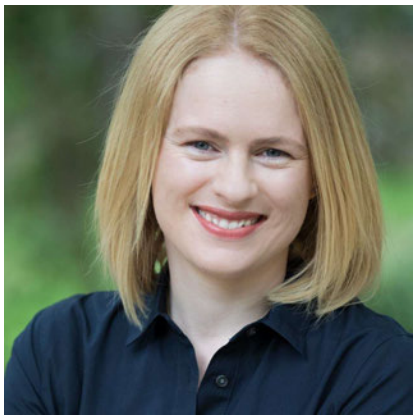
Commissioner brief: Committee members

Senator Amanda Stoker, Chair



Senator for Queensland

Chair of Legal and Constitutional Affairs Legislation Committee

Deputy Chair of Legal and Constitutional Affairs References Committee

Party: Liberal

Webpage: www.amandastoker.com.au

Official biography:

Amanda is married to Adam and is a mother of three young girls. She comes to the Senate after a career in the legal profession. Amanda studied law at Sydney University, and commenced her career at Minter Ellison. She was associate to then Justice Ian Callinan AC QC on the High Court of Australia, and Justice Philip McMurdo, who was then on the Supreme Court of Queensland's commercial list. After some time prosecuting for the Commonwealth in Brisbane and Townsville, Amanda joined the private bar. As a member of Level Twenty Seven Chambers, she practiced in commercial law, administrative law and corporate crime. Amanda has served as Vice-President of the Women Lawyers Association of Queensland.

Amanda joined the Liberal Party at the age of 19. She has spent over a decade growing in the party and giving voice to her convictions. She is motivated by the desire to see Australia return to a country of opportunity based on centre-right values.

As a Brisbane based member of the Liberal National Party, Amanda sits in the Liberal Party room in Canberra. Amanda is on the Economics, Finance and Public Administration, Public Works, Future Work and Regulations and Ordinances Senate Committees, as well as the Joint Standing Committee on the recognition of Indigenous people in the Australian Constitution and the Select Committee on Charity Fundraising.

Areas of interest:

- Religious freedom
- "Transgender agenda" and political correctness
- Protecting small businesses from "double dipping"
- Issues raised at previous estimates hearings:
    - Nil

"They vote for you" profile:

- Voted very strongly for increasing surveillance powers

Commissioner brief: Budget and resourcing

KEY MESSAGES

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

CRITICAL FACTS

- OAIC incurred a total (permitted) financial loss of $0.121million in 2019-20.
    - 2019-20 total revenue was $23.234million — $20.941million is appropriation, $2.323million is MOU and $36,000 received benefit for annual ANAO financial audit[2].
- 2019-20 Budget allocated $25.1 million over three years (including capital funding of $2.0 million) to facilitate timely responses to privacy complaints and support strengthened enforcement action in relation to social media and other online platforms that breach privacy regulations
    - 2019-20 Budget allocated $329,000 to the 2018-19 base and $2.256million over the forward estimates for oversight of the expansion of Medicare data matching.
    - 2020-21 total revenue is $23.304million. $20.948million is appropriation and $2.323 million is MOU
- OAIC has not received additional resourcing for the Notifiable Data Breach Scheme (in 2018/19, 2019/20 or 2020/21).
- OAIC has not received additional funding for its COVID Safe App regulatory role.
- The OAIC did receive $12.911million over forward estimates for Consumer Data Right Scheme (**CDR**) in the **2018-19** Budget (including a once-off capital injection for new office space of $860,000). This is approximately $3,000,000 each year. (terminates following 2021-2022)
- s74 **External revenue (MOU)** increased from $2.257m in 2019-20 to $2.323m in 2020-21. The increase relates to the MOU with Department of Home Affairs relating to National Facial Biometric Capability.

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

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

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
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 **waiting for correct date**
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 • 9 closed **Enquiries** • 24 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 • 2 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

Commissioner brief: Current media issues D2020/020143

Key messages

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

Critical facts

The media stories are broken down into six groups:

- InnovationAus funding story
- COVIDSafe app
- The naming of public servants
- The investigation into Clearview AI
- Telehealth
- The reported SkillSelect Data Breach
- Consumer Data Right and privacy

Possible questions

- The material supplements the Media Folder and other Estimates briefs

Key dates

- The media articles are all sourced from 2020.

