impacts or has relevance to the Privacy Act or handling of personal information, the OAIC will make a submission to provide input or comment on the proposed changes. If this were the case, the OAIC would welcome this opportunity and provide information about the OAIC's role and if appropriate, make recommendations based on the OAIC's experience.

Why isn't the OAIC publishing notifications it has received?

- The NDB scheme does not provide the OAIC with the power to publish notifications. The OAIC's view is that the non-disclosure provisions in the *Australian Information Commissioner Act 2010* (Cth) and the *Privacy Act 1988* (Cth) prevent the proactive publication or disclosure of the details of data breach notifications received under the NDB scheme.[5] The OAIC's view is that the publication of individual notifications cannot occur without legislative change
- The OAIC is publishing regular statistical information about the NDB notifications to assist entities and the public in understanding the operation of the scheme, to illustrate the patterns observed from the notifications being reported to the OAIC, and to highlight the learnings that the NDB scheme has to offer. Using statistical reporting is consistent with the approach taken by comparable data protection authorities in the European Union.[6]
- The OAIC reviewed its publication approach after the first 12 months of the NDB scheme's operation. Given the trends identified in the quarterly reports have remained consistent over the first 12 months, the OAIC decided to move from quarterly to biannual reporting. The OAIC considers that the approach achieves the same objectives of informing government, industry and the public on the operation of the scheme, as well as remaining consistent with international approaches to reporting on mandatory or voluntary data breach notification schemes.

[5] However some information may be released under FOI.
[6] Which either do not publish any information about data breach notifications or publish statistics or general information about data breaches without naming the specific entity involved

Are NDBs being addressed in a timely fashion?

- The OAIC acknowledges each NDB upon receipt. The OAIC monitors matters as they are notified and may choose to prioritise certain NDBs that require immediate attention.

Is the NDB Scheme serving its primary purpose?

- Under the Notifiable Data Breaches (NDB) scheme, entities are required to notify individuals and the OAIC when they experience a data breach that is likely to result in serious harm to any individuals whose personal information is involved in the breach.
- The NDB scheme strengthens the protections afforded to everyone's personal information and improves transparency in the way agencies and organisations respond to serious data breaches.
- This supports greater community confidence that personal information is being protected and respected and encourages a higher standard of personal information security by entities subject to the scheme.
- Notification also provides individuals with the opportunity to take steps to minimise the harm that can result from a data breach, such as by changing passwords or notifying their financial institution.

Is the OAIC concerned that the health sector is the top sector notifying data breaches?

- This trend is similar to reporting trends in overseas jurisdictions. For example, the January 2019 Dutch Data Protection Authority report indicated the health and wellbeing sector was the top sector (29%), and UK Information Commissioner's Office statistics for the July to September quarter of 2019 indicated the health sector was the largest notifier (19%).
- This may be a combination of a number of factors, for instance, the size of sector. In Australia, the Health Sector includes GPs, specialists and private hospitals, as well as any other organisation, regardless of size, that provides a health service, even where that is not the main function of the organisation, such as a gym or child care centre. Additionally, the sensitivity of the information held by the health sector may contribute to more assessments that a data breach is likely to result in serious harm to the affected individuals.

Have you penalised anyone for non-compliance with the scheme?

- The OAIC has focussed on offering advice and guidance to regulated entities and encouraging and facilitating compliance with the scheme.
- If the OAIC identifies serious or repeated non-compliance with the assessment and notification requirements of the NDB scheme, the OAIC has a range of regulatory options available to it to pursue non-compliance.
- As of 31 December 2019, the Commissioner has issued one direction under s 26WR(1) for an organisation to notify individuals of an eligible data breach. The OAIC became aware of the eligible data breach via a referral from a law enforcement body. The respondent complied fully with two of the requirements of the direction but potentially not with another four requirements.

  The Commissioner has a range of options to enforce a direction to notify, which includes seeking an injunction in the Federal Court requiring the organisation to comply with the direction.

Does the OAIC need additional resources and capacity to investigate data breaches?

- The OAIC is given a general appropriation to cover all its activities. It is the Information Commissioner's role to decide how to use that appropriation. The OAIC has not received specific funding for the NDB scheme. OAIC internally funds this from existing appropriation.
- Where additional functions are conferred on the OAIC, the Commissioner endeavours to find ways to run existing functions more efficiently. The OAIC is constantly refining its processes to identify opportunities to run more efficiently.

- If volumes of notifications continue or increase, this will likely impact on timeframes and may influence proactive regulatory activity.

What is the OAIC doing to publicise the NDB scheme?

- Through its website, the OAIC provides detailed advice for regulated entities on how to secure personal information and prevent and respond to data breaches. It also provides advice for individuals about protecting their personal information online.
- The OAIC also works with the Australian Cyber Security Centre (ACSC) to raise awareness about the prevention of data breaches caused by malicious or criminal attack. This includes promoting a joint resource for businesses and agencies on how to prevent data breaches caused by such an attack.
- The OAIC is a major partner in Stay Smart Online Week, working with the ACSC and other organisations to advise the public, business and Australian Government agencies on how to manage cybersecurity risks. It is also a member of the Australian Competition and Consumer Commission's (ACCC) Scams Awareness Network and actively promotes Scams Awareness Week as an opportunity to highlight risks to personal information security, including cyberattacks.
- Advice on protecting individuals, organisations and agencies from malicious or criminal cyberattacks is also provided through the OAIC's participation in webinars, speeches and other events focused on the Notifiable Data Breaches scheme.
- The OAIC continues to collaborate with the ACSC, ACCC, eSafety Commissioner and other Australian Government agencies to promote awareness of data protection issues through regular campaigns and new awareness activities. Protecting personal information online will again feature as a key theme of Privacy Awareness Week 2020.

Other background: NDB Test

- The NDB scheme commenced on 22 February 2018 and applies to entities that have existing personal information security obligations under the Privacy Act.
- Under the NDB scheme a data breach is an 'eligible data breach' where:
    - there is unauthorised access to or unauthorised disclosure of personal information (or the information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur)
    - a reasonable person would conclude it is likely to result in serious harm to any of the individuals whose personal information was involved in the data breach, and
    - the entity has not been able to prevent the likelihood of serious harm through remedial action.
- If an entity suspects that an eligible data breach has occurred, they must undertake an assessment into the relevant circumstances. The entity must take all reasonable steps to complete this within 30 calendar days (s 26WH (2)(b)).

If an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach, they must notify affected individuals and the OAIC as soon as practicable (unless an exception applies).

Key statistics on data breach notifications – July to December 2019

1. Number of people affected by data breach

Number of Individuals affected by data breaches	Number of breaches
Unknown	18
1	132
2 - 10	85
11 - 100	103
101 - 1000	121
10 000 001 or more	1
100 001 - 250 000	2
10001 - 25000	12
5001 - 10000	11
5 0001 - 10 0000	4
1001 - 5 000	41
25001 - 50000	5
1 000 001 - 10 000 000[7]	2
Grand Total	**537**

2. Types of personal information involved in data breach

Type of Personal Information involved in Data Breach	Number	Percentage
Contact information	411	77%
Financial details	198	37%
Identity Information	162	30%
Health information	125	23%
TFN	83	15%
Other sensitive information	38	7%

[7] The two breaches with more than 1 million affected individuals were Sephora (a cosmetics retailer) and Malindo Air

3. Top Five Reporting Sectors by Source of Breach

	Source of Data Breach			
Industry Sector	**Human Error**	**Malicious or Criminal Attack**	**System Fault**	**Total**
Health service providers	51	63	3	117
Finance	30	40	7	77
Education	16	30	3	49
Legal, Accounting & Management services	10	30	0	40
Personal services	8	14	1	23
Grand Total	**115**	**177**	**14**	**306**

Data breach notifications of interest

The OAIC does not generally publicly comment on specific details relating to ongoing processing of data breach notifications, or privacy CII investigations or inquiries.

The below table provides a summary of the status on matters that the OAIC has made a public statement about, or it is otherwise publicly known that the entity has notified the OAIC of the data breach.

Respondent	Description	Date OAIC notified/aware	Status (investigation/inquiries)
PageUp People Limited	Data breach caused by a cyber incident	June 2018	Closed Date of OAIC statement: 18 June 2018
Facebook	Security incident involving access tokens	September 2018	**Closed.** Date of OAIC statement: 29 September 2018
Google	Bug that allowed access to Google+ Profile data	October 2018	Preliminary inquiries OAIC media statement made, confirming inquiries[8]

s 47E(d)

[redacted]

[8] https://which-50.com/google-to-be-permanently-shut-down-following-major-data-breach/
[9] https://news.cathaypacific.com/cathay-pacific-announces-data-security-event-affecting-passenger-data
[10] http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/
[11] https://www.lmw.com.au/about-lmw/news-updates/data-disclosure-incident/

Document history

Updated by	Reason	Approved by	Date
Connor Dilleen	For March 2020 Estimates		

Commissioner brief: Summary of High Profile NDBs

Key messages

- Throughout 2019 there has been sustained media interest in reporting data breaches, ensuring that many Australian businesses experiencing a data breach have been in the public eye.
- Most of the breaches that received significant media coverage in the last twelve months resulted from malicious or criminal attacks, consistent with statistics for all notifications of eligible data breaches received by the OAIC.
- In a number of instances, the company experiencing the data breach initiated media coverage by proactively issuing a public statement.
- These public statements typically followed formal notification to individuals potentially affected by the breach and to the OAIC, as required by the NDB Scheme.
- Media coverage of data breaches has helped build public awareness of privacy rights and issues and can also help consumers understand the risks associated with putting information online and the steps that they can take to protect themselves.

