	Privacy Folder
1	HTB-01: Law reform
2	HTB-02: Significant privacy investigations
3	HTB-06: Amex matters
4	Amex
5	Proactive regulatory action
6	Determinations
7	Omnibus – PSM matters
8	Clearview AI
9	Tracking Pixels
10	Property Lovers
11	Online Safety Amendment (Social Media Minimum Age) Bill 2024
12	Services Australia matters
13	DVA Mates
14	Meta Platforms - Enforceable Undertaking
15	Court Data Australia
16	Qantas
17	FRT
18	NDB Scheme
19	Consumer Data Right
20	Credit reporting and hardship - review of Part IIIA
21	Digital Identity
22	My Health Record
23	Digital Platform Regulators Forum
24	AI
25	Vehicle privacy
26	Children's Code

HOT TOPIC BRIEF OAIC-01

Law reform

PA-Office of the Australian Information Commissioner

Implementation of Tranche 1 privacy reforms is underway. Tranche 2 privacy reforms are under development. Retailers (Bunnings) have called for law reform to allow Facial Recognition Technology to be widely used in stores. The Productivity Commission has recommended reforms to the *Privacy Act*. The Government has announced reforms to the *Freedom of Information Act*.

Privacy

Implementation of Tranche 1 Privacy Act reforms

- ***Children's Online Privacy Code***: OAIC commenced consultation with children and parents in May 2025, and consultation with industry, civil society, and other stakeholders in June 2025. OAIC is analysing feedback and will consult on a draft Code in early 2026.
- ***Tort of serious invasions of privacy***: OAIC does not have a direct role, but the Information Commissioner may, with the leave of the court, appear in proceedings.
- ***Automated decision-making:*** From 10 December 2026, privacy policies will need to note the use of automated decisions which use personal information and may significantly affect the rights/interests of an individual. OAIC consultation begins in early 2026.

Future reforms (Tranche 2)

- The Attorney-General's Department (AGD) is leading reforms and consultations to ensure legal frameworks remain fit for purpose and robust. Policy questions regarding Tranche 2 reforms should be directed to AGD.

Facial recognition technology (FRT) in retail operations – industry calls for law reform

- In November 2024, the Privacy Commissioner found Bunnings Group breached Australians' privacy by collecting personal and sensitive information through an FRT system. Bunnings' appeal to the ART was heard by the Guidance and Review Panel on 22, 23, 24 and 26 October 2025. The Tribunal reserved its decision.
- s47B Woolworths obtained 14 orders in the ACT, which it states has reduced reoffending by 99 per cent.

- In September 2025, the Privacy Commissioner decided Kmart Australia Limited breached Australians' privacy by collecting personal and sensitive information using an FRT system focused on refund fraud. Kmart lodged an application for merits review in the ART.
- On 13 November 2025 the Tribunal adjourned with orders including: The parties are not required to take any further step in this proceeding for 21 days commencing on the day that the GAP delivers its decision and reasons in *Bunnings*.

Anti-money laundering and counter terrorism financing reforms

- The OAIC is updating guidance (by December 2025) for entities subject to the Privacy Act as part of reforms to the Tranche 2 AML/CTF reforms commencing 1 July 2026.
- The OAIC did not receive additional funding to regulate the approx. 120,000 new entities.

Productivity Commission interim report – recommended legislative privacy reform

- The Productivity Commission interim report (August 2025) *Harnessing data and digital technology* recommended the Government implement an alternative compliance pathway allowing entities to fulfil privacy obligations by meeting a 'best interests' test, and not implement a right to erasure. The OAIC made a submission in response.
- The Privacy Commissioner (August 2025) published an opinion piece that while the Privacy Act requires updates to ensure it remains fit for the digital age, the alternative best-interest compliance pathway is "unworkable" if it allows entities to withhold basic controls/protections currently in the law. Privacy Act Tranche 2 reforms will increase the regulatory focus on outcomes without radically moving away from a rights-based regime.
- 62 per cent of Australians see the protection of their personal information as a major concern in their life, while only a third feel in control of their data privacy. 84 per cent want more control and choice over collection and use of their personal information.[1]

Freedom of Information

Freedom of Information (FOI) reforms

- The OAIC was consulted during the drafting of the Freedom of Information Amendment Bill (**the Bill)** in July and August 2025 and commented on implementation issues. We received a consolidated draft of the Bill on 30 August 2025.

[1] OAIC, Australian Community Attitudes to Privacy Survey 2023

- The introduction of the Bill and referral to the Senate Committee provides an important opportunity for a public debate on the best way to improve the FOI scheme.
- The OAIC's submission to the Inquiry on 2 October 2025 focused on the right to access information, the operation of the current Act, and some operational implications:
  - FOI applications made to agencies and ministers increased by 8,750, or 25 per cent, in 2024-25 – to a total of 43,456 requests, the highest number on record.
  - Should the reforms be enacted, there will be two systems of FOI law operating concurrently until legacy cases are finalised. Two different legal frameworks with different requirements will apply, depending on when a request or review application was made.
  - The proposed amendments, and any transition period, will have significant resourcing and regulatory impacts for the OAIC.
  - Implementation will require significant changes to our case management procedures, guidance and templates, Practice Directions, ICT systems, smart forms and public facing information.
- The OAIC appeared at the Senate Inquiry on 17 October 2025, and received questions related to resourcing, consultation on Bill development, document management systems in agencies, and key statistics and responded to questions on notice including
- Bill development, resourcing, vexatious applications and the use of bots.

Community attitudes to information access

- The Information Access – Community Study Report released in September 2025 found that, 96 per cent of Australians (up five percentage points from 2023), regardless of age, gender, or location feel their right to access government information is important (58 per cent very important; 38 per cent quite important).

Version: 2	Cleared by: Elizabeth Tydd	Action officer: Marcel Savary
Current at: 17/11/2025	Phone number: s22	Action officer number: s22

HOT TOPIC BRIEF OAIC-02

Significant privacy investigations

PA-Office of the Australian Information Commissioner

This brief provides a summary of recent significant privacy-related Commissioner initiated investigations that have been made public. It is the OAIC's usual practice to limit public comment in relation to ongoing investigations.

CURRENT SIGNIFICANT COMMISSIONER INITIATED INVESTIGATIONS

Respondent	Bunnings Group Limited & Kmart Australia Limited		
Investigation description	Personal information handling practices arising from the use of in-store facial recognition technology.		
Start Date	1 July 2022	**APPs**	APP 1, APP 3.3 and APP 5
Status	Bunnings determination made on 29 October 2024. Kmart determination made on 26 August 2025. Both determinations included declarations that the respondents interfered with the privacy of individuals whose personal information it collected through its FRT system, must not repeat or continue the acts or practices, and must publish a statement on their website setting out the determination, details of the breach, and advice for customers. Bunnings sought review of the determination in the Administrative Review Tribunal (ART). Bunnings' review was heard by the Guidance and Appeals Panel (GAP) of the ART on 22, 23, 24 and 26 October 2025. The GAP reserved its decision. Kmart has filed for review but has not yet been set down.		
Respondent	Singtel Optus Pty Ltd, Optus Mobile Pty Ltd and Optus Internet Pty Ltd (data breach matter).		
Investigation description	Data breach involving the unauthorised access to Optus systems and exfiltration of personal information of more than 9.5 million individuals, including driver licence, passport and Medicare numbers.		
Start Date	11 October 2022	**APPs**	APP 1, APP 3.2, APP 11.1 and APP 11.2.

Status	Civil penalty proceedings filed in the Federal Court against Singtel Optus Pty Limited and Optus Systems Pty Limited on 8 August 2025, for breaches of APP 11.1. The next Case Management Hearing is on 12 December 2025.		
Respondent	Medibank		
Investigation description	Data breach involving unauthorised access to Medibank's systems and exfiltration of personal information, affecting approximately 9.7 million individuals.		
Start Date	1 December 2022	**APPs**	APP 1 and APP 11.1
Status	Civil penalty proceedings filed in the Federal Court against Medibank on 5 June 2024, for breaches of APP 11.1. The next case management hearing is on 21 November 2025.		
Respondent	Australian Clinical Labs (ACL).		
Investigation description	Data breach involving unauthorised access and exfiltration of personal information of patients of Medlab, a pathology business owned by ACL.		
Start Date	2 December 2022.	**APPs under investigation**	APP 1, APP 11.1 and compliance with Notifiable Data Breaches Scheme.
Status	On 8 October 2025, the Federal Court ordered ACL pay and agreed penalty of $5.8m in civil penalties for beaches of APP 11.1, s 26WH and s 26WK.		
Respondent	American Express		
Investigation description	Arising from an individual complaint that alleges inadequate technical security controls such as access logging and access limitation.		
Start Date	23 March 2023	**APPs**	APP 11.1

Status	Investigation ongoing, however extensive investigative steps have raised systemic issues. A Preliminary View has been issued to the parties. The preliminary view, which is usually kept private to the parties, was disclosed to the media and reported in October 2025. The OAIC has made public commentary clarifying the status of the preliminary view and noting no final decision has been made. Procedural steps have been communicated to parties and resultant action is underway. It is expected to conclude end of 2025.		
Respondent	Latitude Financial Services		
Investigation description	Data breach involving unauthorised access to Latitude's systems and exfiltration of personal information of 14.1 million individuals in Australia and New Zealand.		
Start Date	9 May 2023	**APPs**	APP 3, APP 11.1 and APP 11.2
Status	Investigation ongoing. OAIC is engaging closely with AFCA and other regulators seized of this matter.		
Respondent	HWL Ebsworth Lawyers		
Investigation description	Data breach involving unauthorised access and exfiltration of data from HWLE's systems.		
Start Date	20 February 2024	**APPs under investigation**	APP 11.1
Status	Investigation ongoing.		
Respondent	I-MED Radiology Network Limited / Harrison-AI Pty Ltd		
Investigation description	Preliminary inquiries into the disclosure of medical scans to a third-party entity for the purpose of training an AI model.		
Start Date	27 September 2024	**APPs under investigation**	APP 5 and APP6

Current Status	Report into preliminary inquiries published on 31 July 2025. Commissioner was satisfied that the patient data had been sufficiently de-identified that it was no longer personal information for the purposes of the Privacy Act.

Version: 1	Cleared by: Elizabeth Tydd	Action officer: s22
Current at: 14/11/2025	Phone number: s22	Action officer number: s22

HOT TOPIC BRIEF OAIC-06
AMEX Matter

PA-Office of the Australian Information Commissioner

In 2022 the OAIC received a complaint against American Express (**AMEX**) alleging improper access to the complainant's personal information by an employee of AMEX, who is the complainant's ex-partner. Extensive investigative steps have been taken on this matter. A preliminary view has been provided to the parties.

In October 2025, articles were published in Fairfax Media outlets regarding the OAIC's investigation into AMEX. The articles canvassed the OAIC's Preliminary View, AMEX's response, and broader commentary on privacy regulation, enforcement, and the protection of personal information in Australia. Procedural steps have been communicated to parties and resultant action is underway. It is expected the complaint investigation will conclude by the end of 2025.

Background

- In 2022 the OAIC received a complaint against American Express (**AMEX**) which alleged improper access to a complainant's personal information by an AMEX employee, who the complainant had previously been romantically involved with.

Investigation of complaint

- The OAIC commenced a complaint investigation in March 2023. Extensive investigative steps have been taken on this matter which raises systemic and individual issues. A preliminary view containing the Commissioner's preliminary view on the complaint and proposed declarations was provided to the complaint parties who were invited to provide written submissions and any further information before a decision was made.

Publication of preliminary view and next steps

- The preliminary view, which is usually kept private to the parties, was provided by the complainant to Fairfax media which published parts of the preliminary view in October 2025. The OAIC has made public commentary clarifying the status of the preliminary view and noting no final decision has been made.

Parliamentarian interest

- Senator Shoebridge has shown interest in this matter and has made regular enquiries to the OAIC at Senate Estimates about its progress. Fairfax Media reported in October that Minister Plibersek has written to the Commonwealth Ombudsman in 2024 asking that the Ombudsman consider a complaint made about the OAIC's handling of this matter.

Ombudsman investigation and next steps

- On 11 November 2025, the OAIC was informed that the Ombudsman will investigate a complaint about the OAIC's handling of this matter. The OAIC welcomes the Ombudsman's involvement and will cooperate fully with its investigation. The OAIC will carefully consider and act on any findings or recommendations the Ombudsman may make following the investigation.
- OAIC is working to finalise the complaint as quickly as possible. Procedural steps have been communicated to parties and resultant action is underway. It is expected the complaint investigation will conclude by the end of 2025.