Document history

Updated by	Reason	Approved by	Date
Andrew Stokes	October 2020 Estimates		19-10-2020

Commissioner brief: NDB overview D2020/017430

Key messages

- The OAIC published its latest six-month NDB Statistics report on 31 July 2020, for the period January to June 2020.
  - During this period, the OAIC received 518 notifications under the NDB Scheme.
  - This was a decrease of 3% when compared to the number of notifications received over the previous reporting period (July – December 2019) (532).
- Breaches resulting from malicious or criminal attacks (including cyber incidents) remain the largest source of data breaches (61%), with breaches resulting from human error accounting for 34% of all notified breaches. However in relation to the Health Sector, human error is the largest source of data breaches.
- The health sector is again the highest reporting sector, accounting for 22% of all breaches.
- The finance sector is the second highest, at 14%.
- Most NDB's (65%) involved 100 or less individuals, with contact information and identity information remaining the two most common type of personal information involved in a breach
  - **Contact information** includes information such as an individual's home address, phone number or email address.
  - **Identity information** refers to information that is used to confirm an individual's identity, such as passport number, driver licence number or other government identifiers such as social security number, tax file number or Medicare number. Over a third of data breaches notified during the period involved identity information.
- These trends have been broadly consistent since the scheme began.
- And while the OAIC has identified a steady increase in the number of notifications received across the first three quarters of 2020 – which includes the period of COVID-19 response arrangements – we have no evidence that COVID-19 has directly impacted on notifications to the OAIC, in terms of numbers, sectors, or causes.
- The NDB scheme has been extended to include certain conduct by the National COVIDSafe Data Store administrator, and state and territory health authorities under s 94S of the *Privacy Act*.

Critical issues

- Noting that the NDB Scheme commenced on 22 February 2018, the OAIC received:
  - 305 NDB notifications in FY2017-18
  - 950 notifications in FY2018-19 and