Critical facts

High Profile NDBs from 2019

Entity	Description	Date of Breach	OAIC Action Taken	Public status
s 47E(d)	[redacted]			

Entity	Description	Date of Breach	OAIC Action Taken	Public status
s 47E(d)				

Entity	Description	Date of Breach	OAIC Action Taken	Public status
s 47E(d)	[redacted]			

Possible questions

How does the OAIC ensure it has been notified of all high profile eligible data breaches? (from NDB Overview brief)

- The OAIC may become aware of data breaches through a number of different channels, including referrals from members of the public, privacy complaints, media reports or social media commentary, or from other regulators.
- Where the OAIC becomes aware of a potentially eligible data breach that has not been notified to it, the OAIC may make enquiries with the entity about whether it is completing, or has completed, an assessment of whether the data breach is likely to result in serious harm to affected individuals. In some instances, the entity may commence notification following contact from the OAIC, or may otherwise advise they are still completing an assessment of the data breach.
- In instances where the OAIC disagrees with the entity about its assessment of whether the data breach is notifiable, the Commissioner has the power to direct the entity to notify individuals and the OAIC. The Commissioner has issued one direction to notify to a data base operator.

Has the OAIC received NDB notifications for all high profile data breaches reported in the media?

- The OAIC does not generally make public statements on the details of data breach notifications that we have received, regardless of whether the data breach in questions has received media coverage.
- In some instances, the business experiencing the data breach has made a public statement that it has notified the OAIC.
- The OAIC will confirm that it has been advised of a data breach in certain circumstances, with the view that this increases public confidence in the process.
- The OAIC's view is that the non-disclosure provisions in the *Australian Information Commissioner Act 2010* (Cth) and the *Privacy Act 1988* (Cth) prevent the proactive publication or disclosure of the details of data breach notifications received under the NDB scheme.[2] The OAIC's view is that the publication of individual notifications cannot occur without legislative change.
- The OAIC seeks to provide visibility of eligible data breach notifications that we receive under the NDB scheme by publishing regular statistical information about the NDB notifications. These reports are intended to assist entities and the public in understanding the operation of the scheme, to illustrate the patterns observed from the notifications being reported to the OAIC, and to highlight the learnings that the NDB scheme has to offer.

Other

- The Strategic Communications team and members of the NDB and CII teams actively monitor media reporting on data breaches and typically cross-reference high-profile breaches with notifications received.
- The Strategic Communications team also coordinates a daily 'Media Stand-up' in which relevant media reporting on data breaches is reviewed.
    - This 'Media Stand-up' involves staff from the NDB, CII and Enquiries teams.
    - It can also result in tasking the investigations teams for initial inquiries with the affected entity when the relevant data breach has not yet been the subject of a formal (or informal) breach notification to the OAIC.

[2] However some information may be released under FOI.

Document history

Updated by	Reason	Approved by	Date
Name Connor Dilleen	March 2020 Senate Estimates	Rocelle Ago	

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

Key messages

- The OAIC is committed to ensuring that all public statements on its privacy regulatory action are accurate, fair and balanced, and comply with the OAIC's legal obligations with regards to privacy, confidentiality, and secrecy. Therefore, the OAIC generally does not comment publicly on the specifics of Commissioner initiated inquiries or investigations until the investigation has been finalised.[1]
- The OAIC currently has 25 Commissioner initiated preliminary inquiries or investigations open, including privacy incidents that have attracted media interest or public concern. [*at 7 Feb 2020*]
- The OAIC handles these matters in accordance with the OAIC's *Privacy regulatory action policy*[2] and *Guide to privacy regulatory action.*[3]

Critical facts

- The Commissioner may make inquiries under s 42(2) of any person for the purposes of determining whether to investigate an act or practice under s 40(2) of the *Privacy Act 1988* (Cth) (the Privacy Act).
- Under s 40(2) of the Privacy Act, the Commissioner may, on the Commissioner's own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of Australian Privacy Principle 1, where the Commissioner thinks it is desirable that the act or practice be investigated.
- When considering whether to investigate an act or practice under s 40(2), the Commissioner has regard to the factors outlined in paragraph 38 of our *Privacy regulatory action policy.*[4] These factors include:
    - the seriousness of the incident or conduct to be investigated
    - the specific and general educational, deterrent or precedential value of the particular privacy regulatory action
    - whether the conduct is an isolated instance, or whether it indicates a potential systemic issue
    - the level of public interest or concern relating to the conduct, proposal or activity.
- Where a particular privacy incident is of community concern and has already been reported in the media, the OAIC may confirm publicly that it is investigating or making inquiries in relation to a matter.
- The OAIC may also comment publicly on a particular privacy incident where there is a public interest in doing so, for example to enable members of the public to respond to a data breach.
- The OAIC seeks to work in partnership with other data protection authorities where there is a shared interest in working together to address privacy breaches, threats and risks. The OAIC has found that a coordinated and consistent global response can be an effective regulatory response to a global privacy issue.

[1] *Privacy regulatory action policy.* Paragraphs [53] - [59]. https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/#public-communication-as-part-of-privacy-regulatory-action
[2] Paragraphs [34]-[38]. https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/#selecting-appropriate-privacy-regulatory-action
[3] Chapter 2: Commissioner initiated investigations and referrals. https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-2-commissioner-initiated-investigations-and-referrals
[4] Paragraphs [34]-[38]. https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/#selecting-appropriate-privacy-regulatory-action

Possible questions

What are the OAIC's KPIs for conducting privacy Commissioner initiated investigations?

- The OAIC has a KPI of finalising 80% of privacy CIIs within 8 months.
    - The OAIC conducted preliminary inquiries or opened investigations into 8 matters in 2018-19.
    - In 2018-19 , the OAIC closed 86% of CIIs within eight months an increase compared to 72% in 2017-18.
    - Two preliminary inquiries were closed within 2018-19, both within 8 months of commencement. No CIIs were closed within that period.

What enforcement action can the OAIC take as a result of a privacy CII?

- The *Guide to privacy regulatory action* refers to a range of outcomes that include:
    - **discontinuing** a CII where the Commissioner is satisfied that no breach has occurred or that the breach has been adequately dealt with by the respondent and no further action is warranted
    - **accepting an enforceable undertaking** from the respondent, whereby the respondent agrees to take specific action in order to comply with the Privacy Act
    - **making an enforceable determination**, declaring that a respondent must take specified steps within a specified period to ensure the respondent's ongoing compliance with the Privacy Act
    - applying to the court for a **civil penalty order**
    - **reporting** an act or practice that interferes with the Privacy Act to the relevant Minister.

What are some examples of enforcement action that the OAIC has taken?

- On 28 June 2019, the OAIC accepted an enforceable undertaking from Wilson Asset Management (International) Pty Limited (WAMI) to address the concerns identified in the OAIC's investigation commenced in April 2019. As part of the undertaking, WAMI advised it ceased to have access to stoptheretirementtax website from 22 February 2019 and will destroy the personal information it collected from the website's database.[5]
- On the 27 June 2019, the OAIC accepted an enforceable undertaking from the Commonwealth Bank of Australia (CBA) as a result of the OAIC's preliminary inquiries into data incidents involving the loss of two magnetic data tapes and data access issues which indicated deficiencies in CBA's management of personal information. As part of the undertaking, CBA must develop and submit to the OAIC a work plan and timeframe to address its privacy obligations, including a review of its policies and procedures to ensure compliance.[6]
- In March 2018, the OAIC accepted an enforceable undertaking from the Department of Health, after a dataset was published online for third-party research purposes. This required an independent external review of the Department's policies and procedures for compliance with the Privacy Act, and a follow up audit and report on the adequacy of the Department's implementation and response to any recommendations made.[7]

[5] https://www.oaic.gov.au/privacy/privacy-decisions/enforceable-undertakings/wilson-asset-management-enforceable-undertaking/
[6] https://www.oaic.gov.au/privacy/privacy-decisions/enforceable-undertakings/commonwealth-bank-of-australia-enforceable-undertaking/#s2-background
[7] https://www.oaic.gov.au/privacy-law/enforceable-undertakings/department-of-health-enforceable-undertaking

- In 2017, the OAIC also accepted an enforceable undertaking from the Australian Red Cross Blood Service following a data breach. Red Cross undertook to review its compliance with, and the effectiveness of, its third party management policy and operating procedure within a six month period.[8]
- In 2016, the OAIC accepted an enforceable undertaking from Avid Life Media Inc. (ALM) following a joint investigation with the Office of the Privacy Commissioner of Canada into the 'Ashley Madison' data breach. ALM undertook to review its personal information practices, implement and document an augmented information security framework, and provide the OAIC with a report from an independent third party confirming its compliance.[9]

Current Enforceable Undertakings

Respondent	Date Accepted	Reports Required	Status

s 47E(d)

[redacted]

[8] https://www.oaic.gov.au/privacy-law/enforceable-undertakings/australian-red-cross-blood-service-enforceable-undertaking
[9] https://www.oaic.gov.au/privacy-law/enforceable-undertakings/avid-life-media-enforceable-undertaking

Has the Commissioner ever used the power to apply to the court for a civil penalty?

- No. The Commissioner has not yet taken action to apply to the court for a civil penalty.
- The amendments to the Privacy Act from 12 March 2014 introduced a civil penalty (up to $2.1m for corporations) if an entity does an act, or engages in a practice, that is a serious or repeated interference with privacy (s 13G).
- The OAIC applies its resources strategically, and will take regulatory action where appropriate.
- The OAIC will not shy away from the use of our full range of regulatory powers for appropriate matters, and that includes seeking civil penalties in appropriate circumstances.

Summary table of key CIIs

While the OAIC's Commissioner initiated investigations or inquiries are ongoing, the OAIC does not publicly comment on specific details. The below table provides a summary of the status on matters that the OAIC has made a public statement about. Once the investigation has concluded a further statement will be published.