Version: 1	Cleared by: Elizabeth Tydd	Action officer: Annan Boag
Current at: 14/11/2025	Phone number: s22	Action officer number: s22

ESTIMATES BRIEF: MATTER

Respondent name: American Express (Amex) Australia

Type: Investigation, determination

Key details			
When did OAIC learn of matter?	24 November 2022		
Origin	Complaint		
Is there an issue in the public domain?	Media reporting, statement on OAIC website, questions from Senators in Senate Estimates		
Jurisdiction	General privacy - APPs		
Responsible Branch & team	Regulatory Action Division, Investigations Team		
Content author	s22	Phone	s22
Clearance by	Rowena Park	Phone	s22
Brief current at	**21 November 2025**		

Key talking points

- The OAIC commenced a complaint investigation on 23 March 2023. Extensive investigative steps have been taken on this matter which raises systemic and individual issues. It is expected the complaint investigation will conclude by the end of 2025.
- Part of the preliminary view, which is usually kept private to the parties, was published by Fairfax media in October 2025. The OAIC has made public commentary clarifying the status of the preliminary view and noting no final decision has been made.
- Privacy Commissioner Carly Kind had a telephone call with the complainant on 3 November 2025.

Brief overview of matter

- On 24 November 2022, OAIC received a complaint against American Express (**AMEX**) which alleged improper access to a complainant's personal information by an AMEX employee, who the complainant had previously been romantically involved with.
- The complaint alleged contravention of APP 11.1 in relation to a range of allegedly inadequate technical security controls, including access logging and access limitation. The complainant also alleged that AMEX failed to meet the requirements of the notifiable data breaches scheme.

Current action

Investigation of complaint

- The OAIC commenced a complaint investigation on 23 March 2023. Extensive investigative steps have been taken on this matter which raises systemic and individual issues. A preliminary view containing the Commissioner's preliminary view on the complaint and proposed declarations was provided to the complaint parties who were invited to provide written submissions and any further information before a decision was made.

Recent developments

Publication of preliminary view and next steps

- The preliminary view, which is usually kept private to the parties, was provided by the complainant to Fairfax media which published parts of the preliminary view in October 2025. The OAIC has made public commentary clarifying the status of the preliminary view and noting no final decision has been made.

Ombudsman investigation and next steps

- On 11 November 2025, the OAIC was informed that the Ombudsman will investigate a complaint about the OAIC's handling of this matter. The OAIC welcomes the Ombudsman's involvement and will cooperate fully with its investigation. The OAIC will carefully consider and act on any findings or recommendations the Ombudsman may make following the investigation.

Expected next steps/dates

- OAIC is working to finalise the complaint as quickly as possible. Procedural steps have been communicated to parties and resultant action is underway. It is expected the complaint investigation will conclude by the end of 2025.

Background: public matters only

Issues of note for OAIC

Correspondence with members of parliament

- Senator Shoebridge has shown interest in this matter and has made regular enquiries to the OAIC at Senate Estimates about its progress. Fairfax Media reported in October that Minister Plibersek has written to the Commonwealth Ombudsman in 2024 asking that the Ombudsman consider a complaint made about the OAIC's handling of this matter.

ESTIMATES BRIEF: OTHER

Subject: Proactive regulatory action
Type: Brief

Key details			
When did OAIC learn of matter?	N/A		
Is there an issue in the public domain?	Yes		
Jurisdiction	AIC Act, FOI Act and Privacy Act		
Responsible Branch & team	Regulatory Action Division		
Content author	Annan Boag	Phone	
Clearance by	Rowena Park	Phone	s22
Brief current at	13 November 2025		

Key talking points

- The OAIC has a wide range of regulatory powers and oversees the information handling practices of the entire Commonwealth public sector, all medium and large businesses, and many small businesses.
- The OAIC is a risk-based and harm-focused regulator, directing its actions where they will have the greatest impact.
- Policy decisions and significant actions are made by OAIC Commissioners and the Regulatory Board, while decisions on specific matters follow the OAIC's regulatory policy framework.
- This approach ensures the OAIC's limited resources are applied proportionately and achieve maximum impact.

OAIC regulatory action

- The OAIC has a wide range of powers to take proactive regulatory action. These include powers to work with regulated organisations to encourage FOI and privacy best practice, to monitor and report on FOI and privacy matters, to investigate alleged contraventions of FOI and privacy legislation, and to take enforcement action where contraventions are found.
- These powers are detailed in the OAIC's Regulatory Action Policies.
- The OAIC regulates the entire Commonwealth public sector (for FOI, privacy, and Information Commissioner functions), and most of the private sector, including all businesses with an annual turnover of more than $3 million and many other categories of smaller businesses (for privacy).

Policy framework and approach to deciding what regulatory action to take

- The OAIC's *Statement of Regulatory Approach*,[1] issued in 2024, defines the OAIC's regulatory approach: a proactive and harm-focused approach that prioritises efforts where they will have the greatest impact in reducing risks to the community.
- The Statement of Regulatory Approach is supplemented by an *FOI Regulatory Action Policy* and *Privacy Regulatory Action Policy*, which sets out the range of powers available to the OAIC and circumstances in which it may use them. These documents were last substantively updated in 2020 and 2022 respectively, and are currently under review.

[1] https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/statement-of-regulatory-approach.

- The OAIC also publishes FOI and Privacy *Guides to Regulatory Action*, describing processes for the OAIC when an information officer or their delegate is exercising these powers. These documents are updated on a chapter-by-chapter basis with the most recent updates completed in 2025.

- The OAIC publishes *Regulatory Priorities*[2], most recently published in July 2025, which list the matters OAIC has identified as most needing regulatory attention. Current regulatory priorities are:

    - Rebalancing power and information asymmetries
    - Rights preservation in new and emerging technologies
    - Strengthening the information governance of the Australian Public Service
    - Ensuring timely access to government information

Governance approach

- OAIC has three statutory decision-makers: the Information Commissioner, FOI Commissioner, and Privacy Commissioner. Each can make decisions independently, but actions are coordinated through the OAIC Governance Framework.

- Individual matters are assessed against criteria in the Statement of Regulatory Approach. Decisions are made by Commissioners or delegates depending on the issue and power involved.

[2] https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/oaic-regulatory-priorities.

- The Regulatory Board, chaired by the Information Commissioner, is the primary forum for significant regulatory decisions. It sets policies and decides on major actions, such as civil penalty proceedings, and commencing resource intensive proactive regulatory action.
- This approach ensures OAIC's limited resources are applied proportionately and achieve maximum impact.

Appendix: OAIC regulatory powers

- The OAIC has a range of proactive and reactive regulatory powers, which are detailed in the OAIC's Privacy and FOI Regulatory Action Policy.

- The *FOI Act 1982* confers on OAIC's Commissioners powers to:[3]
    - review FOI decisions of agencies and ministers
    - investigate FOI complaints or investigate on the Commissioner's own initiative
    - issue FOI Guidelines
    - consider extension of time applications
    - consider vexatious applicant declarations
    - make disclosure log determinations
    - oversee the Information publication scheme (IPS)
    - raise awareness of FOI and educate Australians and agencies about their rights and obligations
    - monitor agencies' compliance with the FOI Act
    - compile FOI data and assess trends
    - make recommendations on the operation of the FOI Act

- In relation to an IC review, the Information Commissioner can exercise enforcement powers to compel compliance with, or where relevant, to seek prosecution of a failure to comply with:
    - a notice to produce
    - a notice to appear

[3] Drawn from paragraph 5 of the *Freedom of Information Regulatory Action Policy*.

- an oath or affirmation administered by the Information Commissioner that the answers that a person will give will be true, and
- an IC review decision.

- In relation to an investigation, the Information Commissioner can exercise enforcement powers to compel compliance with or, where relevant, to seek prosecution of a failure to comply with:
  - a notice to produce
  - a notice to appear
  - an oath or affirmation administered by the Information Commissioner that the answers that a person will give will be true, and
  - a recommendation following the investigation of the complaint.

- The *Privacy Act 1988* confers on OAIC's Commissioners:[4]
  - Privacy regulatory powers to work with entities to facilitate compliance with privacy legal obligations and best practice privacy practice, such as:
    - developing or requesting the development of an APP code
    - directing an agency to complete a Privacy Impact Assessment
    - monitor, or conduct an assessment of, whether personal information is being maintained and handled by an entity as required by law

[4] Drawn from paragraph 21 to 23 of the *Privacy Regulatory Action Policy*.

        - require an entity to provide information about an actual or suspected eligible data breach, or to notify affected individuals of a data breach.

- Privacy regulatory powers that can be used to investigate or otherwise deal with an alleged interference with privacy are contained in Part V of the Privacy Act and include powers to:
    - investigate in response to a complaint or on the Commissioner's own initiative
    - conduct preliminary inquiries to determine whether or not to open an investigation
- Enforcement powers, that range from less serious to more serious regulatory action, include powers to:
    - issue an infringement notice or compliance notice
    - accept an enforceable undertaking and bring proceedings to enforce an enforceable undertaking
    - make a determination and declarations following an investigation, and bring proceedings to enforce a determination
    - report to the Minister in certain circumstances following a CII, monitoring activity or assessment
    - seek an injunction including before, during or after an investigation or the exercise of another regulatory power
    - apply to the court for a civil penalty order for a breach of a civil penalty provision.

- Separate to the above FOI and privacy functions, the *Australian Information Commissioner Act 2010* also confers on the Information Commissioner a function of reporting to the Minister on any matter that relates to the Commonwealth Government's policy and practice with respect to:
    - the collection, use, disclosure, management, administration or storage of, or accessibility to, information held by the Government; and
    - the systems used, or proposed to be used, for the activities covered by subparagraph (i); function on the Information Commissioner.

ESTIMATES BRIEF: OTHER

Subject: Determinations

Type: Privacy Act function

Key details			
When did OAIC learn of matter?	**Ongoing function**		
Origin	N/A		
Is there an issue in the public domain?	Determinations published on the OAIC website and Austlii		
Jurisdiction	Privacy Act Part V; in particular section 52		
Responsible Branch & team	Privacy Case Management: Determinations		
Content author	s22	Phone	s22
Clearance by	**Jennifer Perrin**	Phone	
Brief current at	4 November 2025		

Brief overview

- The Commissioner (or delegate) may make a determination under section 52 of the *Privacy Act 1988* (Cth) in relation to
    - a Commissioner-initiated investigation (s 52(1A)), or
    - an individual privacy complaint (s 52(1)).
- Determinations are published on Austlii: Australian Information Commissioner (AICmr) series.
- Determination summaries are published on the OAIC website.

Recent statistics – determinations made by year

2024 calendar year	10 determinations made
2025 calendar year	9 determinations made
2024/25 financial year	10 determinations made
2025/26 financial year	3 determinations made

Determinations made in 2025 calendar year

Determination	APP / legislative regime	Privacy issues (determination catch words)
'ATE' and 'ATF' (Privacy) [2025] AICmr 10 (13 January 2025) *Dispute over mobile phone number*	APP 6, APP 11, APP 1	• No breach. • Complaint dismissed. • Disclosure of personal information • Whether employer directly liable for disclosure by employee • Whether employer vicariously liable for disclosure by employee • Whether reasonable steps were taken to protect personal information from unauthorised disclosure • Open and transparent management of personal information
'ATP' and 'ATR' (Privacy) [2025] AICmr 18 (23 January 2025) *TEQSA Australia, information reported in AGM notices*	APP 6, APP 10.2	• No breach • Complaint dismissed. • Use or disclosure of personal information • Whether personal information was disclosed for a secondary purpose • Whether individual would reasonably expect secondary disclosure • Whether reasonable steps taken to ensure quality of personal information disclosed
'ATQ' and CEO of Services Australia (Privacy) [2025]	APP 6.1, APP 10.2, APP 11.1	• Breach • Intertwinement of sensitive information with that of other individuals

Determination	APP / legislative regime	Privacy issues (determination catch words)
AICmr 19 (23 January 2025) *Digital doppelganger*		• Unauthorised disclosure of personal information • Whether reasonable steps taken to ensure personal information was up-to-date and accurate • Whether reasonable steps taken to protect from unauthorised disclosure • Serious and repeated interferences with privacy – • Breach of APP 6 and APP 10 and APP 11 • Compensation for non- economic loss • Written apology • Specified steps to undertake
'ATU' and 'ATX' (Privacy) [2025] AICmr 23 (30 January 2025) *Dispute arising in the context of a building contract*	APP 12.1, APP 12.9	• No breach • Complaint dismissed. • Access to personal information • Whether valid access requests made • Whether personal information held at the time of access request • Refusal to give access to personal information • Whether written notice of refusal complied with APP 12 obligations
Commissioner Initiated Investigation into Regional Australia Bank Limited (Privacy) [2025] AICmr 89 (14 May 2025) *CDR*	*Competition and Consumer Act 2010* (Cth) Consumer Data Right Rules, Privacy	• Breach • Liability for the actions of a third-party provider • Regional Australia Bank (RAB), in its capacity as a data holder in CDR, breached Privacy Safeguards 1 and 11 by virtue of the conduct

Determination	APP / legislative regime	Privacy issues (determination catch words)
	Safeguards 11 and 1	of its third-party service provider, Biza. • CDR data of up to 197 consumers co-mingled, which created a real risk that RAB would provide inaccurate information to other participants in the CDR ecosystem about an affected consumer.
'AXF' and 'AXG' (Privacy) [2025] AICmr 121 (27 June 2025) *Patient medical records*	APP 11.1	• Breach • Security of personal information • Whether reasonable steps taken to protect personal information • Breach of APP 11.1 • Failure to take reasonable steps • Compensation for non- economic loss awarded • Specified steps to address interference
Commissioner Initiated Investigation into Kmart Australia Limited (Privacy) [2025] AICmr 155 (26 August 2025) *FRT*	APP 3.3, APP 3.4, APP 5.1, APP 1.3, APP 1.4	• Breach • Whether personal information was collected • Whether permitted general situation existed • Whether reasonable steps were taken to notify • Whether the respondent had a privacy policy • Must not repeat or continue acts and practices
'AYN' and Fortrend Securities Pty Ltd (Privacy) [2025] AICmr 167 (15 September 2025) *Former employer disclosed a medical*	APP 6.1	• Breach • Disclosure of personal information • Employee records exemption considered and found not to apply • Compensation for non-economic loss awarded

Determination	APP / legislative regime	Privacy issues (determination catch words)
certificate about the complainant to a third party.		• Aggravated damages awarded • Apology • Specified steps to address interference
Commissioner Initiated Investigation into Vinomofo Pty Ltd (Privacy) [2025] AICmr 175 (17 October 2025) *Data breach in context of data migration project*	APP 11.1	• Breach • Whether reasonable steps taken to protect personal information • Failure to take reasonable steps • Must not repeat or continue acts and practices found to be an interference with individuals' privacy • Specified steps to address interference.