Commissioner brief: Summary of High Profile NDBs

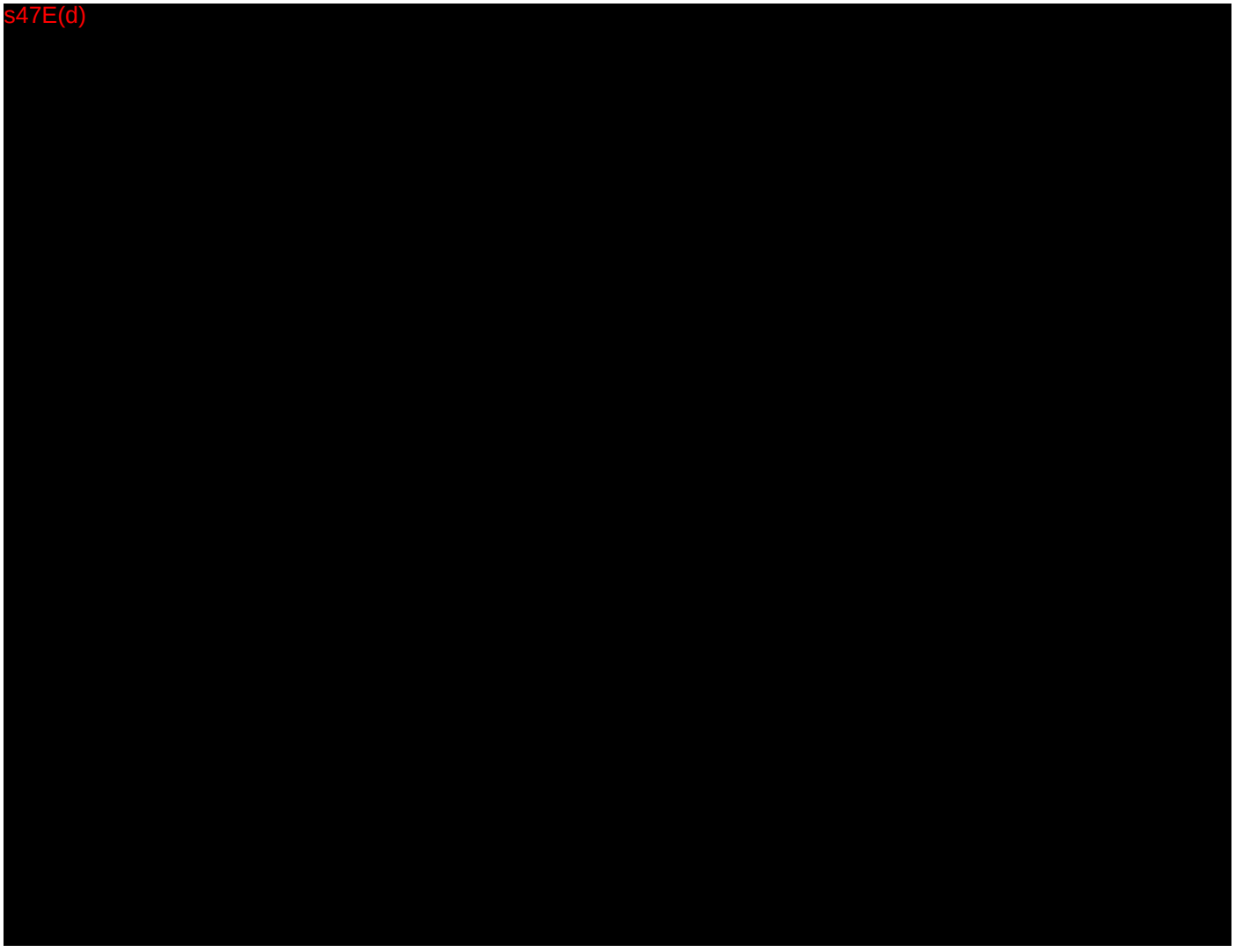
Key messages

- Throughout 2020 there has been sustained media interest in reporting data breaches, ensuring that there is public awareness of many Australian businesses experiencing a data breach.
- Most of the breaches that received significant media coverage in the last 12 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 issues

High Profile NDBs from 2020

s47E(d)



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

Key messages

- As of 30 September 2020, the OAIC has 19 Commissioner initiated preliminary inquiries and investigations (privacy CIIs) open, including privacy incidents that have attracted media interest or public concern.
- The OAIC handles these matters in accordance with the OAIC's *Privacy regulatory action policy* and *Guide to privacy regulatory action.*

Critical facts

- The Commissioner may make inquiries under s 42(2) of the *Privacy Act 1988* (Cth) (the Privacy Act) of any person for the purposes of determining whether to investigate an act or practice under s 40(2) of the Privacy Act.
- Under s 40(2) of the Privacy Act, the Commissioner may, on the Commissioner's own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of Australian Privacy Principle 1, where the Commissioner thinks it is desirable that the act or practice be investigated.
- When considering whether to investigate an act or practice under s 40(2), the Commissioner has regard to the factors outlined in paragraph 38 of our *Privacy regulatory action policy.* These factors include:
    - the seriousness of the incident or conduct to be investigated
    - the specific and general educational, deterrent or precedential value of the particular privacy regulatory action
    - whether the conduct is an isolated instance, or whether it indicates a potential systemic issue
    - the level of public interest or concern relating to the conduct, proposal or activity.
- Where a 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.

Commissioner brief: DHA representative complaint

Key messages

- The OAIC has a representative privacy complaint before it in relation to a data breach by the Department of Home Affairs (then DIBP) that occurred on 10 February 2014. The Department published a detention report on its website in error, which contained the personal information of persons who were in immigration detention facilities, alternative places of detention or under a residence determination as at 31 January 2014.
- A Commissioner Initiated Investigation into this matter was finalised in November 2014 and concluded that the Department had breached the Privacy Act by failing to appropriately secure (APP11), and by disclosing (APP6), personal information of immigration detainees.
- On 24 January 2018 the OAIC published a notice requesting that any individuals affected by the data breach provide evidence of loss or damage they have suffered. Submissions closed in April 2019.
- The OAIC is actively working with the parties to finalise the matter as soon as possible.