Respondent	Description	Date OAIC became aware	Date OAIC opened inv/inquiries	Status (investigation/inquiries)
Privacy Commissioner Initiated Investigations				
s 47E(d) [redacted]				
The Cosmetic Institute	Disclosure of personal information on website which included medical forms and images.	3 June 2017	6 June 2017	Investigation opened in relation to data breach. Statement on website: 18 Aug 2017
Flight Centre	Disclosure of personal information to IT developers	July 2017	15 August 2017	Investigation Statement on website: 18 Aug 2017
Uber	Data breach in 2016 affecting driver and rider data	November 2017	18 December 2017	Investigation Statement on website: 22 Nov 2017

Respondent	Description	Date OAIC became aware	Date OAIC opened inv/inquiries	Status (investigation/inquiries)
Facebook (see Hot Topic brief D2020/000709)	Disclosure of Facebook data to Cambridge Analytica	17 March 2018	5 April 2018	Investigation Statement on website: 5 Apr2018
Aussie Farms Inc	Prescribed as an organisation on 6 April 2019	5 April 2019	Preliminary inquiries: 6 April 2019 CII: 19 November 2019	Investigation. Statement 19 November 2019
Privacy CII - Preliminary inquiries				
Google Inc.	Collection of location data from Android mobile devices	May 2018	14 May 2018	Preliminary inquiries Statement on website: 14 May 2018

s 47E(d)

[redacted]

Document history			
Updated by	**Reason**	**Approved by**	**Date**
Michael Foot / Sophie Higgins	March 2020 Senate Estimates		

Commissioner brief: Health sector issues

Key messages

- Notifiable Data Breaches
- From the commencement of the Notifiable Data Breaches (NDB) scheme on 1 July 2018 to 31 December 2019, the health sector has accounted for approximately 21% of notifications (310notifications). This represents an increase in the percentage of matters notified by the health sector under the voluntary scheme prior to the introduction of a mandatory scheme (7% of notifications in 2016-17).
- The health sector has consistently notified the highest volume of data breaches to the OAIC for each quarter since the scheme commenced. The sector includes any private provider of health services, regardless of annual turnover. This includes private hospitals, GPs, specialists and allied health professionals, dentists, aged care facilities, ambulance services, gyms and pathologists.
- In the first half of 2019-20, malicious/criminal attacks overtook human error as the leading cause of data breaches reported under the NDB scheme for the health sector. There was an increase from 46% to 54%, as compared to the previous 6 months.
- Where the OAIC is made aware of particular incidents or repeated conduct that may indicate a systemic issue, the OAIC will consider appropriate regulatory action in line with its *Privacy regulatory action policy*. The OAIC does not generally comment on ongoing inquiries or investigations.
- The OAIC is also working with key regulators, Australian Government agencies and peak bodies in the health sector to inform them of the types of matters being notified to the OAIC and positive steps participants in the industry can take to improve their security and other personal information handling practices. This includes speaking at industry conferences and publishing the September 2019 Guide to Health Privacy to assist health service providers comply with their privacy obligations and embed best practice.
- Complaints
- The OAIC received 163 complaints about health service providers in the first half of 2019-20. This is consistent with the number of complaints received for 2018-19 financial year (328), and 2017-18 (321).
- Health service providers are the third highest ranked sector for privacy complaints for 2019-20, is consistent with 2018-19.

Critical facts

- The private health sector accounts for about one in five of all data breaches notified to the OAIC under the NDB scheme. This sector does not include state health service providers, which may have obligations under relevant state legislation.
- The NDB scheme 12-month insights report published in mid-2019 indicated that human error was the leading cause of data breaches in the health sector—accounting for 55 per cent of data breaches between 1 April 2018 to 31 March 2019, compared with an average of 35 per cent for all other sectors. Personal information sent to the wrong recipient was the most common human error breach in the health sector, whether by email, mail or other forms of communication.
- However, statistics from the period 1 July – 31 December 2019 indicate that malicious or criminal attacks now account for 54% of all eligible data breach notifications from the health sector, a significant increase from the 46% for the previous six months.

- The health sector's position as a leading reporter of data breaches has so far been consistent with international trends. Jurisdictions with mandatory data breach reporting for the health sector have also seen a high level of notifications, most notably the United Kingdom and the Netherlands.

NDB scheme statistics for the health sector

	1 July –31 December 2018	1 January – 30 June 2019	1 July – 31 December 2019	Total
Notifications from the health sector	20% (99)	26% (105)	22% (117)	321
Total NDBs for period	507	460	537	1504

Source of Breach	1 July –31 December 2018	1 January – 30 June 2019	1 July – 31 December 2019
Malicious/criminal attack	44% (44)	46% (48)	54% (63)
Human error	55% (54)	52% (55)	44% (51)
System fault	1% (1)	2% (2)	2% (3)
Total health NDBs	99	105	117

Other regulatory action

s 47E(d)

[redacted]

Possible questions

What is the OAIC doing to address the number of notifications being received from the health sector?

- The OAIC handles all notifications from the health sector in accordance with the requirements of Part IIIC of the Act. Since the commencement of the Notifiable Data Breaches scheme the OAIC has worked with health service providers to ensure health sector entities are complying with the scheme. This has included:
    - Joint webinar with the Royal Australian College of General Practitioners
    - Panel discussion at the Australian Private Hospitals Association (APHA) 38th National Congress
    - Speech at Medial Software Industry Association (MSIA) 2018 Summit

- Speech at Australian Association of Practice Management (AAPM) 2018 Conference

- In September 2019 the OAIC also launched a new Guide to Health Privacy. The Guide brings together and updates a wide range of guidance from the OAIC to help health service providers safeguard their patients' personal information. This will assist health service providers covered by the Privacy Act 1988 to better understand their privacy obligations and embed good privacy principles throughout their practice. It outlines accessible, step-by-step strategies to ensure patient and client privacy is protected. It also includes practical advice for obtaining consent for the collection, use and disclosure of personal information and managing it securely throughout the information life cycle.

Document history

Updated by	Reason	Approved by	Date
Michael Foot	March 2020 Senate Estimates		

Commissioner brief: Complaint backlog strategy

Key messages

- In 2019, the OAIC was provided with an additional $25 million over 3 years to strengthen protections to personal information.
- The OAIC took a three-pronged approach, focusing on the processes around new incoming complaints, the older complaints awaiting investigation, conciliation, and the matters awaiting determination by the Commissioner.
- In the first 3 months of this project the OAIC:
    - closed 905 complaints, a 48% increase in the number of complaints closed for the same period in 2018-2019
    - reduced the overall numbers of complaints awaiting actioning by the two privacy complaint teams
    - referred 24 complaints for consideration of determination.

Critical facts

- Over the last few years the OAIC has experienced a steady increase in the number of complaints received. This, coupled with limited resourcing and staffing levels, resulted in an increase and backlog of complaints waiting to be allocated to an investigation officer.
- The length of time complaints awaiting allocation to an investigation officer increased to over 12 months.
- 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 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 separate out different 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 an 8-week timeframe for completion of an investigation where early resolution was not successful
    - substantially increasing the volume of conciliations conducted to reach a resolution by agreement between the parties
    - providing additional resources to assist with the determination of matters where appropriate.
- During the first 3 months of the backlog project (4 November 2019 – 31 Jan 2020) the OAIC closed 905 complaints – which compared to the same period the last year (609 complaints) is an increase of 296 complaints, or a 48% increase.

- We have also seen further increases in the numbers of complaints finalised from the beginning of this financial year, 1 July 2019, when the teams began preparing for the Backlog Project. In the 2017-18 financial year, the monthly average number of complaints closed was 230.5, which increased to 243.25 in the 2018-19 financial year, and from 1 July 2019 to 31 January 2020 alone, the average is 300.1 complaints closed per month.

Information about the Early Resolutions Team's project

- The Early Resolution (ER) team ran a 3-month backlog project that commenced on 1 November 2019 and ended on 31 January 2020.
- The ER Team reviewed its current work in progress and drew a line in the sand, setting aside any complaint received before 25 October 2019 and placing 324 matters in a 'backlog' queue. The oldest matter in the backlog queue was received on 17 July 2019 (just over four months old).
- The ER Team engaged 3 FTE contractors to replace three officers in the Privacy ER Team, as those officers stepped out of the team to form the ER Backlog Team. The total cost of these 3 contractors was $114,101.63 (inc gst).
- Of the 324 matters in the backlog queue at 1 November, 119 were unassessed, meaning an officer had not yet reviewed the matter, and the remaining 205 were assessed, meaning a senior officer had reviewed the matter, identified the relevant issues and the action the OAIC was to take.
- At the end of the project, there were only 64 matters that had not been finalised in the ER process. 33 matters went to the Investigations/CII team and 226 were closed. All of the remaining matters had been actioned and have been or will be finalised in coming weeks.
- The team took a strategic approach to the problem which included having a small team in a separate space focus only on the backlog, batching complaints and administrative improvements that made issues easier to identify. They also improved templates, tightened timeframes and streamlined processes.
- When the backlog project began, the ER team had 60 matters for action (37 unassessed meetings and 23 assessed), all of which had been received within one week. As at 27 February 2020, the ER team has 133 matters awaiting action, 85 of which are assessed and 48 are unassessed, with the oldest matter awaiting just over 1 month old.
- The waiting times for allocation have significantly improved. Before this project started the oldest matter awaiting allocation was just over four months old and this has been reduced to being just over two months old.

DR Conciliation and Investigations team's results

- The DR Conciliations and Investigation team has been running its backlog project since 4 November 2019. Backlog numbers have been reduced, all matters awaiting allocation have been assessed and it is anticipated that the backlog of 639 at 1 July 2019 will be reduced by end April 2020.
- Prior to the commencement of the backlog project, the team reviewed and amended its processes for the conciliation and investigation of matters, and appointed 4 new FTE contractors, to fill vacant positions. A number of outstanding privacy complaint matters were also referred in from other teams.
- In the first phase of the project the team focussed on reviewing older more complex matters, preparing current matters for investigation and investigating and conciliating matters to a new 8-week time frame.