When is a determination issued? Why are so few determinations issued?

- Determinations are not issued for all contraventions of the Privacy Act.
- As a regulatory response, the primary purpose of a determination is education and deterrence, where the impact of a decision is likely to influence broader behaviour in the relevant sector.

What awards can be made in a determination?

- The matters that can be dealt with in a determination are prescribed in s 52 of the Act. In summary, this includes declarations that:
    - the respondent has engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct;
    - an award of compensation be paid for any loss or damage suffered by the individual by reason of the act or practice;

- the respondent is required to take specified steps within a specified period to ensure that the conduct is not repeated or continued.

If asked about matters on foot and proceeding to determination

- It is inappropriate to comment on specific ongoing investigations.
- There are approximately (11) investigations or complaints on foot where the OAIC is considering using a section 52 determination to finalise the matter, across both CIIs and individual privacy complaints.
    - These matters include possible contraventions of APPs 3, 5, 6, 10, 11, 12.

If asked about privacy matters subject to review

- It is inappropriate to comment on specific matters before the courts or the Administrative Review Tribunal.

ESTIMATES BRIEF: MATTER

Subject: Privacy Strategy Meeting Decisions

Type: Strategic decisions

Key details			
Decisions dates	Between 7 May 2025 and 13 August 2025		
How was OAIC advised/origin?	Varied – media, data breach reporting, proactive scanning, tip offs		
Jurisdiction	General privacy - APPs		
Date action ceased	Ongoing		
Jurisdiction	APPs		
Responsible Branch & team	Regulatory Action Division		
Content author	s22	Phone	s22
Clearance by	Annan Boag Rowena Park	Phone	s22
Brief current at	26 November 2025		

- This paper provides a summary of recent assessments considered by the OAIC's Privacy Strategy Meeting (PSM).
- In accordance with the OAIC's Regulatory Action Protocol, the PSM considers preliminary assessments and preliminary enquiries to decide whether matters should be brought to the OAIC's Regulatory Board or other action to be taken.

	Matter type and name	Summary of Facts	PIs conducted?	PSM Outcome	Date endorsed	Assessment link[1]
1.	**Data breach** s47E(	Notifiable data breach relating to disclosure of TFNs of s47E(d)	Yes	**No further action** - All records of TFNs deleted by the Respondent. Voluntary commitment provided to the OAIC that an external consultant would be engaged to review privacy governance.	7 May 2025	D2025/014132
2.	**Data breach** s47E(	Notifiable data breach; cyber incident.	Yes	**Ongoing** - Matter to advance to Regulatory Board for decision.	13 Aug 2025	D2025/014252
3.	**CII follow up** s47E (d)	s47E(d) Further engagement with Respondent following closure of investigation.	Yes	**No further action** – matter to be monitored with report back on practices in 12 months.	18 Jun 2025	D2025/009530

[1] These assessments papers contain confidential information and should not be disclosed publicly.

4.	**Internal referral – ID scanning** s47E(d)	Collection and storage of ID documents s47E(d)	Yes	**No further action** – information obtained about ID scanning practices. Compliance Team is in preliminary phases of broader ID scanning project.	18 Jun 2025	D2025/009529
5.	**Data breach** s47E(d)	Notifiable data breach involving a s47E(d)	Yes	**No further action** - s47E(d)	27 Jun 2025	D2025/010543
6.	**External referral – APP 11.2** s47E(d)	Retention of TFNs by s47E(d)	No	**No further action** – due to progression of similar matter involving greater number of impacted individuals	7 May 2025	D2025/010551

7.	**External referral - APP 11.2** s47E(d)	Retention of TFNs by s47E(d)	Yes	**Ongoing** - Further assurance about remediation measures from Respondent required	27 Jun 2025	D2025/010551
8.	**Rep Complaint – APP 6** s47E(d)	Representative complaint in relation to disclosure of employee personal information for induction purposes without consent.	No	**No further action** –Decline under s 41(1)(a) and s41(1)(da) issued 26 November 2025.	2 Jul 2025	D2025/014122
9.	**Media** s47E(d)	Media article s47E(d) :(d)	Yes	**No further action** – following engagement with the Respondent about steps to enable collection, consent mechanisms in place and confirmation that the data is not used to train AI model.	2 Jul 2025	D2025/014126
9.	**Tip off** s47E(d)	Tip off in relation to the use of surveillance (CCTV) in s47E(d)	No	**No further action** – Forward plan to update OAIC website guidance to include surveillance/use of CCTV and engage with/issue guidance	10 Jul 2025	D2025/014124

	s47E(d)			to s47E(d)		
10.	**External referral – Data breaches** s47E(d)	Data Breaches relating to s47E(d) and unauthorised access to members accounts.	No	**No further action** given s47E(d)	16 Jul 2025	D2025/014127
11	**Rep complaint – APP 11.1** s47E(d)	Data breach, cyber incident affecting third party supplier, resulting in exfiltration of personal information	Yes	**No further action** – Following consideration of resourcing, possible compensation, PI affected and OAIC's regulatory priorities, an Intention to Decline under s41(1)(da) is to be issued – currently in progress.	20 Aug 2025	D2025/014770
12	**Internal referral -** s47E(d)	Overcollection of personal information and collection from third party sources	No	**Preliminary inquiries** to be commenced with targeted respondents in relation to collection practices.	14 October 2025	D2025/021380

		(including publicly available sources)				
13	**Data breach – NDB scheme** s47E(d)	Data breach, cyber incident affecting s47E(d)	Yes	**No further action -** pursuant to s7C(4) of the Privacy Act, the s47E(d)	30 October 2025	D2025/023798
14	**Internal referral – collection** s47E(d)	Collection of personal information from s47E(d) and publicly available sources	Yes	**No further action** – following engagement with the Respondent and clarification of collection purposes and processes.	30 October 2025	D2025/026706

ESTIMATES BRIEF: MATTER

Respondent name: Clearview AI

Type: Determination

Key details			
How was OAIC advised/origin?	Media reporting		
Date action commenced	21 January 2020		
Jurisdiction	Privacy		
Responsible Branch & team	Regulatory Intelligence and Strategy Branch		
Content author	s22	Phone	s22
Clearance by	Marcel Savary	Phone	
Brief current at	24 November 2025 (noting no developments in OAIC regulatory action since Privacy Commissioner's statement 21 August 2024)		

Brief overview

2021 Determination

- On 14 October 2021, the Australian Information Commissioner (**Commissioner**) determined that Clearview AI Inc. (**Clearview**) breached Australians' privacy by scraping their biometric information from the internet and disclosing it through a facial recognition tool (**Determination**).
- On 3 November 2021, Clearview applied for merits review of the Determination, which subsequently found Clearview was bound by, and had breached, the *Privacy Act 1988* (Cth) (**Privacy Act**). Before the Tribunal could make final orders, Clearview withdrew its application.

Privacy Commissioner's August 2024 statement

- On 21 August 2024, the Privacy Commissioner released a statement that, after extensive consideration of whether the Office of the Australian Information Commissioner (**OAIC**) should invest further resources in scrutinising the actions of Clearview, she was not satisfied that further action is warranted at this time.
- However, the Privacy Commissioner stated that Clearview's practices were 'troubling' and are 'increasingly common due to the drive towards the development of generative AI models.'
- The Commissioner emphasised that all entities that fall within the jurisdiction of the Privacy Act which engage in the practice of collecting, using or disclosing personal information in the context of AI are required to comply with the Privacy Act and the OAIC would shortly issue guidance for entities seeking to develop and train generative AI models.
- This guidance has now been published:
    - Guidance on privacy and developing and training generative AI models
    - Guidance on privacy and the use of commercially available AI products

Recent global developments relating to Clearview

- **United Kingdom (October 2025):** The UK Upper Tribunal found that Clearview AI's mass scraping constitutes 'monitoring the behaviour' of UK residents, bringing it firmly within the scope of the UK GDPR, regardless of the company's lack of physical presence in the UK.[1]

[1] UK Upper Tribunal hands down judgment on Clearview AI Inc | ICO

- **Canada (May 2025):** The Alberta Court of King's Bench dismissed Clearview's application to quash regulatory orders. While the Court found that certain 'publicly available' data exceptions in privacy law were technically unconstitutional, it upheld the ban on Clearview, ruling that the company's purpose—mass biometric surveillance—was not 'reasonable' and therefore remained illegal.[2]
- **European Union:** Regulators in Italy, France and Greece have imposed maximum penalties (e.g., €20 million by the Italian Garante in 2022) and ordered data deletion. Clearview has generally withdrawn from the EU market but has failed to pay fines, highlighting the enforcement gap for non-resident entities.[3]
- **United States:**
    - **BIPA Class Action Settlement (March 2025):** A US federal judge granted final approval to a settlement of claims under the Illinois *Biometric Information Privacy Act* (BIPA). Due to Clearview's inability to pay a judgment, the settlement provided class members with a 23% equity stake in Clearview AI (valued at approx. USD $51.75M).
    - **ACLU Consent Decree (May 2022):** Clearview remains subject to a permanent nationwide injunction banning it from selling its database to most private companies in the US. However, the settlement explicitly permits Clearview to continue selling its services to federal, state, and local government agencies.

[2] Alberta Court Weighs in on Clearview AI: Wins, Losses and Key Takeaways - McMillan LLP
[3] Facial recognition: Italian SA fines Clearview AI EUR 20 million | European Data Protection Board

Recent Senate Committee discussion

- On 19 November 2025, Colm Gannon (CEO of International Centre for Missing and Exploited Children Australia) gave evidence to the Senate Education and Employment References Committee in its *Quality and safety of Australia's early childhood education and care system* inquiry.
- He stated that the ability of Australian law enforcement agencies to identify victims and perpetrators of child sexual abuse has been constrained 'due to certain decisions that were made by the OAIC' preventing their use of relevant technology tools. He indicated that privacy is being prioritised over the rights of children.

Background

- Clearview is a body corporate incorporated in Delaware in the United States. It provides a service which enables subscribers to upload images of individuals and to match their faces with those contained in Clearview's database of images sourced from public locations on the internet. If the service identifies a matching image, it displays a copy of the image and the web address of the webpage from which the image was obtained. The images in the database are sourced using a software known as a 'web crawler', which trawls from website to website copying images containing faces and their associated web addresses.
- Clearview's service commenced in late 2018 and was promoted by the offering of free trials to users. That included users employed by numerous Australian police forces, including the Australian Federal Police, Queensland Police Service and Victoria Police.

- By March 2020, Clearview had ceased offering trials for law enforcement agencies located in Australia and blocked IP addresses from Australian locations from logging onto the Clearview system.

The Commissioner's Investigation and Determination

- On 4 March 2020, the Commissioner commenced an own-motion investigation into Clearview.
- On 7 July 2020, the OAIC and UK Information Commissioner's Office advised Clearview that the investigation would be conducted jointly.
- On 14 October 2021, the Commissioner determined under s 52(1A) of the Privacy Act that Clearview breached Australians' privacy by scraping their biometric information from the internet and disclosing it through a facial recognition tool. The Determination included findings that Clearview had breached Australian Privacy Principles (**APPs**) 1.2, 3.3, 3.5, 5 and 10.2. The Commissioner declared, amongst other things, that Clearview must cease to collect images in breach of the APPs and delete the images collected.

The Tribunal Proceedings

- On 3 November 2021, Clearview applied for merits review of the Determination.
- On 12 and 13 December 2022, the Tribunal held a hearing in relation to the application for review of the Determination. At that hearing, the founder and CEO of Clearview, Cam-Hoan Ton-That gave evidence that Clearview was continuing to collect images from websites hosted on servers located in Australia.