Critical facts

- The OAIC has a representative privacy complaint before it in relation to this matter.
- On 24 January 2018, the OAIC published a notice about the representative complaint (D2018/001498). The notice requested that any individuals affected by the data breach (class members) provide evidence to the OAIC of loss or damage they have suffered.
- Class members were initially given until 14 April 2018 to respond. The due date was subsequently extended on two occasions to 19 October 2018, based on submissions by representative groups, and in consultation with the Department.
- The Commissioner continued to accept responses after the deadline from persons who had outstanding information requests to the Department as at 19 October 2018, or had not received a response to their request for information from the Department by 10 September 2018. Class members who fell within these categories were permitted to provide a response within 40 days of receipt of the decision on their information request and the material the subject of that decision.
- The Commissioner also granted some class members a further 40 days to respond for each file released by the Department to them after 26 November 2018, and up to and including 31 January 2019.
- On 10 October 2018 the Commissioner made a decision to substitute the representative complainant with another class member, on the basis that the original representative complainant is deceased. The Commissioner considered submissions about this issue from two class members who sought to be substituted and substituted the person who was best able to represent the interests of the class.

Commissioner brief: Complaint backlog strategy

Key messages

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

Critical facts

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

Commissioner brief: Assessments program 2019-20 and 2020-21

Key messages

- The OAIC has a program of privacy assessments (or audits) to identify privacy risks in key programmes where agencies and organisations handle personal information. Where risks are identified, we make recommendations to address them.
- In the 2019-20 financial year focus areas included digital health, government data matching programs, education, finance[1], and telecommunications service providers' processes under the data retention scheme.
- We closed 14 assessments in the last financial year and we have 7 privacy assessments open currently: all carried over from previous financial years. The COVID-19 pandemic has impacted the way that the OAIC conducts assessments. We plan to begin assessments in several more areas of interest as 2020-21 progresses.
- Assessments for the 2020-21 financial year, including those required under memoranda of understanding (MOU) with federal government agencies and the Australian Capital Territory (ACT), will focus on:
    - digital health
    - Medicare data matching
    - border clearance processes
    - COVID app data
    - the Consumer Data Right (CDR)
    - as well as initiatives like the Australian Government Agencies Privacy Code and Notifiable Data Breaches Scheme.

Critical facts

Assessments

- Section 33C of the Privacy Act empowers the Commissioner (or delegate) to conduct an assessment in such manner as the Commissioner sees fit 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.
- Assessment findings are typically not disclosed publicly until an assessment report is published.
- Chapter 7 of the OAIC's *Guide to privacy regulatory action* sets out how OAIC staff exercise the Commissioner's assessment power.
- The majority of the OAIC's 2019-20 assessment program was specifically funded (through MOU arrangements or an appropriation). Staff also have regard to media

[1] These assessments relate to the functioning of the DVS/government's identity management: https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-the-oaics-assessment-of-privacy-policies-of-20-dvs-business-users-in-the-finance-sector/

Commissioner brief: Comprehensive Credit Reporting & Hardship

D2020/017436

Key messages

- The National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Bill 2019 (the draft Bill) was introduced into Parliament in December 2019. The Bill introduces mandatory comprehensive credit reporting (CCR) and hardship reporting reforms and is currently before the Senate (as at 29 September 2020).
- The OAIC has previously made a submission to the Treasury on the exposure draft of the Bill (Extracted at **Attachment 1**).
- Our chief interest has been to ensure that any changes maintain an appropriate balance between facilitating an efficient credit reporting system and protecting individuals' privacy. This is particularly important given that the Bill introduces a new type of credit information, financial hardship information.
- Under the proposed changes, our existing role in overseeing the consumer credit reporting system would continue – that includes working with entities to facilitate compliance and best practice, and using our investigative and enforcement powers in cases where a privacy breach may have occurred.
- The explanatory memorandum to the draft Bill anticipates that changes will be required to the Privacy (Credit Reporting) Code 2014 (the CR Code) which we anticipate will occur in 2021 or 2022.

Critical issues

- The proposed bill will introduce financial hardship into the credit reporting system.
- This reform has attracted strong views from industry and consumer groups during the hardship review run by the Attorney-General's Department.
- The reforms will also require the Commissioner to approve a change to the CR Code. This may be contentious given the controversial nature of the reform.
- The mandatory comprehensive credit reporting aspect of the reform will also result in the bulk disclosure of credit information to CRBs which carries privacy risks.