- For the second phase the team moved to a full conciliation model, where conciliation is attempted prior to opening an investigation, with anticipated closures based on a 72% resolution rate.
- By early February 2020 all matters in the PRV intake queue had been assessed and either moved to a Conciliations queue for listing or to an Investigations queue for assessment for determination, finalisation or investigation as appropriate.
- On 1 July 2019, the total backlog for the DR Conciliations and Investigation team was 639 matters with 367 matters awaiting allocation to 11 case officers and 3 matters assessed for determination by the Commissioner.
- Results as at 4 November 2019 - the commencement of the backlog project:
    - Matters in Allocations PRV queue (intake from ER) 359
    - Matters under investigation (10 Investigation officers including 2 part-time) 168
    - Total backlog 527
    - Of the 527 backlog 9 matters had been assessed for determination
- Results as at 17 January 2020 – end phase 1:
    - Matters in Allocations PRV queue (intake from ER) 354
    - Matters under investigation (13 Investigation officers including 2 part-time) 124
    - Total backlog 478
    - Of the 478 backlog matters 26 had been assessed for determination
- Results as at 2 March 2020 – mid phase 2:
    - Matters in Allocations PRV queue (intake from ER) 0
    - Matters in conciliation (3 officers and 3 contractors) 143
    - Matters to be assessed for investigation, determination or close 20
    - Matters under investigation (10 Investigation officers including 2 part-time) 188
    - 26 matters have been assessed for determination
- Four team members are trained conciliators and 3 have been dedicated to conciliations. One part-time team member has been dedicated to scheduling conciliations and one officer has been deployed to manage the conciliation queue and one to manage the investigation queue. These officers now have nil or reduced case loads.
- The listing capacity is 6 matters per day by team conciliators (3 conciliators undertaking 2 conciliations per day). Additional external contractors are being engaged on a per diem basis to conciliate a further 3 matters per day each.
- In the period February to March 2020, 98 matters have been listed for conciliation.
- In the period from 4 November 2019 to end January 2020 (12 weeks) 16 conciliations were conducted by the team with 12 matters successfully resolved, equating to a 75% resolution rate.
- In the second phase, from 3-28 February 2020, (4 weeks) 21 matters were conciliated with 16 resolved giving a resolution rate of 76.5%. This figure demonstrates a 400% increase in conciliations compared with the average for any of the three previous months and an increasing resolution rate.
- Of the 143 matters remaining in the Conciliation queue as at end February 2020, 73 are listed for conciliation and the remainder await a listing date likely to be listed in March-April. In this way the

conciliation backlog will have been removed and the team will from there on be listing matters as they come in from ER (rather than from backlog allocations).

- It is anticipated that by end March-April 2020, all remaining current matters in the Conciliation queue will have been listed.
- As successful resolutions equate with immediate closure of matters, the substantial increase in conciliations also boosts closure rates. In the period from 1 July 2019 to December 2019, the average closure rate was 61 matters per month and in January 2020, the team closed 33 matters, whereas at 27 February 2020, the team had closed 128 matters.

Information about the Determinations Team's approach

- The Determinations Team (DT) is comprised of one EL2 FTE and 1.5 FT contractors. It was established in October 2019, for commencement 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 to make a determination.
- DT also uses powers under s 44 of the Privacy Act to complete investigations as required and provides advice to investigations officers on evidence gathering.
- The DT has established new processes and templates to support this function.
- DT has drafted seven PVs. Submissions have been received in two matters.

Possible questions

- ***Has the backlog project been successful?***

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

  We have also seen an increase in the numbers of complaints resolved from the beginning of this financial year, 1 July 2019, when the teams began preparing for the Backlog Project. In the 2017-18 financial year, the monthly average of complaints closed was 230.5, which increased to 243.25 in the 2018-19 financial year, and from 1 July 2019 to 31 January 2020 alone, the average is 300.1 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.

- ***Has the average time taken to close a complaint improved from the Backlog Project?***

  For the period 4 November 2019 to 31 January 2020, the average time taken to close a complaint was 132 days, or 4.3 months. This is 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.

- ***What is the current average time taken to close a complaint?***

From 1 July 2019 to 31 January 2019, we are tracking at an average of 4.8 months taken to close a complaint. In the 2018 – 2019 financial year, the average time taken to close a complaint was 4.4 months.

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

  The waiting times for allocation have improved in the Early Resolution space, as before the backlog project the oldest matter awaiting allocation was just over 4 months old, and as at 6 February 2020 the oldest matter awaiting allocation is just over 1 month old.

  In the Conciliations and Investigation space, all matters awaiting allocation have been assessed. Complainants have either had their matter listed for conciliation or have been contacted in the last month to confirm the status of their complaint and discuss next steps in the resolution of the matter

Key dates

- Backlog project commenced on 4 November 2019
- The Early Resolution team ran a 3 month backlog project that commenced 31 January 2020.
- 28 January 2020 the DR Conciliations & Investigation team began working on the conciliation focussed model that is now in place.

Document history

Updated by	Reason	Approved by	Date
Cecilia Rice / Riki Jamieson-Smyth	March 2020 Senate Estimates	Name	

Commissioner brief: Assessments program 2018-19 and 2019-20

Key messages

- The OAIC has a program of privacy assessments (or audits) to identify privacy risks in key projects where agencies and organisations handle personal information. Where risks are identified, we make recommendations to address them.
- Focus areas for assessments the 2018-19 financial year included digital health, government data matching programs, and telecommunications service providers' processes under the data retention scheme.
- We have 13 privacy assessments open currently: four started this financial year, and the rest carrying over from previous financial years. We plan to begin assessments in several more areas of interest as 2019-20 progresses.
- Assessments for the 2019-20 financial year, including those required under memoranda of understanding with government agencies, will focus on finance and digital health, border clearance processes, as well as initiatives like the Australian Government Agencies Privacy Code and Notifiable Data Breaches Scheme.

Critical facts

- Section 33C of the Privacy Act empowers the Commissioner (or delegate) to conduct an assessment of whether personal information held by an APP entity is being maintained and handled in accordance with the APPs, a registered APP Code or a small number of certain other provisions. The Commissioner may conduct an assessment in such manner as the Commissioner sees fit.
- They way in which OAIC staff exercise the Commissioner's assessment power is set out in Chapter 7 of the OAIC's *Guide to privacy regulatory action*.
- The majority of the OAIC's 2018-19 assessment program was specifically funded (for example through MOU arrangements or an appropriation). The objectives of the assessments are, to some extent, directed by the purposes of the funding arrangement. Staff also have regard to media reporting, OAIC complaints data, trends in other assessments and feedback from prospective assessment targets when determining the scope of assessments.
- The tables below this page set out the completed assessments for 2018-19 and the open and planned assessments for 2019-20.
- The OAIC conducted a series of assessments that considered the access security controls that a number of emerging participants in the MHR system use to protect personal information. Specifically the OAIC conducted a survey of 14 pharmacies, 8 pathology and diagnostic imaging service providers, and two private hospitals for compliance with APP 11 and Rule 42 of the *My Health Records Rule 2016*. Findings from the assessments showed that some pharmacies and one private hospital did not have a written MHR access security policies in place in breach of the minimum requirements of Rule 42. The findings from these surveys will inform guidance on access security to all MHR system participants. The reports for these assessments have been published on our website.. Having regard to the seriousness of the circumstances, as Privacy Commissioner I exercised my discretion to take further regulatory action by opening Commissioner initiated investigations in relation to one of the private hospitals and the pharmacies under section 40 of the Privacy Act. The investigations were closed after initial enquiries, with no further regulatory action, on the basis that...

- On 15 November 2017, the OAIC signed an MoU with Home Affairs[1] for the provision of two privacy assessments in relation to the National Facial Biometric Matching Capability and National Driver Licence Facial Recognition Service. This MoU was varied on 8 May 2019, deferring the commencement of the privacy assessments for two years, until there is more certainty regarding the rollout of the government's identity matching services.
- Assessment findings are typically not disclosed publicly until an assessment report is published.

Possible questions

- ***How are assessments funded?*** Generally, the OAIC's 2018-19 assessments were specifically funded. The OAIC's assessments relating to digital health (ADHA), the Unique Student Identifiers Office and the ACT government were funded through MOU arrangements. Data matching assessments were specifically funded through a government appropriation expiring at the end of 2018-19. In 2019-20, assessments relating to digital health (ADHA), Passenger Name Record information handled by the Department of Home Affairs, the ACT government and the NFBMC are tied to specific funding.
- ***How many staff work on assessments?*** There are currently 7 staff (6.8 FTE) in the assessments section (1 x EL2, 4 x EL1, 3 x APS 6).
- ***Are privacy assessments the same as privacy impact assessments?*** No, although there are some similarities. Privacy impact assessments (PIAs) are a strategy to identify and manage privacy risks in a process that involves personal information, and are ideally conducted at the inception stages of a project. Privacy assessments are a regulatory measure available to the Privacy Commissioner under s 33C of the Privacy Act, and are typically conducted to assess the presence of privacy risks once a project is operational (for this reason they can be characterised as 'audits').
- ***What are your KPIs for assessments?*** The OAIC reports on four KPIs for conducting privacy assessments:
    - 1- assessments are completed in accordance with the schedule developed in consultation with the assessment target
    - 2 - monitoring and compliance approaches are coordinated with the business and operational needs of the assessment targets
    - 3 - high proportion of recommendations accepted by assessment targets
    - 4 - key assessment outcomes and lessons learnt are publicly communicated where appropriate.

  The OAIC did not achieve KPI 1 in 2018-19 because the finalisation of assessment reports was not completed on schedule in all cases. We will continue to improve our assessment reporting process in the next financial year and work with the organisation or agency being assessed to assist them to finalise responses to draft assessment reports. All other KPIs were achieved in 2018-19.
- ***How long does it take to complete an assessment?*** Of all assessments completed in 2018-19, the average time taken to complete an assessment was 15 months. This is measured from the time an assessment target is formally notified about the assessment, to the time an assessment target accepts any recommendations in a draft report. The OAIC will continue to improve our assessment reporting process in order to reduce the overall time for completion.
- ***How do you make sure implementations are recommended?*** In some instances, assessment targets are able to implement recommendations quickly after assessment fieldwork and respond to the assessment report noting that a recommendation has been actioned. Where a recommendation requires a longer term implementation effort, the OAIC typically allows an implementation period of

[1] https://www.oaic.gov.au/about-us/our-corporate-information/memorandums-of-understanding/mous/mou-in-relation-to-national-facial-biometric-matching-capability/.