- On 8 May 2023, the Tribunal found Clearview was bound by the Privacy Act and breached APPs 3.3 and 1.2 and directed the matter be listed for further hearing to determine the terms of the Tribunal's decision.
- On 19 May 2023, the Tribunal directed the Commissioner to set out the form of relief she sought before a further hearing to determine the final relief. On 14 June 2023, the Commissioner provided her submissions.
- On 3 July 2023, Clearview lodged their submission in relation to the proposed declarations together with a statement of Mr Ton-That which asserted, for the first time, that in October 2022 Clearview had ceased all web crawling to deploy a new database and that, by the time it recommenced web crawling in January 2023, it had implemented functionality to prevent any crawling from servers located in Australia.
- At the hearing on 10 July 2023, the Tribunal was unable to make final orders given the statements Clearview had sought to file were contrary to the material upon which the Tribunal had made its findings at the hearing. Instead, the Tribunal ordered a further hearing in September to resolve the factual contest about whether Clearview ceased scraping from Australian servers in October 2022 and for the Tribunal to make final orders.
- The Tribunal also ordered Clearview to produce, by 14 August 2023, documents evidencing (amongst other things) that the functionality of the Clearview system prevents crawling or the collection of data from Australian servers.
- On 8 August 2023, Clearview withdrew its application.

AFP Determination

- Between 2 November 2019 and 22 January 2020, members of the AFP-led Australian Centre to Counter Child Exploitation used the Facial Recognition Tool on a free trial basis, to test the functionality of the tool, and in some cases, to try to identify persons of interest and victims in active investigations.
- On 26 November 2021, the Commissioner determined that the AFP:
    - failed to complete a privacy impact assessment (**PIA**) before using the Facial Recognition Tool, in breach of clause 12 of the Privacy (Australian Government Agencies – Governance) APP Code 2017 (**the Code**), which requires a PIA for all high privacy risk projects; and
    - breached APP 1.2 by failing to take reasonable steps to implement practices, procedures and systems in relation to its use of Clearview to ensure it complied with clause 12 of the Code.
- The Commissioner directed the AFP to:
    - engage an independent assessor to review and report to the OAIC on residual deficiencies in its practices, procedures, systems and training in relation to privacy assessments, and make any necessary changes recommended in the report; and
    - ensure that relevant AFP personnel have completed an updated privacy training program.

ESTIMATES BRIEF: MATTER

Respondent name: Tracking Pixels

Type: Preliminary inquiries

Key details			
When did OAIC learn of matter?	EU children's data rulings: April 2023 and September 2023 December 2023 reports in media re TikTok's use of tracking pixels		
How was OAIC advised/origin?	Media, senate estimates hearings		
Date action commenced	13 November 2024		
Date action ceased	Ongoing		
Jurisdiction	APPs		
Related representative action?	No		
Responsible Branch & team	Regulatory Action Division, Investigations Team s22		
Content author	s22	Phone	s22
Clearance by	Annan Boag Rowena Park	Phone	s22
Brief current at	10 November 2025		

- A tracking pixel is a piece of code generated by a third-party provider that can be placed on an organisation's website to collect information about a user's activity.

- When a user visits a webpage with a tracking pixel, the pixel loads and sends certain types of data to the server of the third-party provider.

- Social media companies including Facebook and TikTok offer tracking pixels.

<u>Inquiries of TikTok (January – May 2024)</u>

- On 19 January 2024 the OAIC issued preliminary inquiries to TikTok Pty Ltd (TikTok), a company incorporated in Singapore and the entity responsible for providing the TikTok application.

- The inquiries related to TikTok's handling of personal information, particularly children's information and the TikTok tracking pixel.

- The OAIC finalised the assessment of the matter on 22 May 2024.

- On 29 May 2024, the Privacy Commissioner made a public statement outlining the reasons for the finalisation of the matter, including because 'there is no clear and obvious breach of Australian privacy law that would warrant opening an investigation'.

    - The statement said: 'We are considering next steps to address broader issues raised by tracking tools that have become commonplace on websites today, with a focus on tools that could facilitate the transfer of sensitive information. We will also be publishing information on key privacy issues organisations must consider when configuring and deploying tracking tools on their websites.'

Current action and next steps

- 4 November 2024 - the OAIC published guidance about organisations' privacy obligations in relation to their use of tracking pixels where it results in the collection, use or disclosure of personal information.

- The guidance sets out general considerations for private sector organisations that use third-party tracking pixels on their websites.

- The OAIC is also considering the use of tracking pixels by health service providers that may collect sensitive health information via their websites.

- The OAIC is conducting inquiries and has opened investigations into health service providers about their use of tracking pixels and compliance with the Privacy Act and APPs 3, 5 and 7.

ESTIMATES BRIEF: MATTER

Respondent name: Master Wealth Control Pty Ltd t/as DG Institute; Property Lovers Pty Ltd

Type: Determinations

Key details			
Date of determinations	Master Wealth Control – 18 Nov 2024 Property Lovers Pty Ltd – 22 Nov 2024		
Contraventions found	Breach of APPs 1.3, 3.5, 5.1 and 10.2		
Responsible Branch & team	Regulatory Action Division, Investigations and Compliance		
Content author	s22	Phone	s22
Clearance by	**Annan Boag** **Rowena Park**	Phone	s22
Brief current at	26 November 2025		

Brief description of matter

- On 19 May 2023, the OAIC commenced investigations into Master Wealth Control Pty Ltd t/a DG Institute and Property Lovers Pty Ltd.

- These entities offered training courses in relation to property investment, wealth management and asset protection. Courses included live seminars and online broadcasts, plus documentary guidance and instruction.

- Clients of the 'Elite Mentoring Program' received weekly 'on and off-market leads lists.' These included properties owned by individuals who had appeared in court listings for reasons including bankruptcy, divorce, deceased estate, mortgagee repossession and company liquidations.

- The entities generated lists combining this information with data obtained from online property data brokers so clients could target these properties for below market value sales.

Outcome of investigation

- In November 2024, the Privacy Commissioner made determinations that found each entity had contravened Australian Privacy Principles (APPs) 1.3, 3.5, 5.1 and 10.2.

- The declarations declared that both entities must:
  - not repeat or continue the acts and practices;
  - immediately, cease collecting personal information of individuals from third parties in a manner that is contrary to APP 3.5;
  - within 30 days of the determination, ensure specified leads lists and any personal information collected from third parties for the purposes of compiling its leads lists were destroyed;
  - review and, to the extent necessary, update its privacy policy to ensure that individuals are notified of all APP 1.4 matters;
  - in the case of Property Lovers, within 7 days of the determination, publish a written apology on its website for at least 30 days.
- The entities were required to provide the OAIC with evidence of completion of the declarations within 14 days of completing each declaration.

Actions since declarations

- As of 10 February 2025, Master Wealth Control no longer operates, following the Federal Court's orders disqualifying its sole director from being involved in the management of a corporation for five years – until 18 July 2029.
- The OAIC is not taking further action in relation to this entity or its determination.

- Property Lovers has published a written apology on its website and provided a statutory declaration stating that it had ceased the distribution of lead lists and destroyed all specified lead lists (plus an independent report from an IT consultant). However, the OAIC holds concerns that Property Lovers may be continuing the conduct identified in the determination.

- On 11 April 2025, the OAIC commenced a new investigation into Property Lovers and the Fastproperty.ai platform. Enquiries have been made with several parties involved in the development of the platform and the investigation remains active.

Correspondence with Senator Shoebridge – August 2025

- On 11 August 2025, Senator Shoebridge wrote to the Privacy Commissioner expressing concerns of non-compliance with the determinations and that the entities continue to engage in 'predatory marketing', promotion of asset protection strategies and unsolicited communications to former clients.

- On 29 August 2025, the Privacy Commissioner replied to Senator Shoebridge noting that although the determinations imposed declarations on each entity, they did not require either business to cease operations or take down their websites.

- The Privacy Commissioner also advised Senator Shoebridge that the OAIC is currently taking steps to assess Property Lovers' compliance with its determination, including whether there is a continuation of the conduct identified in the determination.

- A copy of the correspondence is enclosed.

Our reference: CII25/00005

Senator David Shoebridge
Senator for NSW
Suite 201, Level 2
1A Lawson Square
Redfern NSW 2016

By email: Senator.Shoebridge@aph.gov.au

Property Lovers alleged non-compliance with determinations

Dear Senator

I refer to your letter of 11 August 2025 concerning Property Lovers.

Determinations

The OAIC has issued two determinations in connection with Property Lovers following investigations examining their privacy practices.

The first determination, on 18 November 2024, was issued against Master Wealth Control Pty Ltd, trading as DG Institute (**Master Wealth**). The second determination, on 22 November 2024, was issued against Property Lovers Pty Ltd (**Property Lovers**).

The determinations found the respondents had contravened Australian Privacy Principles 1.3, 3.5, 5.1 and 10.2, and required specified actions to be taken to ensure the contraventions did not continue.

The determinations did not require Property Lovers or Master Wealth to cease to operate or take down their websites, but they did require both business to take certain steps to address the breaches identified in the determinations.

Master Wealth

As of 10 February 2025, Master Wealth is no longer operating, following the Federal Court's orders banning Ms Grubisa from acting as a director. Given this business is no longer operating, the OAIC is not taking further action in relation to this respondent or determination.

Property Lovers

In relation to Property Lovers, the OAIC is currently taking steps to assess Property Lovers' compliance, including by further investigating the acts or practices of Property Lovers and related entities in relation to the continuation of conduct identified in the determination.

Other issues

I appreciate that privacy issues that are subject to the OAIC's jurisdiction cover only a portion of the concerns outlined in your letter. Some of the concerns in your letter may be better directed at other regulatory agencies. The OAIC has been liaising in its investigation with other agencies with an interest in those aspects of the Property Lovers business.

Yours sincerely

Carly Kind
Australian Privacy Commissioner

29 August 2025

ESTIMATES BRIEF: OTHER (REGULATORY PRIORITY, PROMINENT ISSUE)

Subject: Online Safety Amendment (Social Media Minimum Age) Act 2024
Type: Update

Key details			
Jurisdiction	Privacy / Social Media Minimum Age		
Responsible Branch & team	Privacy Reform Implementation Taskforce, RIS Branch		
Content author	s22	Phone	s22
Clearance by	Marcel Savary	Phone	s22
Brief current at	28 November 2025		

Brief overview of issue

- The *Online Safety Amendment (Social Media Minimum Age) Act 2024* requires age-restricted social media platforms to take reasonable steps to prevent Australians under 16 from having social media accounts.
- The Act commences on 10 December 2025, and it imposes significant penalties for breaching this obligation.
- Platforms are likely to meet the obligation through the use of age assurance technologies.
- 'Age assurance' encompasses a range of methods for estimating, inferring or verifying the age or age range of users.
    - Methods may involve referencing against identification documents (e.g. a licence or passport), or estimating or inferring age, or an age range, based on analysis of facial features or online behavioural signals.

- Platforms must not collect government-issued ID or require the use of Digital ID unless a reasonable alternate means is also offered.

- The Act, at section 63F, includes privacy safeguards, which place limitations on the use and disclosure of personal information collected by entities for the purposes of satisfying the minimum age obligation, and require the destruction of information following its use. Key privacy provisions are outlined at **Attachment A.**

- The OAIC is preparing to perform the Information Commissioner's functions under the Act. Activities include:

  - promoting guidance for regulated entities about privacy obligations in the Act and the *Privacy Act 1988*. This was published on 10 October 2025.

  - promoting communication materials for the public about age assurance technologies and the privacy protections that apply. These were published on 23 October 2025.

  - preparing for enquiries and complaints.

- The OAIC's SMMA regulatory role is funded through a MYEFO 2024–25 measure which provided $5.0 million over four years and $1.1 million per year ongoing from 2028–29 to the OAIC to oversee the privacy safeguards in the Act.

Recent developments

OAIC guidance and enforcement

- The OAIC is committed to ensuring the successful rollout of the SMMA regime by robustly applying and regulating the privacy rules contained in the legislation, in order to reassure the Australian community that their privacy is protected.
- On 10 October, the OAIC published regulatory guidance for age-restricted social media platforms and age assurance providers on compliance with the privacy provisions in the SMMA scheme.
- The guidance reflects the stringent legal obligations on entities to ensure that age assurance is applied proportionately and through privacy-respecting approaches.
- The OAIC will be actively monitoring platforms to ensure they stay within the bounds by deploying age assurance proportionately and lawfully.
- Failure to meet these obligations may constitute 'an interference with the privacy of an individual' and may trigger compliance and enforcement action.
- Penalties for a breach are substantial, with the maximum for corporations being the greater of either $50 million, three times the value of the benefit obtained from the contravention, or 30% of the body corporate's adjusted turnover during the breach period.
- **Attachment B** contains a summary from the guidance.

Reasonable steps guidance

- On 16 September, the eSafety Commissioner published regulatory guidance on reasonable steps platforms should take to prevent age-restricted users having accounts.

- Through development of the guidance, the OAIC provided feedback to eSafety on privacy safeguards of the scheme and observed several of the consultation roundtables hosted by eSafety between July and August 2025.

High court challenge

- We are aware of the legal challenge to the SMMA scheme filed in the High Court on 27 November and that the defendants named are the Commonwealth of Australia, the eSafety Commissioner and the Minister for Communications and Sport.
- The OAIC is not a party to the proceedings but is monitoring the progress of the proceedings and considering any ramifications.
- The OAIC remains ready to regulate under the SMMA scheme on and from the commencement date of the legislation.