Possible questions

- ***What is the OAIC's oversight role for proposed mandatory CCR?*** My existing oversight of the consumer credit reporting system would continue under the mandatory CCR regime. These include powers that allow my office to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred.
- ***What protections will there be for financial hardship information?*** Financial hardship information will be subject to the additional protections currently provided for

Commissioner brief: Consumer Data Right

Key messages

- The 'Consumer Data Right' (CDR) allows consumers to direct a business to securely transfer their data to an accredited data recipient. It commenced in the banking sector on 1 July 2020 and will apply economy-wide, sector-by-sector as designated by the Treasurer.
- The Office of the Australian Information Commissioner (OAIC) and Australian Competition and Consumer Commission (ACCC) co-regulate the CDR system. The OAIC is the primary complaint-handler and has responsibility for regulating the privacy aspects of the system.
- The OAIC and ACCC continue to work closely on implementation of the CDR, to ensure a 'no wrong door' approach to receiving consumer complaints and enquiries. Since 1 July 2020, consumers and CDR participants have been able to lodge enquiries, reports and complaints via a central portal (the CDR.gov.au website).
- The OAIC has also prepared a suite of guidance to assist regulated entities and consumers to understand their rights and obligations under the CDR. This has included the release of guidelines on the privacy safeguards to assist industry in understanding their privacy obligations.

Critical Issues

- The CDR system seeks to give consumers greater control over how their data is used and disclosed. It commenced in the banking sector on 1 July 2020 and will apply in certain sectors of the Australian economy, as designated by the Treasurer. The energy sector was designated on 26 June 2020.
- The CDR allows consumers to direct a business to securely transfer their data to an accredited third-party data recipient. Both individuals and businesses are able to transfer their data under the CDR.
- The OAIC has worked closely with the ACCC in the development of the CDR Rules, which entered into force on 6 February 2020. The CDR Rules complement Part IVD of the *Competition and Consumer Act 2010* (Cth) (Competition and Consumer Act), including by defining the elements for consent, outlining the accreditation framework, and elaborating on the Privacy Safeguards. The OAIC will continue to work closely with the ACCC on any further updates to the CDR Rules.
- On 24 February 2020 the OAIC published the CDR Privacy Safeguard Guidelines to assist industry in interpreting their privacy obligations under the CDR following consultation with industry, the ACCC and other key stakeholders. An updated version of the Guidelines was published in July 2020. The OAIC has also published a suite of guidance materials for consumers on its website.

Commissioner brief: Data Encryption

Key messages

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

Critical facts

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

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

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

Key messages

- 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 have undertaken a program of 6 assessments to examine government data-matching practices. Four assessments have been finalised and 2 assessments are in the reporting stage.
- The OAIC's assessment of Department of Human Services' (DHS) Pay-As-You-Go (PAYG) program found that DHS has taken some steps to address issues with the quality of the personal information it collects, but also identified potential privacy risks associated with the PAYG program and made 5 recommendations to address these risks. All recommendations have been implemented.
- We will continue to progress the data matching assessments of DHS (now Services Australia) and other government agencies and will publish our reports on our website when they are finalised.

Critical facts

- The OAIC has regulatory oversight of 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, being used only by the Department of Veterans' Affairs (DVA).
    - Part VIIIA of the *National Health Act 1953*
        - matching of information held by the Chief Executive Medicare for the purposes of ensuring the integrity of Medicare programs including the Medicare Benefits Schedule and Pharmaceutical Benefits Scheme (MBS/PBS.[1]
    - the voluntary Guidelines on Data Matching in Australian Government Administration (voluntary guidelines)

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

Commissioner brief: Data Retention Regime

Key messages

- The data retention regime (Regime) under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) requires telecommunication service providers (service providers) to retain certain types of metadata relating to telecommunication services for a minimum of two years. Under sections 306 and 306A of the *Telecommunications Act 1997* (Telecommunications Act), the OAIC has the role of overseeing record keeping practices of service providers when they disclose information to law enforcement in relation to the Regime.
- The OAIC has conducted inspections of these records at 4 telecommunications service providers in 2015 and 2017 and has conducted privacy assessments of these providers' implementation of their requirements under the Regime across the 2017-18 and 2018-19 financial years.[1]
- The OAIC published a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) statutory review of the Regime in July 2019.[2]
    - We recommended that amendments be made to the TIA Act to ensure the proportionality of the Regime, and for an appropriate balance to be struck between Australian citizens' right to privacy and law enforcement and national security objectives. The OAIC also provided evidence to the PJCIS at a public hearing held on 7 February 2020 and made a supplementary submission to the PJCIS on 21 February 2020.