12-18 months before following-up with the assessment target by letter. The OAIC will determine whether further action is required after reviewing the assessment target's response to the letter, and any supporting information they provide.

Document history

Updated by	Reason	Approved by	Date
Karin Van Eeden Angela Qi	March 2020 Estimates	Dimitrios Kormas	30-1-2020

Table of assessments closed in 2018-19

Summary: 7 assessments with 27 separate entities (1 agency, 26 organisations). None of the reports have been published.

No.	Assessment	Commenced	APPs	Status	Planned public report?
1	Telstra's practices, procedures and systems under the 'data retention scheme'	30-Nov-17	11	Closed 16 November 2018	Y – combined summary report
2	DVS business users privacy policies	17-Jul-18	1, 5	Closed 23 January 2019	Y – combined summary report
3	Follow up of Optus's implementation of recommendations in the 2016 assessment of personal information disclosure to law enforcement agencies	21-Sep-18	11	Closed 26 June 2019	Y – a short update in existing public reports
4	Follow up on retail loyalty programs (Coles and Woolworths)	4-Sep-18	1, 5	Closed 28 June 2019	N – note in annual report
5	Qantas Frequent Flyer program privacy governance	13-Apr-17	1, 5	Closed 30 June 2019	Y – with redactions
6	Virgin Velocity program privacy governance	23-May-17	1, 5	Closed 30 June 2019	Y – with redactions
7	Pay-as-you-go program data matching assessment assessment with DHS	8-Aug-17	1.2, 3, 5	Closed 30 June 2019	Y – in full

Table of assessments open at end of 2018-19, closed in 2019-20 or currently in progress

No.	Assessment	Commenced	APPs	Status	Planned public report?
1	Follow up on recommendations in the 2015 PNR assessment report with Home Affairs; destruction and de-identification of PNR data	30-Mar-17	6, 11	Closed 25 July 2019	Y
2	Assessment of Healthscope's management of MHR/HI access (ADHA MOU)	18-Jul-17	11	Closed 24 December 2019	Y
s 47E(d) [redacted]					
4	Non-employment Income Data Matching (NEIDM) Program assessment with DHS	8-Sep-17	10, 13	Closed 30 September 2019	Y
5	Housing and Community Services ACT assessment (ACT MOU)	14-Dec-17	TPP 6, 11	Closed 20 December 2019	Y
6	Assessment of Home Affairs 'Connected Information Environment' relating to PNR data	2-Jan-18	11	Closed 19 December 2019	Y – with redactions
s 47E(d) [redacted]					

s 47E(d)

[redacted]

16	Assessment of the USI Transcript Service (USI MOU)	23 April 2019	1	Closed 14 August 2019	Y

s 47E(d)

[redacted]

Table of planned 2019-20 assessments

Note: an assessment forward plan for 2019-20 is subject to Executive approval. The forward plan contemplates strategic assessments on a range of areas, with the highest priority areas including the finance sector, digital health, the Australian Government Agencies Privacy Code and the notifiable data breaches scheme. The table below only includes assessments where work has been undertaken/the executive has provided notional approval.

No.	Assessment	APPs	Status	Planned public report?
s 47E(d)	[redacted]			

Commissioner brief: Consumer Data Right

Key messages

- The 'Consumer Data Right' (CDR) is a right for consumers to access particular data in a readily usable form, and to direct a business to securely transfer that data to a data recipient. It will apply in certain sectors of the economy designated by the Treasurer, and aims to give consumers greater control over how their data is used and disclosed in order to create more choice and competition.
- The OAIC regulates and advises on the privacy aspects of the CDR scheme in conjunction with the Australian Competition and Consumer Commission (ACCC), the agency regulating the broader scheme. The OAIC has been provided with additional funding of $12.9 million in the 2018-19 Budget over four years to perform this role.
- The OAIC welcomes the introduction of the CDR and supports initiatives seeking to give individuals greater choice and control over how their data is used.

Critical facts

- The CDR scheme seeks to give consumers greater control over how their data is used and disclosed. It will apply in certain sectors of the Australian economy designated by the Treasurer, allowing consumers to access particular data in a readily usable form and to direct a business to securely transfer that data to an accredited third-party data recipient. The CDR is not limited to individuals - businesses will also be able to access and transfer their data under the CDR.
- The Treasury Laws Amendment (Consumer Data Right) Act 2019 was passed on 1 August 2019 to insert a new Part IVD into the *Competition and Consumer Act 2010* (Competition and Consumer Act). The OAIC was consulted throughout the development of the legislation.
- The OAIC worked with the ACCC on the implementation of the CDR regime, including by supporting the ACCC in its development of the Rules. The Rules complement Part IVD of the Competition and Consumer Act, including by defining the elements for consent, outlining the accreditation framework for data recipients, and elaborating on the Privacy Safeguards.
- The ACCC have formally made the CDR Rules for the banking sector and they entered into force on 6 February 2020.
- On 24 February 2020 the OAIC published guidelines on the privacy safeguards to assist industry in interpreting their privacy obligations under the CDR. The OAIC finalised these following consultation with industry, the ACCC and other key stakeholders.
- The CDR Data Standards Body, Data61, is responsible for developing technical standards to support the data sharing which will occur under the legislation and rules. The OAIC is an observer on the Data Standards Advisory Committees for both the banking and energy sectors. On 31 January 2020, the Data Standards Body released a new version of the data standards which represent the baseline for implementation ahead of CDR launching in July 2020.
- On 23 January 2020, the Treasurer announced an Inquiry into Future Directions for the CDR led by Mr Scott Farrell, due to make recommendations by September 2020. A key issue will be to examine how the CDR could be expanded beyond its current 'read' access to include 'write' access. Allowing write access would mean that the recipient, instead of only viewing the data, will be able to vary it, and potentially able to make payments on behalf of the consumer. This would enable, for example, for recipients to make changes to a customer's data and use this data to facilitate account switching or payment initiation.
- There has been significant stakeholder and media commentary on screen scraping of CDR data following the establishment of a Select Committee Inquiry into the Financial Technology and Regulatory Technology in September 2019. FinTech Australia has been advocating for CDR to be easier

and cheaper than screen scraping, arguing the cost of accreditation and maintaining CDR technology does not make sense given screen scraping is cheaper and less complex to access. The major banks and consumer advocate groups are advocating a ban to screen scraping claiming it poses risks to consumers, and CDR will make screen scraping technology redundant.

Possible questions

Will the OAIC be ready for the July 2020 start date?

- Yes, the OAIC will be ready to undertake its regulatory role in relation to privacy aspects of the CDR scheme from 1 July 2020. The OAIC continues to engage closely with the ACCC regarding implementation activities, particularly in relation to implementation of the Government's 'no wrong door' approach to complaint handling.
- The OAIC has several governance measures in place to ensure we remain on track and joined up across government. For example, the OAIC participates in a number of cross-agency governance fora, including the CDR Board and the CDR Operational Committee. The OAIC also has an internal 'CDR Governance Board' which meets on a monthly basis to actively manage a CDR project plan which sets out key deliverables and deadlines.

If asked about screen scraping practices

- The OAIC is aware of concerns about data being transferred outside of the CDR system, particularly in the context of screen scraping.
- Screen scraping involves an individual allowing a third party to access the individual's account using the individual's access credentials such as their internet banking username and password. This presents a range of information security risks for individuals, vulnerable persons in particular.
- The introduction of CDR presents an opportunity to consider whether other methods of providing access to sensitive financial data, particularly screen scraping, should be restricted in light of the availability of the more secure and protective CDR method.

If asked about expanding the CDR to non-accredited third parties

- One of the bedrock tenets underpinning the CDR regime has been that consumer data should be transferred to trusted and accredited parties. This reflects the sensitive nature of CDR data, and is designed to prevent misuse of this data and build consumer trust in the system.
- Permitting transfers of CDR data to non-accredited entities raises privacy risks associated with CDR, particularly those posed to vulnerable consumers, and could potentially undermine the stringent privacy protections in CDR.

If asked about the complexity of the CDR scheme

- The OAIC is aware of concerns about the potential complexity of the CDR regulatory framework, and its interaction with the Privacy Act framework.
- The OAIC and ACCC have agreed to operationalise a no wrong door approach and refer matters to ACCC and recognised External Dispute Resolution bodies where appropriate. We are also working closely with the ACCC to ensure co-ordinated co-regulation of the CDR.
- The OAIC has also developed guidance on the privacy safeguards to ensure the application of the CDR and Privacy Act frameworks, and the interaction between the two, are clear to CDR participants.

What was OAIC's involvement in Treasury's development of the Privacy Impact Assessment (PIA)?

- Treasury undertook a PIA in accordance with its obligations under the Australian Government Agencies Code. Treasury undertook an initial PIA on the draft legislation between late 2018 and 1 March 2019. An external consultancy undertook a second PIA for the full CDR scheme (including the

legislation, the Rules and the standards), which was published on 11 December 2019. As the regulator, the OAIC does not have a role in undertaking or approving PIAs. However, the OAIC did provide the external consultant with some general comments on early drafts of the second PIA.