Senate Inquiry

- On 27 August 2025, the Senate referred an inquiry into the implementation of regulations aimed at protecting children and young people online.
    - The Senate Inquiry on the Internet Search Engine Services Online Safety Code captures issues associated with the Social Media Minimum Age and the industry codes created under the *Online Safety Act 2021*.
    - The Privacy Commissioner provided evidence at a public hearing on 13 October 2025 and responded to Questions taken on Notice on 27 October.
    - The final report was published on 26 November 2025.

- Relevant to privacy, the Terms of Reference captured:
    - privacy and data protection implications of age verification
    - the expansion of corporate data collection and user profiling capabilities enabled by code compliance requirements.

- Relevant to privacy, the Final Report recommended delaying commencement of the SMMA scheme by 6 months. Given the current status of the report, our work to implement the SMMA scheme is unchanged.
- The Report also recommended a prohibition on the monetisation of children's data. The OAIC is considering such matters in the context of developing the Children's Online Privacy Code to be registered by December 2026.

Age Assurance Technology Trial

- On 31 August 2025, the Government published in full the final report of the independent Age Assurance Technology Trial.

- The media response to the report criticised weaknesses in the trial methodology and scepticism around the effectiveness of facial age estimation.

- The OAIC provided stakeholder feedback to the trial provider, Age Check Certification Scheme (ACCS), at particular points in the trial process. This was voluntary and not a requirement of the independent trial process.

Online Safety (Age-Restricted Social Media Platforms) Rules 2025

- On 29 July 2025, the Minister for Communications made the Online Safety (Age-Restricted Social Media Platforms) Rules 2025.

- The rules exclude certain services from the minimum age obligation, including messaging, gaming, education and health services.

- An earlier version of the Rules exempted YouTube by name, but the final Rules do not.

Collaboration with eSafety

- eSafety and the OAIC are working together to ensure a cohesive and consistent approach to addressing online harms for all Australians.

- Priority areas for collaboration are implementing the social media minimum age scheme, the development of 'Phase 2' Online Safety Industry Codes, and the development of the Children's Online Privacy Code (Code).

- Given the intersections, both eSafety and the OAIC are working closely together to ensure clear and aligned requirements, to ensure these important initiatives are both privacy- and safety-affirming for all Australians.

Discord Data Breach

- Discord is not an age-restricted social media platform for the purposes of the SMMA scheme.
- On 22 September, Discord became aware of a data breach from an outsourced customer service provider who had access to their customer support portal. OAIC was notified and the incident was contained.
- Personal information that was breached included identification documents collected as part of a review process for age assurance, unrelated to SMMA.
- On 10 November, Discord advised the OAIC that 86,498 Australians were impacted, an increase from the earlier quoted figure of 68,122. Discord estimates that roughly 5.5M customer support tickets worldwide were exposed.
- As of 13 November, Discord has said they have notified all affected Australian users.
- OAIC issued two rounds of preliminary enquiries and is satisfied that Discord has met its NDB obligations.

Passage of the Online Safety Amendment (Social Media Minimum Age) Bill 2024

- Key points raised in the OAIC's submission to the Environment and Communications Legislation Committee inquiry in November 2024 were:
    - The introduction of a minimum age for access to social media will have privacy impacts for all Australian users of social media.

- Age assurance checks will need to be conducted for all Australian social media users (not just children). This is likely to incentivise the collection, use and storage of additional personal information about all users of the service, which increases privacy risks and impacts.

- The introduction of a fair and reasonable test for the collection, use and disclosure of personal information would dramatically increase the ability of the OAIC to address harmful and unfair data practices in the online environment.

- While the OAIC is concerned about the overarching privacy impacts of the legislation, our submission supported the revised definition of consent, and the specific privacy protections in section 63F of the Bill.

Attachment A

Key privacy provisions in the Online Safety Act

- Section 63DA empowers the Minister for Communications to exclude specified types of information being collected and used by platforms for the purposes of meeting the minimum age obligation, having regard to advice sought from the eSafety Commissioner and the Information Commissioner.

- Section 63DB specifies that platforms must not collect government-issued identification or require the use of Digital ID, unless a reasonable alternate means is also offered.

- Section 63F contains privacy safeguards that:

    - prohibit entities from using or disclosing personal information collected for age assurance for any other purpose unless the individual has consented or APPs 6.2(b), (c), (d) or (e) applies

    - require entities to destroy information collected for age assurance purposes after using or disclosing it for the purposes for which it was collected

    - require consent to be voluntary, informed, current, specific and unambiguous. This definition is a higher threshold than in the current Privacy Act and is consistent with proposals agreed-in-principle by the Government in its response to the Privacy Act Review report

- require entities to destroy information after using or disclosing it for the purposes it was collected
- state a breach of the above safeguards will be an interference with privacy under s 13 of the Privacy Act. This enlivens the Information Commissioner's investigation and enforcement powers.

- Under s 63K, if the Information Commissioner is satisfied that the provider has used, disclosed or failed to destroy information in a way that is taken to be an interference with privacy, the Information Commissioner may:
  - prepare a statement (platform provider notification) to that effect
  - give a copy to the provider of the platform, and
  - publish the statement on the OAIC website if the Information Commissioner considers that is appropriate.

ATTACHMENT B – EXTRACT OF OAIC GUIDANCE 'Privacy Guidance on Part 4A (Social Media Minimum Age) of the Online Safety Act 202'

1. Key considerations

- Part 4A of the Online Safety Act 2021 operates alongside the Privacy Act 1988 and Australian Privacy Principles. Part 4A introduces additional, more stringent obligations on age-restricted social media platform providers and third-party age assurance providers when handling personal information for social media minimum age (SMMA) compliance purposes.
- When choosing or offering an age assurance method (or combination of methods) ensure it is necessary for SMMA compliance purposes and proportionate to the legitimate aim of preventing age-restricted users from having accounts. Consider alternate methods and how you can use low-intrusion techniques within an age assurance method(s). Escalate to more intrusive personal information handling only as necessary.
- Take a privacy by design approach and consider the privacy impacts associated with each age assurance method (e.g. inference, estimation and verification) and whether the circumstances surrounding the specific chosen method(s) justify the privacy risks.
- Undertake a privacy impact assessment (PIA) when choosing an age-assurance method(s) to identify potential privacy impacts at the outset and implement recommendations to manage, minimise or eliminate them. This will assist to ensure that a privacy by design approach is embedded from the start.

- Minimise the inclusion of personal and sensitive information in age assurance processes. Only retain enough personal information in outputs to meet defined purposes, such as to explain the measures implemented for a user and to facilitate reviews or complaints, then destroy on schedule.
- Destroy any inputs that have been collected immediately once the purposes of collection have been met. Personal information, including sensitive information, that is collected for SMMA compliance purposes (e.g. biometric information, biometric templates, identity documents) must be destroyed once all purposes have been met. Avoid purpose 'padding' and ensure destruction includes caches and storage.
- Existing personal information used for age assurance does not need to be destroyed where the original purposes for its collection are ongoing. Using personal information that was collected for a non-SMMA purpose (e.g. age inference) for SMMA compliance purposes does not, by itself, put that information within the remit of s 63F of Part 4A. However, entities must comply with Australian Privacy Principle (APP) 6 to establish the basis for this type of secondary use.
- Be thoughtful when designing consent requests for secondary uses and disclosures of personal information collected for SMMA. Secondary use and disclosure should be strictly optional and easily withdrawn. The consent request should be written and designed so users of all abilities can understand what they are being asked to agree to and change their mind.

- Be transparent, at the moment it matters. Use APP 5 just-in-time notices to explain key information such as what is collected, why, by whom, how long it is retained, and the user's choices (including alternative methods and review processes). APP 1 privacy policies should be updated with clear and transparent information, with clear policies and procedures to facilitate this transparency.

ESTIMATES BRIEF: OTHER

Subject: Services Australia matters

Type: Brief

Key details			
When did OAIC learn of matter?	**Ongoing**		
Origin	Individual Complaints		
Is there an issue in the public domain?	N/A		
Jurisdiction	Privacy		
Responsible Branch & team	Privacy Case Management		
Content author	s22	Phone	s22
Clearance by	**Jennifer Perrin**	Phone	s22
Brief current at	7/11/2025		

Brief overview

- On 23 January 2025, the Privacy Commissioner published a determination (the digital doppelganger determination) which found that Services Australia breached the Privacy Act when it failed to take reasonable steps to protect an individual's personal information, and when it disclosed sensitive personal information for a secondary purpose without consent or authorisation under the Act.
    - *'ATQ' and CEO of Services Australia* (Privacy) [2025] AICmr 19.
    - Services Australia has advised that it has complied with the declarations made in the determination.

How many privacy complaints are on hand about Services Australia?

- The OAIC has a number of individual privacy complaints on hand relating to Services Australia.
    - As at 31 October 2025, 52[1] open individual privacy complaints on hand where Services Australia is the respondent.
        - These are at various stages.
        - 14 are over 12 months old.
    - Five investigations are underway.
        - Under the Privacy Act, the Commissioner has a range of powers to support the conduct of investigations, including the power to compel the production of documents and information (s.44) and the power to examine witnesses (s.45).
        - While it is inappropriate to comment on investigations that are on foot, the Commissioner uses the investigative powers available under the Privacy Act when appropriate and necessary.

Engagement between OAIC and Services Australia

- SES meetings between OAIC and Services Australia held regularly (quarterly).
- Officer level engagement occurs as required on matters, and every 6- weeks to proactively progress privacy complaints as quickly and early as possible. Conciliation is considered where appropriate.

[1] OAIC has multiple respondent names for Services Australia in Resolve. This data includes records for the respondents 'Services Australia' and 'Services Australia (Centrelink)'.

ANAO Audit

- The ANAO has an audit in progress on 'Managing the privacy of client information in Services Australia'[2] with the following criteria:
    - Has Services Australia developed appropriate arrangements to manage the privacy of client information consistent with the Privacy Act 1988 (Privacy Act) and other legislative requirements?
    - Has Services Australia effectively implemented arrangements to manage the privacy of client information?
- The report is expected to be tabled in December 2025.

[2] https://www.anao.gov.au/work/performance-audit/managing-the-privacy-of-client-information-services-australia

ESTIMATES BRIEF: OTHER

Subject: DVA MATES

Type: Brief

Key details			
When did OAIC learn of matter?	**Ongoing**		
Origin	Individual and representative complaints		
Is there an issue in the public domain?	Representative complaint; Media coverage re discontinuation of MATES Program; Federal Court claim (14 November 2023)		
Jurisdiction	Privacy related		
Responsible Branch & team	Regulatory Action Division, Investigations Team		
Content author	s22	Phone	s22
Clearance by	**Annan Boag** **Rowena Park**	Phone	s22
Brief current at	**24 November 2025**		

Brief overview

- On 26 April 2023, the OAIC made a determination on a privacy complaint which found that DVA contravened the *Privacy Act 1988* in connection with its Veterans' Medicines Advice and Therapeutics Education Services (**MATES**) program. The determination awarded compensation to the complainant.

- The OAIC currently has 51 further complaints on hand relating to DVA MATES concerning breaches of APPs 3, 5, 6 and 11.

- These complaints comprise:

    - 1 representative complaint received 18 December 2023; and

    - 50 individual complaints received between 30 July 2023 and 26 August 2025 (49 complaints over 12 months old).

- All complaints allege repeated breaches of their sensitive information and that consent was not provided for the MATES program.

Current action and next steps

- OAIC has been engaging with DVA and the complaint parties.
- On 11 September 2025, the Australian Information Commissioner sent a letter to the Secretary of DVA in relation to the progress of these matters.
- On 29 October 2025, the Acting Executive General Manager, Regulatory Action Division sent a letter to the Chief Counsel and CAE, DVA in relation to the progress of these matters.
- On 19 November 2025, OAIC responded to correspondence from DVA in relation to the progress of these matters.
- OAIC is unable to discuss the detail of ongoing investigations and/or inquiries.

Background: public matters only

- 26 April 2023, Australian Information Commissioner's Determination ('ADJ' and The Secretary to the Department of Veterans' Affairs (Privacy) [2023] AICmr 29 (26 April 2023)) was made, finding:

- DVA breached APP 3 by collecting the complainant's prescription information from the Department of Human Services (**DHS**) on the collection dates as the complainant did not provide consent to the collection for the purpose of the MATES program
- DVA breached APP 6 by using and disclosing the complainant's prescription information to the University and the GP
- Awarded $5,000 in compensation to the complainant.

- 29 August 2023, Statement from the Department of Veterans' Affairs - Veterans' MATES program – Update which responds to the determination and which includes:

  … The recent determination by the Office of the Australian Information Commissioner (OAIC) relates to an individual case in 2017 whereby the individual opted out of participation in the program and DVA did not fully implement this request. DVA has unequivocally apologised for this.

  Veterans have always had the ability to opt out of the program, however DVA has taken steps to more prominently communicate this, so veterans can make an informed decision about their participation.

  The OAIC determination has highlighted that DVA's notices to veterans could include more information about how their billing information would be used for the purpose of the Veterans' MATES program. More information about privacy, and the ability of veterans to opt-out of the Veterans' MATES program has been added to DVA's website and Veterans' MATES program materials.