Critical facts

- Since 2015, the OAIC has undertaken a program of work to identify and mitigate key privacy risks in the information handling lifecycle of retained data under the Regime. This includes undertaking inspections and follow-up assessments of Telstra, Optus, Vodafone, and TPG's record keeping practices under s309 of the Telecommunications Act in 2015[3] and 2017.[4] The OAIC has an oversight role under the Telecommunications Act in relation to these records.
- In 2016-2017, the OAIC assessed 4 service providers' information security practices under Australian Privacy Principle (APP) 11, when disclosing personal information under the TIA Act (conducted prior to the commencement of the Regime).[5]

---

[1] https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-oaic-assessments-of-telecommunications-organisations-information-security-under-the-telecommunications-interception-and-access-act-2015-telstra-vodafone-optus-tpg/.

[2] https://www.oaic.gov.au/engage-with-us/submissions/review-of-the-mandatory-data-retention-Regime-submission-to-the-parliamentary-joint-committee-on-intelligence-and-security-pjcis/.

[3] https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-oaics-inspection-of-telecommunications-organisations-records-of-disclosure-under-the-telecommunications-act/.

[4]

[5] https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-oaic-assessment-of-telecommunication-organisations-information-security-practices-when-disclosing-personal-information-under-the-telecommunications-interception-and-access-act-1979/.

Commissioner brief: Biometrics

Key messages

- The OAIC has privacy oversight of Identity-Matching Services such as the National Facial Biometric Matching Capability (NFBMC) and the National Drivers Licence Facial Recognition Solution (NDLFRS), which involve the collection and handling of large volumes of sensitive information afforded higher protections under the *Privacy Act 1988* (Cth) (Privacy Act).
- Following recommendations from the Parliamentary Joint Committee on Security and Intelligence's (PJCIS's) advisory report on the *Identity-Matching Services Bill 2019* (the IMS Bill),[1] we continue to engage with the Department of Home Affairs (Home Affairs) to incorporate additional safeguards into the draft legislation and the NFBMC's associated governance framework. s47E(d) [redacted]
- We have an MoU with Home Affairs to conduct two privacy assessments, one of each of the NFBMC and NDLFRS respectively.
- We have opened a joint investigation with the UK's Information Commissioner's Office (ICO) into the personal information handling practices of Clearview AI, focusing on the company's use of 'scraped' data and the biometrics of individuals. The investigation highlights the importance of enforcement cooperation in protecting the personal information of Australian and UK citizens.

Critical facts

- Home Affairs operates the NFBMC to prevent identity crime, and for general law enforcement, national and protective security, and identity verification purposes. The NFBMC facilitates the sharing of facial images between the Commonwealth and states and territories, through its identity-matching services.
    - Services include the Face Verification Service ('one to one' matching) and Face Identification Service ('one to many' matching). The NDLFRS (as part of the NFBMC) will be a centralised database of driver licence holdings from every state and territory.
- The IMS Bill and the *Australian Passports Amendment (Identity*-Matching *Services) Bill 2019* provide the legal framework for Home Affairs to operate these identity-matching services. The OAIC made a submission to the PJCIS in 2018,[2] recommending that Home Affairs specified the privacy protections that would apply to the NFBMC within this overarching legislation. The OAIC has also provided Home Affairs with a range of policy advice in relation to the NFBMC's governance documents. s47E(d) [redacted]