Key dates

- The CDR will be rolled out across one sector of the Australian economy at a time. Banking is the first sector to which the CDR applies, where it is called 'Open Banking'.
- The Treasurer formally designated the banking sector on 4 September 2019 via the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. The next sector to be designated is the energy sector.
- The CDR has a phased implementation in the banking sector, with major banks and voluntarily-participating authorised deposit-taking institutions (ADIs) to release product and consumer data in stages.
- From 1 July 2020, major banks will commence sharing consumer data regarding credit and debit card, deposit account and transaction account data. Consumer data relating to mortgage and personal loan data will be required to be shared after 1 November 2020.
- This timetable was announced by the ACCC on 20 December 2019. Prior to this, major banks were due to commence sharing consumer data in February 2020.
- On 29 August 2019 the Treasurer announced that the energy sector will be the next sector designated under the CDR. A designation instrument for the energy sector expected to be finalised by June 2020.
- In August 2019 the ACCC released a positions paper setting out the "gateway" model as the preferred data access model for CDR in the energy sector, and Treasury publicly consulted on which energy datasets should be prioritised for the energy Designation Instrument. The OAIC provided the Treasury with a public submission recommending that a PIA be conducted before designating the particular datasets for the energy sector.

Regulatory model

- The OAIC will co-regulate the CDR scheme with the ACCC. The responsibilities of each regulator are outlined in the Competition and Consumer Act and the OAIC and ACCC have an MOU to support their working relationship.
- The OAIC will advise and coordinate with the ACCC on privacy aspects of the CDR. In particular, the OAIC will have primary responsibility for the handling of consumer complaints using a 'no wrong-door' approach.
- The OAIC will also have a role in dealing with systemic or serious privacy breaches of the CDR framework, sector designation, the rule-making process, consumer education and reviewing technical standards.
- The OAIC and the ACCC are currently working together on implementation matters, including the development of a system to receive and process CDR matters. The OAIC and ACCC are also working together to develop a joint approach to compliance and enforcement, including the creation of joint committees, the development of joint audit and assessment programs, and the future establishment of regular meetings to monitor the types of CDR matters received.

Privacy

- A strong privacy and security framework to protect consumers' information is necessary to maintain the integrity of the CDR scheme.

- The Competition and Consumer Act sets out 13 Privacy Safeguards based on the APPs in the Privacy Act. The OAIC provided advice to the Treasury on the development of these safeguards, and to the ACCC on the development of the accompanying Rules.
- Consent is the primary basis upon which CDR data may be handled. The Rules seek to ensure that consent is 'voluntary, express, informed, specific as to purpose, time limited and easily withdrawn'. In addition, consent must not be bundled with other directions, permission, consent or agreements.
- Small business operators (not normally covered by the Privacy Act) who are accredited to receive data under the CDR scheme will be covered by the Privacy Act in relation to their handling of personal information outside of the CDR regime.
- Treasury undertook an initial PIA on the draft legislation between late 2018 and 1 March 2019. An external consultancy undertook a second PIA for the full CDR scheme (including the legislation, the Rules and the standards), which was published on 11 December 2019.
- The OAIC is in the process of engaging an external consultant to undertake a separate PIA for the CDR complaints handling system and processes.
- The CDR scheme is not intended to limit the credit reporting provisions in Part IIIA of the Privacy Act.

Governance

- In January 2020, Treasury established the CDR Board and the CDR Operational Committee to strengthen accountability for program delivery of the CDR by the relevant government agencies, and to provide high level co-ordination and direction-setting to align CDR policy and implementation. The Australian Information Commissioner and the Deputy Commissioner are members of these governance bodies.
- Internally, the OAIC also has an internal 'CDR Governance Board' which meets on a monthly basis to actively manage a CDR project plan which sets out key deliverables and deadlines.
- The OAIC also participates in a range of other cross-agency governance fora, including a monthly senior executive level update and coordination meeting, a fortnightly ACCC-OAIC Coordination Committee meeting, and other regular officer-level meetings such as a compliance and enforcement Working Group.
- The OAIC and ACCC have an MOU to support their working relationship, and are in the process of updating the MOU ahead of 1 July 2020.

Document history

Updated by	Reason	Approved by	Date
Shona Watson	March 2020 Additional Estimates hearings	Stephanie Otorepec	6 February 2020

Commissioner brief: Data Matching Centrelink

Key messages

- Sharing and comparing data from different sources can help to improve efficiency and streamline services across government departments, but it must be done in accordance with the Privacy Act.
- We work closely with government agencies to ensure they understand these privacy obligations and adopt best practice when undertaking data matching.
- We will continue to progress the data matching assessments of the Department of Human Services (DHS – now Services Australia) and other government agencies and will publish our reports on our website when they are finalised.
- The OAIC has made a submission to the Senate Standing Committee on Community Affairs' inquiry into the Centrelink compliance program.[1] The submission focuses on the findings of the OAIC's assessment of the PAYG program.
- The OAIC's assessment of the PAYG program found that DHS has taken some steps to address issues with the quality of the personal information it collects and uses and has implemented many changes to the PAYG program following an investigation by the Commonwealth Ombudsman (Ombudsman) in early 2017. However, the OAIC also identified potential privacy risks associated with the PAYG program and made five recommendations to address these risks.

Critical facts

- In addition to our regulatory oversight under the Privacy Act, the OAIC has a general regulatory oversight role for government data matching under:
    - the *Data-matching Program (Assistance and Tax) Act 1990* (the Data Matching Act) and the Guidelines for the Conduct of Data-Matching Program (the statutory guidelines), which apply when Tax File Numbers (TFNs) are used for data matching. As far as we are aware, only the Department of Veterans' Affairs is currently using this statutory regime.
    - the Guidelines on Data Matching in Australian Government Administration (voluntary guidelines). The voluntary guidelines are not mandatory and a breach of the guidelines will not necessarily result in a breach of the Privacy Act. However, a number of agencies have adopted the voluntary data matching guidelines and must seek an exemption from the Commissioner should they wish to depart from any of the requirements. The OAIC may not maintain the voluntary Guidelines in their current form. The National Archives of Australia have recently revoked the records disposal authority for data-matching that underpins the Guidelines in relation to records destruction.[2] Consequently, the OAIC is currently reconsidering the Guidelines—in particular, how they align with the Privacy (Australian Government Agencies – Governance) APP Code 2017 and the requirement to conduct Privacy Impact Assessments in accordance with that Code.
- Some agencies conduct higher volumes of data matching than others. An example of such an agency is DHS. Under the 'Enhanced Welfare Payment Integrity – non-employment income data matching' 2015-16 budget measure, the OAIC was allocated $4,774,000 from 1 January 2016 to 30 June 2019 to provide regulatory oversight of privacy implications arising from DHS's increase in data matching

[1] The submission to the Senate Standing Committee on Community Affairs' inquiry can be found at https://www.oaic.gov.au/engage-with-us/submissions/inquiry-into-centrelinks-compliance-program-submission-to-senate-community-affairs-references-committee/.

[2] See paragraph 11 of the OAIC's submission to the Department of Health in October 2019 on the Exposure Draft: Health Legislation Amendment (Data-matching) Bill 2019. The repealed records disposal authority is General Disposal Authority 24: Records Relating to Data Matching Exercises.

activities using new methodologies and processes. As part of this oversight role, the OAIC decided to conduct six privacy assessments. As of January 2020, fieldwork for all six privacy assessments, funded under the 2015-16 budget measure, have been completed. A table on page 6 sets out the status of each assessment.

- DHS's data matching activities attracted significant and ongoing media attention following the rollout of the automated debt raising and recovery system known as the Online Compliance Intervention (OCI) system. The OCI system is in use for the Pay-As-You-Go (PAYG) program. It was later renamed the Employment Income Confirmation (EIC) system and now known as the Check and Update Past Information (CUPI) system (since October 2018). While the Commissioner decided not to conduct a CII of the OCI system, noting the findings of the Commonwealth Ombudsman's inquiry were released in April 2017, the OAIC conducted a risk-based privacy assessment of the PAYG program in December 2017, focussing on APPs 10 and 13. The report for this assessment was published on the OAIC website in September 2019.
- In September 2019, the OAIC also made a submission to the Senate Standing Committee on Community Affairs' inquiry into the Centrelink compliance program. The submission focused on the findings of the OAIC's assessment of the PAYG program (see 'Possible questions' below for a summary of the findings of the PAYG assessment).
- In November 2019, DHS announced that it will cease the use of income averaging to calculate overpayments and will review all debts where the averaging method was used.[3] On 28 January 2020,[4] it was reported that Services Australia proposes to change Centrelink's compliance program so that welfare recipients report their actual fortnightly earnings to Centrelink to enhance the accuracy of income reporting, rather than calculating earnings based on their wage and hours worked. Draft legislation underpinning the changes was released for consultation in February 2020[5].
- Assessment work by the OAIC, in order of when fieldwork was conducted (more detail provided in the table on page 6):
    - **DHS** – an APP 1.2, 3 and 5 assessment of the Non-Employment Income Data Matching (NEIDM) program. The report for this assessment was published on the OAIC website in September 2019.
    - **DHS** – an APP 10 and 13 assessment of the PAYG program (mentioned above). The report for this assessment was published on the OAIC website in September 2019.
    - **DHS** – an APP 11 assessment, which considered the security measures DHS takes in relation to both the NEIDM and PAYG programs
    - **ATO** – an APP 11 assessment on the ATO's involvement in the NEIDM and PAYG programs
    - **DHS** – an APP 1.2, 5 and 12 assessment of the Annual Investment Income Report (AIIR) program
    - **DVA** – an APP 1.2 assessment on the Department of Veterans' Affairs
- Four of the six data matching assessments have been publicly disclosed in last year's annual report, namely DHS's assessments on the NEIDM and PAYG programs and the APP 11 assessments of DHS and the ATO. The remaining two assessments (DHS-AIIR and DVA) will be reported on in this year's annual report.
- See table on page 6 for information about other data matching related work conducted by the OAIC.

[3] https://www.abc.net.au/news/2019-11-19/robodebt-scheme-human-services-department-halts-existing-debts/11717188
[4] https://indaily.com.au/news/national/2020/01/28/new-centrelink-income-rules-after-illegal-robo-debt-debacle/
[5] This is the Social Services and Other Legislation Amendment (Simplifying Income Reporting and Other Measures) Bill 2020. As of 27 February 2020, the Bill was before the Senate.