The Secretary has requested a review of the Veterans' MATES program to ensure that all requests to opt out of the program have been actioned appropriately, and to provide further assurance of compliance with the opt out provisions under the program. As part of this review, DVA has temporarily suspended provision of further data while it ensures individual requests regarding participation are dealt with, and frameworks are in place to ensure the circumstances addressed by the OAIC in its determination do not reoccur. DVA will complete this process as quickly as possible.

- A similarly worded statement was also published on 10 August 2023, Statement from the Department of Veterans' Affairs - Veterans' MATES program.

- On 12 February 2024, DVA statement on the Veterans' MATES program noting the withdrawal of Defence and HREC approval of the program due to concerns in the veteran community in relation to the sharing of data via the program.

ESTIMATES BRIEF: MATTER

Respondent name: Meta Platforms – Enforceable Undertaking

Type: Enforceable Undertaking, Privacy Complaints

Key details			
When did OAIC learn of matter?	**2016**		
How was OAIC advised/origin?	Media		
Date action commenced	CII began Apr 2018, EU signed 17 Dec 2024		
Jurisdiction	APPs		
Related representative action?	**Yes**		
Responsible Branch & team	EU – Compliance, Complaints – PCM		
Content author	s22	Phone	s22
Clearance by	**Rowena Park**	Phone	s22
Brief current at	14 November 2025		

Brief description of matter

- In 2020 the Information Commissioner commenced court proceedings alleging Meta Inc breached APPs 6 and 11 in relation to the 'This is your digital life' app from March 2014 to May 2015.
- In December 2024, the Commissioner agreed to a $50 million payment program as part of an enforceable undertaking (EU) received from Meta to compensate individuals impacted by the Cambridge Analytica matter.
  - Under the terms of the EU, the OAIC withdrew the civil penalty proceedings.
  - Meta did not admit liability.
- KPMG is administering the payment program. It is currently accepting registrations (registrations are open from 24 June 2025 to 31 December 2025). The Administrator has advised that it expects to be able to notify Claimants of their Interim Distribution Statement in June 2026.

Current action

- To date, Meta has complied with the conditions of the EU.

- The next obligation for Meta will be to notify the OAIC when the Administrator has commenced the process for determining the payment that each of the 2 classes of claimant is entitled to receive. (This should happen the first half of 2026.)
- Meta must also notify the OAIC when the Administrator has determined the aggregate amount to be distributed to all claimants and the aggregate amount to be distributed. This must occur within 2 years of the EU's commencement date (by 17 December 2026).
- The OAIC will continue to monitor compliance with the EU.
- All individual complaints and a representative complaint lodged with the OAIC were finalised in 2024-25.

Recent developments

- On 20 June 2025, Meta notified us that registrations for the payment plan would commence on 24 June 2025. They will close 31 December 2025.

Background: public matters only

- In proceedings commenced by the Information Commissioner in the Federal Court of Australia on 9 March 2020, the Commissioner alleged that from March 2014 to May 2015, Meta Inc and Facebook Ireland:
  - disclosed the personal information of Australian users to the 'This is Your Digital Life' app (**the app**) in breach of Australian Privacy Principle (APP) 6. Most Australian users did not install the app; their personal information was disclosed via their friends' use of the app; and
  - did not take reasonable steps to protect Australian Users' personal information from unauthorised disclosure, in breach of APP 11.

- The Commissioner further alleged that Meta Inc and Facebook Ireland:
  - engaged in acts or practices that were serious interferences with the privacy of Australian Users, contravening s 13G(a) of the Privacy Act; and
  - further, or in the alternative, repeatedly engaged in acts or practices that were interferences with the privacy of Australian Users, contravening s 13G(b) of the Act.
- Following mediation, the Commissioner agreed to a $50 Million payment program as part of an EU received from Meta to settle civil penalty proceedings, without admitting liability.
- As part of the resolution, the Commissioner withdrew the civil penalty proceedings.
- Funds of $50 million will be available to 'Eligible Australian Users'.
  - A person is an 'Eligible Australian User' if the person held a Facebook Account at any time during the period of 2 November 2013 and 17 December 2015 (Eligibility Period), was located in Australia for 30 days or more during the Eligibility Period and during the Eligibility Period, either installed the Life App using Facebook Login or was Facebook friends with another Facebook user who had installed the Life App using Facebook login.
- Eligible Australian Users can register as a 'Claimant' under the Payment Program if they suffered loss or damage, being either:
  - specific economic and/or non-economic loss and/or damage (beyond a generalised concern or embarrassment) (Class 1); or
  - a generalised concern or embarrassment (Class 2).

- The Administrator will use their absolute discretion, using the evidence available whether a person is an Eligible Australian User and if a person has provided enough evidence to substantiate their Class 1 claim registration.
- The Administrator will determine the payment that each Class 1 and Class 2 claimant is entitled to receive and make that payment in a timely manner.

ESTIMATES BRIEF: MATTER

Respondent name: Court Data Australia

Type: Determination and open privacy complaints

Key details			
When did OAIC learn of matter?	**7 June 2020**		
How was OAIC advised/origin?	Privacy complaint		
Date action commenced	**Determination 12 February 2024** **ART decision 28 May 2025**		
Age of matter in days	**Primary matter finalised**		
Jurisdiction	APP 3.5, 5, 10.		
Related representative action?	**n/a**		
Responsible Branch & team	Privacy Case Management, Investigations and Conciliations		
Content author	s22	Phone	s22
Clearance by	**Jennifer Perrin**	Phone	s22
Brief current at	7 November 2025		

Key issues

- On 12 February 2024, the Commissioner made a determination under section 52 of the Privacy Act that Court Data interfered with the privacy of an individual when, in summary, it collected the individual's personal information by a means that was not fair; failed to notify the individual that their personal information has been collected; and failed to take reasonable steps to ensure that the personal information it disclosed about the individual was accurate.
    - 'AHM' and JFA (Aust) Pty Ltd t/a Court Data Australia (Privacy) [2024] AICmr 29 (12 February 2024)
    - [declarations are provided in full below, see background]

- On 28 May 2025 the Administrative Review Tribunal affirmed the Commissioner's decision and declarations.
    - Court Data Australia and Office of the Australian Information Commissioner [2025] ARTA 876 (28 May 2025)
- On 12 July 2025, the Respondent advised the OAIC that it had fully complied with the Commissioner's declarations and had deleted the personal information that was the subject of the determination.
- The determination and declarations relate to one individual.

Does the determination require Court Data to remove the personal information of all individuals?

- While the determination relates to an individual complaint, and the majority of the declarations are specific to the personal information of that complainant, the determination also provides a clear statement on the application of the Privacy Act in the context of the acts and practices of Court Data with respect to the Court Data Australia Database.
- The final sentence of the declaration makes it clear that further collection, use or disclosure of personal information by Court Data contrary to APPs 3.5, 5 and 10.2 may result in further regulatory action.

If asked whether other complaints have been made?

- Individuals can make a complaint to the OAIC if they consider there has been an interference with their privacy.
- It would not be appropriate to comment on individual complaints that may or may not be under consideration by the Office.
    - *If pressed:* 9 individual complaints on hand at various stages.

What other action will you take if Court Data continues to publish personal information in breach of the Privacy Act?

- The Privacy Act confers a range of powers on the Commissioner including:
    - the power to investigate, conciliate and make determinations in relation to individual complaints
    - the power to undertake commissioner initiated investigations, and
    - powers to issue infringement notices and compliance notices, enter into enforceable undertakings and seek to commence civil penalty proceedings before a court.
- The OAIC's statement of regulatory approach provides information about how the Commissioner prioritises regulatory effort.

How does the Court Data Database work?

- Court Data collects information, including personal information, contained in court lists published by each Australian court and holds the information in the Court Data Australia Database (Database).
- Through its website, Court Data allows people to search the Database for the name of an individual or company in order to, as it describes it, 'see whether they have been scheduled to appear before all types of criminal or civil courts in any Australian state'.

Background

Full text – Declarations

'AHM' and JFA (Aust) Pty Ltd t/a Court Data Australia (Privacy) [2024] AICmr 29

The Commissioner made the following declarations under s 52(1)(b)(i)(B) of the Privacy Act:

the respondent engaged in conduct constituting an interference with the privacy of the complainant by:

a. *collecting the complainant's personal information in a way that was not fair, in that the respondent collected the complainant's personal information in a way that breached the Portal conditions of use, the complainant was not aware that the respondent was collecting their personal information, and the complainant could not reasonably have expected the respondent to collect their personal information, in breach of APP 3.5;*
b. *failing to take steps that were reasonable in the circumstances to ensure the complainant was aware of the APP 5 matters, including publishing a notice on its website setting out the APP 5 matters, in breach of APP 5;*
c. *failing to take steps that were reasonable in the circumstances to ensure the personal information it disclosed about the complainant was accurate, up-to-date, complete and relevant, having regard to the context and purpose for which that information was disclosed, including by failing to clearly articulate on its website the limits of the personal information it holds and discloses, and by inviting users of the Database to draw adverse inferences based on the personal information it discloses, in breach of APP 10.2;*

and must not repeat or continue such conduct.

The Commissioner also made the following declarations under s 52(1)(b)(i)(B) of the Privacy Act:

a. *The respondent must cease to collect personal information from the Portal in breach of the Portal's Conditions of Use and without the knowledge of the complainant whose personal information is collected.*

b. *The respondent must, within 30 days of this determination, ensure that any personal information that it has collected from the Portal in breach of the Portal Conditions of Use and without the knowledge of the complainant whose personal information is collected for the Database, is destroyed.*
c. *The respondent must, within 14 days of compliance with [b], report to the Office of the Australian Information Commissioner the steps that it took to ensure that the personal information referred to in [b] was destroyed.*

A failure by the respondent to cease collecting, using or disclosing any personal information contrary to APPs 3.5, 5 and 10.2 may result in further regulatory action.

ESTIMATES BRIEF: MATTER

Respondent name: Qantas

Type: Data breach notification/Individual and Representative complaints

---

Key details			
When did OAIC learn of matter?	**2 July 2025**		
How was OAIC advised/origin?	NDB		
Date action commenced	**11 July 2025**		
Age of matter in days	**Approximately 70 days**		
Jurisdiction	APPs, NDB		
Related representative action?	**Yes**		
Responsible Branch & team	Regulatory Action Division		
Content author	**Annan Boag**	Phone	s22
Clearance by	**Rowena Park**	Phone	s22
Brief current at	14 November 2025		

Brief description of matter

- Qantas suffered a data breach in late June 2025 due to a social engineering attack targeting an employee at an offshore contact centre.
- The incident affects the personal information of approximately 5.7 million Qantas customers.
- The OAIC has been working with Qantas to ensure it meets the requirements of the notifiable data breaches scheme, and we are satisfied it has done so.
- Separately, we have been handling individual and representative complaints made against Qantas. We are progressing these in accordance with Part V of the *Privacy Act 1988*.

Chronology

- On 30 June 2025, Qantas detected unauthorised access to a third-party platform used by one of its contact centres.
- On 2 July 2025, Qantas notified the OAIC about the incident as a precursor to a formal notification under the notifiable data breaches scheme. It also began notifying affected individuals.
- On 8 July 2025, Qantas provided a formal notification to the OAIC.

- On 17 July 2025, the OAIC received a representative complaint lodged by Maurice Blackburn Lawyers.
- On 11 September 2025, the OAIC wrote to Qantas informing it that we were satisfied it had met the requirements of the notifiable data breaches scheme.
- To date the OAIC has received 93 individual complaints, 47 were declined (most often because the individual had not complained to Qantas before complaining to the OAIC) and 46 remain active.

Current action

- We are satisfied that Qantas has met its obligations under the NDB scheme.
- We are considering the representative and individual complaints in accordance with Part V of the Privacy Act. This will involve consideration of whether the OAIC should investigate the data breach and whether it points to a failure by Qantas to take reasonable steps to secure personal information, as required by Australian Privacy Principle 11.

Background: public matters only

Incident

- In late June 2025, Qantas disclosed a significant data breach that affected approximately 5.7 million customers. The breach involves unauthorised access to personal information stored on a third-party IT platform used by a Qantas contact centre.
- The breach was the result of a social engineering attack targeting an employee at an offshore contact centre. This provided the malicious actor with access to a customer service platform. Qantas has stated that its primary systems were not compromised.
- The personal information of millions of frequent flyers was exposed. Qantas has indicated that for the majority of customers the compromised records were limited to:
    - Name
    - Email address
    - Qantas Frequent Flyer number (and in some cases, tier, status credits and points balance)

- Some customer records also include:
    - Address - this is a combination of residential addresses and business addresses including hotels for misplaced baggage delivery,
    - Date of Birth,
    - Phone number - mobile, landline and/or business,
    - Gender, and
    - Meal preferences.
- Qantas has stated no identity documents, credit card numbers or personal financial details were accessed or compromised as a result of the incident.

Response and regulatory engagement

- Qantas reported the incident to the Office of the Australian information Commissioner (OAIC) under the notifiable data breaches (NDB) scheme. It also informed the AFP and the ACSC.
- The OAIC has engaged with Qantas to ensure its compliance with the NDB scheme.[1] The OAIC wrote to Qantas on 10 September 2025 and indicated the OAIC was satisfied Qantas had met the requirements of the NDB scheme.