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

Commissioner brief: My Health Record

Key messages

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

Commissioner brief: National Data Commissioner

Key messages

- The Office of the Australian Information Commissioner (OAIC) is supportive of the Productivity Commission's (PC) underlying policy objectives in its *Data Availability and Use Inquiry* report, which seek to enable better use of, and greater access to, valuable government-held data.
- The Office of the National Data Commissioner (ONSC) has now published the Exposure Draft of the Data Availability and Transparency (DAT) Bill, which aims to address the recommendations of the Productivity Commission. The Bill aims to strengthen protections around the sharing of Commonwealth datasets for particular purposes and includes privacy and security protections that are specific to this data sharing context.
- The Commonwealth Privacy Act or equivalent State/Territory privacy legislation will continue to apply where data sets that are shared under this framework include personal information.
- The OAIC intends to make a public submission to the consultation that will identify opportunities to further enhance the privacy protections in framework, for example by placing a greater emphasis on agencies using datasets that do not contain personal information, and explicitly requiring Accredited Entities to tell Data Custodians if they have experienced a data breach.
- The OAIC welcomes the collaborative approach that the Office of the National Data Commissioner has taken to developing this data sharing framework so far. We look forward to continuing to work with the ONDC to ensure that data can be shared safely and securely under this framework, and in line with community expectations.

Critical Issues

- The ONDC published the Exposure draft of the DAT legislative package on 14 September. Since publication, there have been some media articles published about the framework, some of which have raised questions about the privacy and security aspects of the data sharing proposals e.g. citing lack of trust in government agencies to handle data safely, based on past data incidents, no ability for individuals to object or appeal decisions to share data.[1] Other media articles are more neutral, and report the outline of the framework as presented by the consultation paper.[2]
- The OAIC supports better use of government-held data in the public interest but will continue to advocate for the strongest privacy safeguards in the Data Availability and Transparency framework.
- The OAIC continues to work closely with the ONDC as it develops the new system, including by providing informal comments, making formal submissions, and through

[1] https://www.abc.net.au/news/2020-09-16/government-draft-law-share-personal-data-between-agencies/12666792
[2] https://www.zdnet.com/article/the-idea-of-consent-works-its-way-back-into-australias-data-sharing-bill/

Commissioner brief: Privacy law reform

Key messages

- The OAIC welcomes the Government's commitment to strengthen the Privacy Act to ensure Australians' personal information is protected in the digital age, including the introduction of higher penalties for privacy breaches, a code of practice for digital platforms and a review of the Privacy Act.
- The reforms outlined in the Government's response to the Digital Platforms Inquiry final report will ensure that our regulatory framework protects personal information into the future and holds organisations to account.
- The OAIC looks forward to continuing to work closely with the Attorney-General's Department during its review of the Privacy Act throughout 2020 and 2021.

Critical Issues

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

Possible questions

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

Commissioner brief: International regulatory developments

Key messages

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

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

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

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

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

Commissioner brief: Digital Identity

Key messages

- The OAIC welcomes the development of legislation for the Digital Identity scheme.[1]
- It is important that the legislation contains strong privacy protections to ensure that the identity information of Australians is protected, regardless of which type of entity is using that information.
- We consider that it is appropriate for the OAIC to regulate the additional privacy protections that are introduced through legislation, and that participants that are not currently covered by the Privacy Act or comparable privacy law must opt in to the Act to ensure that there is a consistent application of privacy protection.
- The Digital Transformation Authority (DTA) has also received funding to expand Digital Identity to connect a greater number of services to the system (including state and territory services) over the next three years. The OAIC will receive funding in the 2021-22 financial year to undertake two privacy assessments (audits) of the system and develop guidance materials.[2]
- We welcome the opportunity to engage with the DTA in its development of a privacy protective scheme through our monitoring, guidance and advice functions.

Critical Issues

- The DTA is currently undertaking two main areas of work in relation to Digital Identity:
    - Developing legislation to underpin this scheme. This will enable the scheme to be used by State and Territory governments and the private sector, in addition to Federal Government agencies. It is proposed that the legislation will include additional privacy protections related to the scheme.
    - The DTA received funding in the 2020-21 Budget to expand the scheme over the next three years. This will include the rollout of the scheme to MyGov and a greater number of consumer-facing services integrated with the scheme.
- The OAIC is involved in both of these projects:

---

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

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

Commissioner brief: Coronavirus – Emergency declaration

Key messages

- The Privacy Act is not a barrier to necessary information sharing in a declared emergency or disaster.
- Part VIA of the Privacy Act contains special provisions for the collection, use and disclosure of personal information in an emergency or disaster that affects Australians in Australia or overseas.
- These provisions take effect if the Prime Minister or Minister responsible for the Privacy Act (the Attorney-General) declares an emergency under Part VIA of the Privacy Act.
- Entities will not be in breach of the Australian Privacy Principles (APPs) if they have complied with Part VIA.
- Coronavirus has NOT been declared an emergency under Part VIA of the Privacy Act.