Possible questions

- ***How much funding did the OAIC receive for its data matching oversight?*** The OAIC has been allocated $4,774,000 from 1 January 2016 to 30 June 2019. These funds exclude indexation/efficiency dividend and other measures:
    - 2015/16: $818,000
    - 2016/17: $1,311,000
    - 2017/18: $1,319,000
    - 2018/19: $1,326,00
- ***Will the OAIC continue to monitor data matching activities even though the funding has come to an end?*** Yes - the Commissioner has a range of regulatory functions and enforcement powers under the Privacy Act, including specific functions with respect to data matching:
    - 'undertaking research into, and monitoring developments in, data processing and technology (including data matching and linkage) to ensure that any adverse effects of such developments on the privacy of individuals are minimised'
    - 'examining a proposal for data matching or linkage that may involve an interference with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals'.

  The OAIC also oversees compliance by Australian Government agencies with the *Data-matching Program (Assistance and Tax) Act 1990* (Data Matching Act), the Guidelines for the Conduct of Data-Matching Program (the statutory guidelines), and the Guidelines on Data Matching in Australian Government Administration (voluntary guidelines).
- ***What has the OAIC found during its assessments?*** Final copies of the NEIDM and PAYG reports were sent to DHS on 10 September 2019. The reports were published on our website on 30 September 2019. The PAYG report (which concerns Centrelink's compliance program) is attached to this brief (at **Attachment A**).
    - The **NEIDM** assessment[6] found that DHS has taken steps to build privacy awareness and risk management into their data matching processes. However, the OAIC identified potential risks associated with the NEIDM program and made four recommendations to DHS to:
        - enhance internal policies related to the handling of personal information
        - update the NEIDM data matching protocol
        - develop a process for monitoring the implementation of privacy risk assessments
        - ensure the requirements of its internal privacy policies and procedures are followed in practice.
    - The **PAYG** assessment[7] (which relates to Centrelink's compliance program) found that DHS has taken some steps to address issues with the quality of the personal information it collects and uses and has implemented many changes to the PAYG program following an investigation by the Commonwealth Ombudsman (Ombudsman) in early 2017. However, the OAIC also identified

[6] The NEIDM assessment report can be found at https://www.oaic.gov.au/privacy/privacy-assessments/handling-of-personal-information-department-of-human-services-neidm-data-matching-program/. A summary of the recommendations is at paragraph 1.4.

[7] The PAYG assessment report can be found at https://www.oaic.gov.au/privacy/privacy-assessments/handling-of-personal-information-department-of-human-services-payg-data-matching-program/. A summary of the recommendations is at paragraph 1.4.

additional potential privacy risks associated with the PAYG program and made recommendations to DHS to:

- ensure the accuracy, currency and completeness of the personal information it collects and uses under its compliance program
- improve Centrelink's compliance program process to ensure the outcome of the process, following review by customers, is that any debt calculation is based on accurate, up-to-date and complete information
- implement measures to ensure it is adhering to the minimum procedural requirements under the Privacy Act (APP 13) in relation to the correction of personal information whenever a customer raises concerns about their personal information being incorrect
- continue to conduct, review and monitor the implementation of privacy risk assessments, especially if any future changes are made to the compliance program.

Regarding the other four assessments, the OAIC does not routinely comment on open assessments. We will continue to progress the data matching assessments of DHS and other government agencies and will publish our reports on our website when they are finalised.

- ***Why have your assessments taken so long to become publicly available?*** The PAYG assessment was postponed for a period given that the Commonwealth Ombudsman was conducting an investigation into the automated debt raising and recovery system in 2017 (and then an implementation review in 2019). The reason for postponing the PAYG assessment was to avoid any potential duplication of Commonwealth resources on substantially similar matters.
- ***Is automated data matching legal?*** The OAIC did not consider the legality of automated data matching activities when conducting its privacy assessments. While we understand that certain questions relating to the legality of the Centrelink compliance program have been considered by the courts[8] and are still the subject of court action, in the context of the Privacy Act, as with most of the OAIC's privacy assessments, the OAIC took a risk-based approach to its assessment of DHS's PAYG data matching program that focuses on identifying privacy risks to the effective handling of personal information. Where risks are identified, recommendations are made based on the OAIC's estimates of the relative privacy risk against the relevant legislative requirements, with the aim of assisting entities to improve their observed privacy practices and procedures.
- ***Are you concerned about the Centrelink's compliance program?*** The OAIC engages with DHS on an ongoing basis regarding its implementation of recommendations from our privacy assessments.

  In April 2019, the Commonwealth Ombudsman published the Centrelink's Automated Debt Raising and Recovery System Implementation Report (Implementation Report). The purpose of this investigation and report was to seek assurances that the Department of Social Services (DSS) and DHS had implemented the agreed recommendations in the 2017 Ombudsman report. The investigation found that DSS had implemented the recommendation for which it was responsible, and DHS had made significant progress in implementing the remainder of the recommendations. The Ombudsman made an additional four recommendations as part of the Implementation report.[9]

  These further changes to the PAYG program and the Ombudsman's additional recommendations align with the OAIC's expectations in relation to APPs 10 (quality of personal information) and 13 (correction of personal information).

[8] See: https://www.theguardian.com/australia-news/2019/nov/27/government-admits-robodebt-was-unlawful-as-it-settles-legal-challenge

[9] Commonwealth Ombudsman, *Centrelink's Automated Debt Raising and Recovery System*, April 2019, page 3.

The OAIC also made a submission to the Senate Standing Committee on Community Affairs' inquiry into the Centrelink compliance program in September 2019. The submission focuses on the findings of the OAIC's assessment of the PAYG program.

- ***Have you taken any action in response to the Centrelink compliance program?*** Having regard to DHS's response to the OAIC's recommendations to the PAYG program and the actions taken in response to the Ombudsman's 2017 review, the OAIC has been satisfied to date that further regulatory action is not necessary.

Key dates

- See table below.

Background information – Summary of NEIDM, PAYG and AIIR programs

Name of program	Matching agency	Information matched	Method used to confirm income (at time of assessments)
NEIDM	DHS	Income tax return information collected from taxpayers (including non-employment income sources such as dividend payments)	Staff-assisted (i.e. manual)
PAYG	DHS	PAYG payment summary information collected from employers	Staff assisted (i.e. manual) and automated processes
AIIR	DHS	Bank interest information sourced from the ATO's Annual Investment Income Report	Staff-assisted (i.e. manual)

- Where the matching process indicates a discrepancy between what has been reported to DHS and to the ATO, DHS may begin the income confirmation process to determine whether a debt is owed.
- All three programs are conducted under the OAIC's voluntary data matching guidelines as they do not use TFNs.

Document history

Updated by	Reason	Approved by	Date
Angela Qi	March 2020 Estimates	Dimitrios Kormas	31 January 2020

Assessments (fieldwork complete)

Assessment	APPs	Date of notification letter	Fieldwork dates	Draft report sent to target	Draft report with comments received from target	Final report sent to target
NEIDM (DHS)	1.2, 3 and 5	8 August 2017	24-25 October 2017	23 May 2018	10 December 2018	10 September 2019
PAYG (DHS)	10 and 13	8 September 2017	12-13 December 2017	23 May 2018	10 December 2018	10 September 2019

s 47E(d)

[redacted]

Other activities (complete)

Activity	Description of activity	For which agency?
Advice regarding data matching protocols (1 July 2018 – 31 January 2020)	Reviewing data matching protocols and/or exemption requests Following the revocation of GDA 24 by National Archives, the OAIC has not received any data matching protocols and/or exemption requests since July 2019.	-11 from DHS -five from the ATO -one from Department of Home Affairs
General policy advice (1 July 2018 – 31 January 2020)	Provided policy advice and guidance on the: • applicability of the voluntary guidelines regarding a proposed ATO data matching program • applicability of the voluntary guidelines regarding a proposed DHS data matching program • timing of seeking an exemption and publishing a protocol for a data matching program	 ATO DHS ATO

	• applicability of the voluntary guidelines to the State government's data matching activities • Privacy Code requirements, such as PIAs that agencies should consider before commencing a data matching program • applicability of the voluntary guidelines to the Exposure Draft: Health Legislation Amendment (Data-matching) Bill 2019.	Office of State Revenue, Western Australia National Disability Insurance Agency (NDIA) Department of Health

s 47E(d)

[redacted]

Attachment A

PAYG assessment report - https://www.oaic.gov.au/privacy/privacy-assessments/handling-of-personal-information-department-of-human-services-payg-data-matching-program/

s 47E(d)

s 47E(d)

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 individuals. The records are available to individuals and participating healthcare providers.
- Based on the number of people eligible for Medicare as at 31 January 2019 (25,459,544), the participation rate is 90.1%, with a national opt-out rate of 9.9%. The opt-out period for the My Health Record (MHR) system commenced on 16 July 2018 and ended on 31 January 2019 (having previously been extended on two occasions).
- In this context, the OAIC's regulatory work has been focusing on:
  - providing consumers with clear and up-to-date information about the MHR system through our refreshed website content, consumer-facing MHR website and recent digital health campaign which ran across OAIC social media channels. These resources are aimed at both individuals and healthcare providers, and provide information about privacy, data breach requirements, privacy controls and handling sensitive information in the MHR system
  - engaging with the ADHA and Department of Health on privacy aspects of the MHR system
  - regulatory oversight of the MHR system, including responding to enquiries and complaints, handling mandatory data breach notifications, providing privacy advice, and conducting privacy assessments under our Memorandum of Understanding (MOU) with the ADHA.
- On 27 June 2019, the OAIC and ADHA signed an updated MOU, effective from 1 July 2019 until 30 June 2020, to provide dedicated privacy-related services under the *Privacy Act 1988*, *My Health Records Act 2012* and *Healthcare Identifiers Act 2010*.
- On 25 November 2019, the Australian National Audit Office (ANAO) released its report: *Implementation of the My Health Record system*.