Current status

- Qantas has notified impacted customers and is offering a range of support services.[2]
- Plaintiff law firm Maurice Blackburn has lodged a representative complaint to the OAIC about the incident.[3]
- The OAIC is progressing the individual and representative complaints in accordance with Part V of the *Privacy Act 1988*.

[1] OAIC (2 July 2025) *Statement of Qantas Cyber Incident*. https://www.oaic.gov.au/news/media-centre/statement-on-qantas-cyber-incident.
[2] Qantas (11 September 2025) *Information for customers on cyber incident*. https://www.qantas.com/au/en/support/information-for-customers-on-cyber-incident.html.
[3] Maurice Blackburn, *Qantas Data Breach Representative Complaint*. https://www.mauriceblackburn.com.au/class-actions/join-a-class-action/qantas-data-breach/

Other issues

- **Managing potential conflicts of interest:** OAIC Commissioners are members of the Qantas Chairman's Lounge,[4] numerous OAIC staff are members of Qantas's frequent flyer program, and OAIC is a corporate customer of Qantas.
- Any declared real or apparent conflicts of interest in this matter will be managed in accordance with the OAIC's conflict of interest policies and procedures.

[4] OAIC (2025), *Gifts and benefits register*. https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/accountability/gifts-and-benefits-register

ESTIMATES BRIEF: OTHER Subject: Facial Recognition Technology

Type: Determinations

Key details			
Jurisdiction	Privacy		
Responsible Branch & team	**Determinations Team – Privacy Case Management**		
Content author	s22	Phone	s22
Clearance by	s22	Phone	s22
Brief current at	18 September 2025		

Brief overview

- The OAIC has finalised two Commissioner initiated investigations into the use of FRT in a retail setting: Bunnings and Kmart.
- Guidance on the use of FRT in commercial and retail settings was published in November 2024.

Bunnings determination

- Privacy Commissioner determination made 29 October 2024.
  - See D2025/013969.
- On review in the ART.
  - Heard by a full bench (3 members) of the Guidance and Review Panel on 22-26 October 2025.
  - The ART has reserved its decision.
- Bunnings' public statements on the appeal have focused on the need for safety for workers and customers in their stores, and their belief that they took a 'balanced approach' to implementing FRT. The following specific statements about the appeal come from the 'background' section of a linked media release issued by Bunnings:

- The [FRT] technology complemented extensive training, resources, leadership tools and policies Bunnings has in place to equip its team to handle threatening situations.
- Only a small team had access to the data and on positive identification, there was a clear process whereby it was checked to avoid false positives.
- To the extent that Bunnings does collect personal information in the course of our business, this is explained in our Bunnings Privacy Policy, which is available on our website. In addition, we let our customers know how we handle that information through signs at the various entry points to our stores, this includes a conditions of entry notice and a privacy information poster.
- *We acknowledge that* when we first started using FRT we did not specify this on our conditions of entry poster, however, we did make changes during the trial to refer to our use of FRT on both our entry sign and in our privacy policy.
- For the 12 months ending April 2024, there were about 700,000 retail crime events recorded by Australian retailers with 16% of those constituting threatening or violent behaviour, and 60% of store thefts are conducted by the same 10% of people.
- Theft is a major driver of abusive or threatening encounters, with one in five instances of recorded theft in Bunnings stores also involving verbal or physical abuse towards team.
- We would never act in a way that we believe would jeopardise customer privacy.

- On 27 February 2025, the Privacy Commissioner delivered a speech at the Retail Risk Conference.

- Referred to the Bunnings determination.
- Speech is available on the OAIC website.

Kmart determination

- Privacy Commissioner determination made 26 August 2024; published 18 September 2025.
  - See D2025/013969.
- Kmart has appealed the determination to the Administrative Review Tribunal (filed on 24 September 2025).
  - The review proceedings have been stayed by the ART until 21 days after a decision is made in the Bunnings appeal (orders made by the ART President, Justice Kyrou, on 13 November 2025).

Education and stakeholder engagement on FRT use and privacy

- On 2 July 2025 the OAIC, together with the Human Technology Institute, convened a stakeholder workshop to discuss and develop a better understanding of the benefits, risks and challenges when using FRT.
  - A key purpose of the workshop was to inform the development of further OAIC guidance for businesses on privacy protective practices when using FRT.
  - The workshop brought together a range of external stakeholders with interests in FRT, including industry representatives, retail associations, academics and civil societies.
- In January 2025, Commissioner Kind appeared on ABC's RN Breakfast and Radio Melbourne to respond to questions about the use of FRT at the Australian Open.

ESTIMATES BRIEF: OTHER

Subject: NDB Scheme

Type: Report

Key details			
Jurisdiction	Part IIIC of Privacy Act (NDB Scheme)		
Responsible Branch & team	Information Rights, Intake and Eligibility Branch		
Content author	s22	Phone	s22
Clearance by	**Rowena Park**	Phone	s22
Brief current at	**21 March 2025**		

Notifiable data breaches

- The threat of data breaches, especially through the efforts of malicious actors, is unlikely to diminish, and the OAIC continues to provide information to educate entities to help them keep personal information secure and to ensure they have an appropriate action plan should a breach occur.

- The latest NDB figures for the six months to 30 June 2025, show the OAIC was notified of 532 data breaches during the period, a 10% decrease compared with the previous six months. Since the start of the NDB scheme, the OAIC has observed a trend where more notifications are received in the second half of the calendar year.
- As part of our educational approach and to ensure our regulatory decisions are targeted and evidence-based, we have launched an interactive NDB dashboard.

Brief overview of NDB statistics

- In the 24-25 FY to 30 June we received 1,126 NDBs, a 12.5% increase from the previous year.
- Malicious or criminal attacks remained the largest source of data breaches (64% or 718 notifications).
- The health sector continues to have the most reported data breaches (19% of reported data breaches), followed by the Australian Government agencies (15%) and the finance sector (11%). In the previous year the positions of Australian Government agencies and the finance sector were reversed.
- We finalised 1,155 notifications under the NDB scheme in 2024-25, with 86% of notifications finalised within 60 days, exceeding our target of 80%.

Large scale data breaches

- In the 24-25 FY, we received:
    - 70 data breaches impacting more than 5,000 individuals
    - Two data breaches impacting more than 1 million individuals were notified.

ESTIMATES BRIEF: OTHER

Subject: Consumer Data Right

Type: Report

Key details			
What?	**Updates on CDR regime**		
Jurisdiction	Consumer Data Right		
Responsible Branch & team	RIS (Policy and Statutory Functions)		
Content author	s22	Phone	s22
Clearance by	Marcel Savary	Phone	s22
Brief current at	21 November 2025		

Implementation of government announced 'reset' of CDR

- In August 2024, the Government announced a 'reset' of the Consumer Data Right (CDR) to encourage adoption, reduce compliance load on participants, simplify the consent process and ensure safety for consumers.

- This reset is currently underway through ongoing updates to the CDR Rules, the expansion to non-bank lending and implementing suggestions outlined in the Costs Review Report for Treasury on CDR compliance.

- As part of the August 2024 CDR reset, the Government also signalled an intention to consider a full and formal ban on screen scraping and has asked the Treasury to advise on a way forward. The OAIC strongly supports this commitment, which reflects numerous submission recommendations made by the OAIC.

OAIC strategic planning

- The OAIC is currently adjusting how it performs its CDR role to reflect the government-announced reset and the shifting direction of the program.

- The OAIC's CDR Regulatory Strategy will outline our key areas of focus and key activities and will align with the whole-of-program strategy and policy decisions of Government about the future of the program.

- While this approach is still under development, the intention is to shift the emphasis of OAIC's CDR-related activities to include not only a focus on assurance of the CDR privacy safeguards, but also a wider focus on whole-of-economy data frameworks for data sharing, including the Australian Privacy Principles, which aligns with the proposals in Treasury's strategic plan for the future of the CDR.

Key updates to CDR scheme

Legislation

- On 4 March 2025, amendments to the *Competition and Consumer (Consumer Data Right) Rules 2020* took effect, which extended the operations of CDR to the non-bank lender sector.

- There will be staged implementation for consumer data sharing obligations from 9 November 2026, allowing a transition period for regulators and regulated entities to prepare.

- The OAIC is currently updating the Privacy Safeguard Guidelines and other guidance pieces following the rules changes.

Proposed CDR Rules amendments: operational requirements

- Treasury is currently consulting with CDR agencies on proposals for upcoming Rules amendments relating to operational matters that will align the Rules with the change in whole-of-program strategy to reduce costs for participants and increase uptake of CDR.

CDR assessments

- This year the OAIC has published 2 CDR assessments:
    - Outsourcing arrangements (on 28 April 2025), and
    - Data quality obligations for data holders (on 29 May 2025).
- To date, the OAIC has conducted 8 CDR assessments.

CDR complaints

- The OAIC manages all CDR complaints and operates the primary complaints portal (on the CDR.gov.au website).
- In 2025–26, as of 31 October 2025, we have received 85 contacts via the Online Complaint Tool – 33 for the ACCC and 53 for the OAIC.
- Of the 53 OAIC contacts, 47 have been declined under Section 36. When contacts are declined under section 36, it is deemed not a CDR-related complaint. If it is a privacy complaint, the complainant will be referred to the appropriate process.
- Three CDR complaints have been received so far this financial as of 31 October 2025, with one referred to EDR. One is still open, one has been withdrawn and the complaint referred to EDR is now closed.
- The remaining three contacts not declined under section 36 and not CDR complaints were enquiries where the OAIC provided general information about the CDR or referred the enquiry to a non-CDR regulator.
- For more information see pages 31 and 32 of the Key Statistics brief: D2025/026870

ESTIMATES BRIEF: OTHER

Subject: Credit reporting – Variation to the CR Code, soft enquiries framework and review of Part IIIA of the Privacy Act

Type: Report

Key details			
Jurisdiction	Part IIIA of the Privacy Act		
Responsible Branch & team	Regulatory, Intelligence and Strategy Branch, Policy and Statutory Functions Team		
Content author	s22	Phone	s22
Clearance by	Marcel Savary	Phone	s22
Brief current at	12 November 2025		

Complaints and enquiries data

- For the 2024-25 financial year, the OAIC received:
  - 106 enquiries relating to credit reporting, representing 3% of all privacy enquiries, and
  - 33 complaints relating to credit reporting, representing 2% of all privacy complaints.

Review of Australia's credit reporting framework (Part IIIA Review)

- The final report of the *Review of Australia's credit reporting framework* was publicly released on 27 November 2024.
- We understand Treasury is currently considering the report and intends to consult stakeholders on the report's recommendations.
- Several recommendations in the report relate to the OAIC's role as regulator, which we are currently considering (listed at **Attachment A**).

- The review also identified shortcomings in the current regulatory framework for the CR Code, including a need for more active regulation and enforcement. The review recommended either:
    - moving regulatory responsibility away from the OAIC, to give more oversight to general financial system regulators (especially ASIC), and/or
    - providing additional resources to the OAIC as the existing regulator for the system, to support more active enforcement.
- **Note:** In May 2025, a change to the Administrative Arrangements Order (AAO) formally transferred responsibility for credit reporting from the Attorney-General's portfolio to the Treasury portfolio, reflecting a Machinery of Government (MOG) change. This means functions relating to consumer credit reporting previously administered by AGD are now under the Treasury portfolio.

Soft enquiries framework and access seeker provisions

- One of the key recommendations from the *Review of Australia's credit reporting framework* relates to the establishment of a soft enquiries framework.
- The OAIC has outlined our position in a blog post on 13 March 2025. This blog was developed in consultation with key stakeholders.
- The aim of the blog post was to describe:
    - the intent of the access seeker provisions
    - the current uses of the access seeker provisions to conduct preliminary checks or soft enquiries

    - the findings and recommendations from the *Review of Australia's credit reporting framework* (the Review), and the OAIC's interim regulatory approach while the Government considers the review.

- Pending a government decision clarifying the use of the access seeker provisions, the OAIC will exercise discretion to ensure continued lawful use of the access seeker provisions in the Act, while discouraging further expansion of the use of those provisions when this is likely to be more closely regulated in future.

Variation to the *Privacy (Credit Reporting) Code 2024* (CR Code)

- On 20 March 2025, the Privacy Commissioner, with approval from the Information Commissioner under section 12(4) of the *Australian Information Commissioner Act 2010*, varied the independent review requirements of the CR Code, which requires the Commissioner to initiate an independent review every four years, to allow for a discretionary extension of up to two years.
- Public consultation was undertaken from 13 January 2025 to 21 February 2025.
- The OAIC received two submissions during the public consultation, both generally supportive of the proposed variation.
- The OAIC made amendments to its proposed variation in response to these submissions, and proceeded with the amendment.
- The Privacy Commissioner relied on this provision to defer the next independent review from March 2025 to 2027. Stakeholders did not express any concerns with this during the public consultation.