Critical facts

Government response in Australia

- Neither the Prime Minister nor the Attorney-General has declared an emergency under Part VIA of the Privacy Act.

- However, the Prime Minister announced activation of the Australian Health Sector Emergency Response Plan for Novel Coronavirus (COVID-19): 'the emergency response plan' on 27 February 2020.

- The emergency response plan is a living document designed to guide the Australian health sector response. It states that:

    - Australia has taken a precautionary approach to coronavirus 'in line with preparedness and response guidance for a pandemic'
    - the coronavirus outbreak represents a significant risk to Australia, with the 'potential to cause high levels of morbidity and mortality and to disrupt our community socially and economically'
    - communication is a priority and the emergency response plan specifically addresses information sharing between stakeholders involved in managing the response.

Overview of Part VIA of the Privacy Act and application to coronavirus outbreak

- Part VIA of the Privacy Act regulates how entities—including persons, agencies, and organisations— may collect, use and disclose personal information in a declared emergency or disaster.

Commissioner brief: Alinta Energy

Key messages

- The OAIC commenced preliminary inquiries into Alinta Energy's handling of Australians' personal information on 3 March 2020.

s 47E(d) [redacted]

- The APPs do not prevent an organisation from sending personal information overseas. However, organisations need to carefully consider steps that may need to be taken to comply with the APPs when doing so.

Critical facts

- On 2 March 2020, the media reported a whistle blower raising issues regarding Alinta Energy's privacy compliance. In particular, the reports referred to an internal audit by Ernst & Young into Alinta Energy's privacy compliance.
- On 3 March 2020 we commenced preliminary inquiries with Alinta Energy, requesting they answer a number of questions. s 47E(d) [redacted]

s 47E(d) [redacted]

- The Senate Economic References Committee inquiry into foreign investment proposals has a focus on Alinta Energy, and the Commissioner appeared before this inquiry on 15 May 2020. The report for this inquiry is due to be presented by 16 December 2020.

Commissioner brief: COVIDSafe and Part VIIA of the Privacy Act

Key messages

- In May 2020 the Privacy Act 1988 (Cth) (Privacy Act) was amended to insert a legal framework of privacy protections established under Part VIIIA to protect COVID app data.
- The OAIC has engaged extensively with key stakeholders in relation to the development and deployment of the COVIDSafe app.
- The OAIC has commenced a series of assessments under Part VIIIA examining the information lifecycle of COVID app data.

Critical Issues

COVIDSafe policy advice

- Pursuant to my advice-related functions under section 28B of the Privacy Act, my office has engaged extensively with key stakeholders in relation to the development and deployment of the COVIDSafe app.
- My office proactively reached out to the responsible agencies, including the Digital Transformation Agency (DTA) and the Department of Health, in late March and early April 2020, to offer our assistance and privacy expertise to the development of a national contact tracing app for Australia.
- My office provided advice and guidance in relation to the scope and recommendations of the Privacy Impact Assessment (PIA) that was commissioned by the Department of Health. I was pleased to see that the Government accepted all of the recommendations of the PIA, including a key recommendation that important privacy protections – such as purpose limitation, prohibited uses and disclosures and accountability and oversight mechanisms – be enshrined in a legislative framework.
- I have sought regular updates from the Department of Health in relation to the implementation of the PIA recommendations. s47E(d) [redacted]
- My office worked closely with the Department of Health and the Attorney-General's Department in relation to the drafting of the *Privacy Amendment (Public Health Contact Information) Act 2020*, which commenced on 16 May 2020.
- The new law provides an expanded regulatory oversight role for the OAIC to ensure personal information is handled in accordance with the legislation's requirements. This

s47E(d)

[redacted]

Commissioner brief: FOI IC reviews

Key messages

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

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