Critical facts

Our regulatory oversight work

- The number of enquiries and complaints received by the OAIC in relation to the MHR system increased significantly in the 2018/19 financial year (compared to previous years). The increase during this time can be attributed to the increase in community interest in the My Health Record system during the opt-out period. So far in the 2019–20 financial year, the number of enquiries and complaints appear to have decreased significantly compared to the 2018–19 financial year.

	July 2012 (MHR system commencement) to 30 June 2018	1 July 2018 to 30 June 2019		1 July 2019 to 31 January 2020
Enquiries	83	155		5
Complaints	12	104 (62 received, 42 finalised)		26 (6 received, 20 finalised)
Mandatory data breach notifications	88	35		1

- Whilst the number of data breach notifications has significantly decreased in the current financial year, in previous financial years the data breach notifications have generally involved incorrect information being uploaded to a MHR. 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.
- The OAIC completed 15 privacy assessments of the MHR system and Healthcare Identifier service between 2014 and 2018.
    - 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.
    - The ADHA (and previously the Department of Health) responded to and accepted almost all of the OAIC's recommendations. We are working with the ADHA to implement them.
- During the first half of 2019, the OAIC commenced and conducted a series of assessments that looked at whether new participants in the MHR system have 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 and 11, and Rule 42 of the *My Health Records Rule 2016* (MHR Rule). The OAIC also conducted fieldwork for the two private hospital assessments. These assessments are still under consideration and the finalised reports will soon be published on our website. Findings from these assessments will inform future policy guidance relating to access security for all MHR system participants.

Coverage of State and Territory bodies

- Sections 72 and 73 of the MHR Act relate to the OAIC's jurisdiction to take action against a State or Territory instrumentality or authority regarding their handling of MHR information.

Changes to the MHR system

- In November 2018, the *My Health Records Amendment (Strengthening Privacy) Act 2018* passed both Houses of Parliament - introducing privacy-enhancing measures to the MHR system. These measures provide individuals with greater certainty and control over how their MHR information will be handled. Key amendments include:
    - requiring the System Operator to permanently delete health information about a healthcare recipient who has cancelled their MHR
    - restricting the ability of the System Operator to disclose health information contained in a MHR to law enforcement agencies and government agencies without an order by a judicial officer
    - specifying that MHR information cannot be used for insurance or employment purposes
    - preventing a person from being an authorised representative of a minor if they have restricted access to a minor or if this may pose risk to the minor or another person
    - increasing civil and criminal penalties for breaches of key privacy protections. While the MHR Act does not expressly provide a referral power to the Information Commissioner in this regard, if the Commissioner becomes aware of a potential offence, the Commissioner could inform the affected individual—and advise that if they want to pursue a criminal penalty, they should raise it with the authorities
    - providing a more extensive legislative basis for implementation of the framework relating to the use of My Health Record data for research or public health purposes
    - removing parents' access to a young person's record from age 14, except where the young person has nominated them as an authorised representative.

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.
- In September 2019 the OAIC ran a 10-week digital health campaign across our social media channels (which included a total of 40 health related posts across Facebook, LinkedIn and Twitter). The campaign highlighted the importance of our *Guide to health privacy* and other health guidance materials (including MHR-related guidance).
- Since the decision to move to opt-out, the OAIC has developed a number of resources to assist both individuals and healthcare providers in the MHR system. This includes a consumer-facing MHR website which contains information on privacy, data breach requirements and handling sensitive information in the MHR system. To coincide with this, the OAIC's website content was consolidated and refreshed to assist user navigability. In April 2019, the OAIC released a number of MHR-related videos on social media to raise awareness of the privacy controls available in the MHR system. These videos continued to be shared on the OAIC's website throughout 2019.

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

- A key focus of the OAIC's MHR assessments has been the security of the NRS. The NRS is the database system operated by the MHR National Infrastructure Operator (currently Accenture). Under the MHR system, consumers' health records are either uploaded into the NRS or obtained from participating repositories. The MHR National Infrastructure Operator (NIO) is responsible for providing and managing the system on behalf of the System Operator, including managing the system's security controls, which holds the key data sets that make up a My Health Record, including shared health summaries, event summaries, discharge summaries, specialist letters, consumer entered health summaries and consumer notes.

- The OAIC conducted an APP 11 assessment of ADHA in June 2018 which focused on the handling of personal information stored in the NRS. The risk-based assessment considered the governance mechanisms of ADHA's security measures - including training, internal practices, procedures and systems, ICT security, physical security, access security, third party providers, data breaches, destruction and de-identification as well as the application of relevant security standards. The assessment did not include a physical review or testing of the technical capabilities of the ICT systems used by the System Operator or NIO, but considered past third-party reviews, which the assessors re-examined. The OAIC found that at the time of the assessment ADHA had taken some reasonable steps to secure personal information according to APP 11. However, the assessment also identified some issues relating to document quality, documentation processes, security organisation and management oversight.

- The ADHA has informed the OAIC during assessments that the MHR system meets relevant Australian Government Security Standards, in particular the Australian Information Security Manual (ISM) and Essential Eight Strategies to Mitigate Cyber Security Incidents. However, we note that the recent ANAO audit report found that further work is required to implement all ISM security controls.
- Our previous assessments have identified end user security as an area requiring assessment of privacy risk.
- The OAIC's current assessments are focussed on end users to assess the system readiness of healthcare providers and governance arrangements to manage security risks associated with accessing the MHR system (MHR Rule 42). We are currently undertaking 4 assessments of the following health care providers:
    - 14 pharmacies (1 assessment)
    - 8 pathology and diagnostic imaging services (1 assessment)
    - 2 private hospitals (2 assessments)

  We will continue to progress these assessments and publish the reports on our website when they are finalised.

s 47E(d)

[redacted]

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

- The OAIC is currently considering the findings of the final report as part of our ongoing regulatory role. The report identifies a number of privacy-related risks which are also under consideration by the OAIC, such as in our recent privacy assessments.

- The OAIC supports the recommendations made and would welcome 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 have been completed (that is, a finalised report has not been issued to the entities involved), the OAIC has conducted the document review and fieldwork component for the four privacy assessments – including providing feedback to entities during an exit interview - within the MOU timeframe. Reporting for these assessments will be finalised in the 2019-20 financial year.

Key dates

- On 25 November 2019, the ANAO released its report: *Implementation of the My Health Record system*.
- On 27 June 2019, the ADHA and the OAIC signed an updated MOU effective 1 July 2019 to 30 June 2020.
- The *My Health Records Amendment (Strengthening Privacy) Bill 2018* was introduced on 22 August 2018, passed on 26 November 2018 with amendments, and received Royal Assent on 10 December.
- The opt-out period started on 16 July 2018 and concluded on 31 January 2019 (having been extended on two occasions).

ANAO Audit

- On 25 November 2019, the ANAO released its final 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.

- Notably for the privacy aspects of the system, the report found the following.
    - **End-to-end privacy assessment:** The ANAO considers that now that MHR is operating as an opt-out model, a comprehensive, end-to-end privacy risk assessment on its ongoing operation should be conducted. This assessment should address shared risks, discussed below.
    - **Shared risks:** risks relating to privacy and the IT core infrastructure were largely well managed, but management of shared cyber security risks was not appropriate. In particular, the report identifies issues with ADHA oversight in relation to the following entities connecting to the MHR system:
        - third-party software (such as clinical software and mobile apps) – concerning compliance with the Information Security Manual
        - HPOs accessing the MHR system – concerning compliance with legislated security requirements

- **Emergency access – assurance arrangements**: The AHDA did not have sufficient assurance arrangements to satisfy itself that all instances of emergency access by HPOs did not constitute a breach of privacy. The ADHA monitoring procedure does not include steps for receipt, assessment or monitoring of responses from HPOs. In a number of instances, ADHA did not receive a response from HPOs and in such cases, the ADHA could not satisfy itself that the circumstances of the emergency access did not constitute an interference with privacy. **Emergency access – contraventions unreported:** Where responses from HPOs have been received, some have indicated a potential contravention of the Act. Neither the ADHA nor the HPOs have notified the Information Commissioner of any of these instances (as required under section 75 of the My Health Records Act 2012).

- The report made five recommendations, four of which relate to the above issues.
  - **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 recommendations.

Document history

Updated by	Reason	Approved by	Date
Emma Robins	March 2020 Senate Estimates	Kellie Fonseca	TBA

s 47E(d)

s 47E(d)

s 47E(d)

s 47E(d)

Commissioner brief: Privacy law reform

Key messages

- The OAIC has welcomed reforms to strengthen the Privacy Act to ensure Australians' personal information is protected in the digital age
- The reforms outlined in the Government's response, including a review of the Privacy Act, will ensure that our regulatory framework protects personal information into the future and holds organisations to account
- The OAIC has also welcomed the government's continued commitment to introduce higher penalties for privacy breaches and a code of practice for digital platforms.
- The reform roadmap is an important step in enabling effective regulation of personal information handling, in line with community expectations for the digital environment and beyond.

Critical facts

- 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.
- 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.

Possible questions

Are you happy with the government response to the DPI?

Yes. 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.

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.

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. In our response to the DPI we advocated for x, y z. We are currently commissioning a number of research pieces that consider international experiences to analyse how they could be of benefit to the Australian privacy framework.

Key dates

- The timetable for reforms has not been made public.

Other background

- In order to support effective privacy regulation, the OAIC's experience is that there are four key pillars:
    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.
- To facilitate our active participating in the law reform process, we are commissioning external research into the following subject matter areas:
    - The definition of personal information
    - Notice and Consent
    - Harms in the digital age
    - Vulnerable people
    - Certification schemes
    - Online identifiers
    - New technologies (drones, smart cities, smart vehicles etc)
    - Facial recognition and biometrics

Document history

Updated by	Reason	Approved by	Date
Melanie Drayton	Estimates March 2020		

s 37

s 37

s 37

s 37

s 37