Consumer advocate roundtables

- In May 2025, the Privacy Commissioner held 2 roundtable sessions with consumer advocates to discuss credit reporting compliance.
- The roundtables were an opportunity for consumer advocates to raise issues ahead of the review of the CR Code in 2027.
- The sessions were an invaluable source of intelligence to help shape the OAIC's regulatory guidance and work priorities in relation to credit reporting, and we are currently considering this feedback.

Attachment A: Key recommendations of the *Review of Australia's credit reporting framework* relating to the OAIC

Rec #	Recommendation	Detail
19	Establishing a clear framework for soft enquiries in primary law	Amend the Privacy Act to set out categories of credit enquiries ('Information Requests') made to credit bureaus, such as for purposes of pre-screening and indicative pricing of credit applications, including 'soft enquiries' that cannot be disclosed to third parties, with details to be specified in the Privacy Regulation.
20	Clarifying the use of the access seeker provision	Amend the Privacy Act to improve the privacy and information security protections by: a) requiring Access Seekers to hold an Australian Credit Licence or be the consumer's professional advisor or advocate holding an authority (such as financial counsellors or financial advisors) b) prohibiting Access Seekers from disclosing a consumer's credit reporting information to third parties without the consumer's explicit consent.
24	Licensing of credit reporting bodies	Amend the legislation to introduce the following requirements on credit reporting bodies and the relevant regulator: a) credit reporting bodies should be required to hold a licence from the relevant regulator (OAIC or ASIC) b) the regulator should maintain and publish a register of licensed credit reporting bodies c) the regulator should have authority to implement appropriate risk management and related standards for credit reporting bodies as part of the licence conditions.

Rec #	Recommendation	Detail
25	Modernise the objects of the credit reporting legislation	Amend the Privacy Act to modernise the objects of credit reporting legislation to reflect important concepts such as fairness and competition, in addition to the existing objects of privacy and efficiency.
27	Streamlining credit reporting legislation	The Government should consider consolidating the credit reporting framework in the Privacy Act and Credit Act into its own streamlined Act.
28	Consider co-regulatory models to give ASIC a greater role	The Government should consider alternative models to improve regulatory oversight for credit reporting, such as by establishing a formal co-regulatory model between OAIC and ASIC.
29	Elevating credit reporting as a regulatory priority	Revise the Ministerial Statement of Expectations for the OAIC to expressly reference credit reporting. The OAIC and ASIC should develop an appropriate performance measure for credit reporting.
30	Enhanced regulator powers	Amend the Privacy Act to introduce new regulatory powers for instrument-making, exemption and surveillance activities specifically related to credit reporting to improve accountability, flexibility, and compliance, and to better align the regulation of credit reporting with financial sector regulation.
31	Improved regulator resourcing for credit reporting	The Government should increase budget resourcing for the relevant regulators to reflect the increased responsibility and compliance activity recommended by this Review.

ESTIMATES BRIEF: OTHER (REGIME)

Subject: Digital Identity

Type: Update

Key details			
Jurisdiction	Digital ID Act 2024 / general privacy		
Responsible Branch & team	Policy & Statutory Functions, Regulatory Intelligence and Strategy		
Content author	s22	Phone	s22
Clearance by	Marcel Savary	Phone	s22
Brief current at	10 November 2025		

Brief overview

- The Digital ID Act 2024 and Digital ID (Transitional and Consequential Provisions) Act 2024 and associated legislative instruments commenced on 1 December 2024.
- The OAIC is supportive of the legislative framework for Digital ID and the intention for the scheme to reduce the amount of personal information that needs to be shared across the economy.

OAIC activities

- On 26 February 2025, the OAIC published its Digital ID Regulatory Strategy which outlines how the OAIC will apply its range of powers to support a shift to more privacy protective identity verification practices and support trust and confidence in Australia's Digital ID system.
- The OAIC has a program of assessments underway to ensure that the privacy protections within the Digital ID system are operating effectively.

- The most recent Digital ID framework assessment, published on 27 August 2025, assessed the ATO in its role as operator of myID and the Relationship Authorisation Manager (RAM). It considered compliance with requirements for handling requests by enforcement agencies for access to personal and biometric information collected by myID and the RAM.
- As part of its *Digital ID Regulatory Strategy*, the OAIC also published an assessment on 29 October 2025 assessing the open and transparent management of personal information under APP 1 by Gateway Service Providers in the Document Verification Service.
- The OAIC continues to provide advice to the Department of Finance on proposed changes to the Digital ID rules and standards.

OAIC Digital ID operations

- The OAIC has transitioned from an implementation taskforce to prepare for Digital ID to a business-as-usual model.
- This model integrates Digital ID functions across the broader workforce, allowing the OAIC to manage its Digital ID responsibilities as part of its general operations.

Funding

- The OAIC has $5.6M in funding (or 25.5 ASL) for Digital ID activities, which terminates on 30 June 2026.
- We are in discussions with the Department of Finance about extending funding to support our continuing role overseeing privacy in Digital ID, including as Digital ID expands to onboard private sector entities to the Australian Government Digital ID System by the end of 2026.

ESTIMATES BRIEF: OTHER

Subject: My Health Record

Type: Report

Key details			
Jurisdiction	Privacy/My Health Record		
Responsible Branch & team	Policy and Statutory Functions, Regulatory Intelligence and Strategy		
Content author	s22	Phone	s22
Clearance by	Marcel Savary	Phone	s22
Brief current at	12 November 2025		

Brief overview of the OAIC's regulatory role

- The OAIC regulates the privacy aspects of the My Health Record (MHR) system and is conferred with specific functions for this purpose under the *My Health Records Act 2021* (Cth).
- This includes:
    - responding to enquiries and complaints about privacy breaches arising under the MHR system
    - handling data breach notifications relating to the MHR system, and
    - conducting privacy assessments and providing guidance.

Enquiries and complaints

- In the 2024/25 financial year, the OAIC received 4 privacy complaints and 18 enquiries relating to the MHR system.
    - This represents an 73% decrease in complaints, and 28% decrease in enquiries compared to the 2023/24 financial year.

- It is not possible to infer trends conclusively from one year of data, however the reduction in the number of notifications could indicate improved levels of maturity.

- In the 2025/26 financial year, as at 31 October 2025, the OAIC has received 4 privacy complaints and 2 enquiries relating to the MHR system

Notifiable Data Breaches

- In the 2024/25 financial year, the OAIC received 18 MHR data breach notifications. 17 out of 18 (94%) were closed within 60 days.
    - This is a 54% decrease in mandatory My Health Record data breach notifications compared to the 2023/24 financial year.
- As at 31 October 2025, for the 2025/26 financial year the OAIC has received 9 MHR data breach notifications.
    - 4 have been closed and 5 remain on foot.
    - 2 of the 4 closed notifications (50%) were finalised within 60 days.

Assessments and other regulatory activity

- In 2024/25, the OAIC commenced 2 assessments of private hospitals, examining their preparedness to respond to data breaches in the MHR system. The OAIC intends to finalise these 2 assessments in 2025/26.
- In 2024/25, the OAIC finalised our assessment of the ADHA's *myhealth* mobile health application.

- The OAIC assessed the ADHA's *myhealth* mobile health application and its compliance with APPs 1.2 (open and transparent management of personal information), APPs 1.3 and 1.4 (clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information) and APP 5 (notification of the collection of personal information).

- The assessment identified 3 medium privacy risks regarding the *myhealth* app's privacy policy's compliance with APPs 1.3 and 1.4. ADHA has accepted all of the assessment recommendations.

- The assessment has been published on our website.

Guidance and stakeholder engagement

OAIC guidance

- In 2024/25, the OAIC updated Chapter 8 of the *Guide to Health Privacy*, to assist clinicians to better understand their obligations under the Privacy Act when notifying at-risk relatives of genetic information with patient consent.
- The updates to Chapter 8 clarify that clinicians may legally collect relatives' contact details from patients and use those to contact at-risk relatives where there is patient consent.
    - The updates make no changes to the current guidance about notification without patient consent.

- The guidance makes it clear that the collection and use of the relative's contact details must still be done in accordance with the Privacy Act, but is permitted where a clinician reasonably believes the collection and use are necessary to lessen or prevent a serious threat to the life, health or safety of that relative.
- The guidance is available on our website.

Stakeholder engagement

- In 2024/25, officers from the OAIC met with government agencies and regulatory bodies that have administrative responsibilities for health services and policy to discuss the uptake in AI scribes across the medical profession.
    - Australian Health Practitioner Regulation Agency, the Australian Commission on Safety and Quality in Health Care (ACSQHC), Therapeutic Goods Administration, Australian Digital Health Agency and the Royal Australian College of General Practitioners.
        - if an AI scribe provides diagnostic suggestions, treatment recommendations, or performs analysis beyond transcribing, it is considered a medical device and must be included in the Australian Register of Therapeutic Goods.
- We reviewed AI guidance developed by ACSQHC and provided comments relating to privacy impacts.
- OAIC staff also met with AI Scribe providers to better understand potential privacy impacts resulting from use in a clinical setting.

Funding arrangements

- The OAIC's MHR regulatory role is funded through a terminating measure announced in the 2023/24 Federal Budget.
    - The funding was provided for 2023/24 and 2024/25; and subsequently extended to 2025/26 (with a 10% decrease).
- Our MHR function was previously funded under other terminating measures, and by way of Memoranda of Understanding arrangements with the Australian Digital Health Agency (ADHA).

Updating and modernising the MHR legislative framework

- OAIC is working on remaking the sunsetting *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016*, which prescribe the Information Commissioner's approach to exercising regulatory powers for the MHR system.
    - The revised instrument will address updates to the Commissioner's powers under the MHR Act and Privacy Act since 2016.
- OAIC has also provided input the Department of Health on drafting instructions around the remaking of MHR legislative instruments that will soon sunset.
    - This input focused on alignment with the APPs and guidance around retention periods for audit logs.
- OAIC has provided input to the Department of Health on draft Rules for implementing sharing-by-default for pathology and diagnostic imaging services for the MHR system.

- This input focused on recommendations to promote proactive transparent disclosure and privacy protections for consumers.

ESTIMATES BRIEF: OTHER

Subject: Digital Platform Regulators Forum

Type: Collaborative forum

Key details			
Jurisdiction	Privacy / Digital platforms		
Responsible Branch & team	Privacy Reform Implementation Taskforce, RIS Branch		
Content author	s22	Phone	s22
Clearance by	Marcel Savary	Phone	s22
Brief current at	21 November 2025		

Brief overview

- The Digital Platform Regulators Forum (known as DP-REG) was established in March 2022.
- DP-REG members share information about, and collaborate on, cross-cutting issues and activities involving the regulation of digital platforms. This includes consideration of how competition, consumer protection, privacy, online safety and data issues intersect.
- DP-REG's strategic priorities for 2024–26 are:
    - increase members' digital platforms regulatory capability
    - increase information/intelligence-sharing capability
    - collaborate on regulatory development
    - proactive engagement, and
    - understanding, assessing and responding to the benefits, risks and harms of technology, including AI models.

- The Information Commissioner attends the DP-REG Heads meeting, alongside the eSafety Commissioner Julie Inman Grant, ACCC Chair Gina Cass-Gottlieb and ACMA Chair Nerida O'Loughlin.

Current action

- The OAIC is continuing to engage at the Regulator Heads and Steering Committee levels.

Recent developments

- On 24 September 2025, DP-REG published a working paper on immersive technologies.
- On 16 September 2025, DP-REG members made a joint submission in response to the Productivity Commission's *Harnessing data and digital technology interim report*.
- On 27 June 2025, DP-REG members published a joint statement on the ACCC Digital Platform Services Inquiry 2020–2025, highlighting the ACCC's recommendation that DP-REG be endorsed as a permanent forum.

Background: public matters only

- DP-REG's joint submissions have largely raised awareness and provided information about the work of DP-REG and how it promotes a streamlined and cohesive approach to the regulation of digital platforms in Australia.

ESTIMATES BRIEF: OTHER (PROMINENT ISSUE)
Subject: AI (e.g. ChatGPT)

Key details			
Jurisdiction	General privacy		
Responsible Branch & team	Policy and Statutory Functions, Regulatory Intelligence and Strategy		
Content author	s22	Phone	s22
Clearance by	Marcel Savary Rowena Park	Phone	s22
Brief current at	12 November 2025		

Brief overview

- The OAIC is taking an active approach in monitoring the development of new AI technologies and particularly the emergence of generative AI.
- We are also engaging closely with international counterparts on regulatory investigations they are conducting into the global companies at the top of the artificial intelligence 'supply chain' under the auspices of the Global Privacy Assembly and the Asia Pacific Privacy Association.
- The OAIC has recently published guidance on:
    - Privacy and developing and training generative AI models
    - Privacy and the use of commercially available AI products

DeepSeek

- The OAIC supports the regulatory initiatives launched by Italy, Belgium, South Korea and elsewhere in relation to DeepSeek, and we are in regular contact with our international counterparts.

- At this stage, we are committed to continuing with our existing strategy and priorities as our global peers complement this action with actions into DeepSeek.

- The government has released a Protective Security Policy Framework Direction that bans all DeepSeek products, applications and web services from federal government systems and devices.

- South Australia has implemented a similar ban while other states and territories are considering further action.

Safe and responsible use of AI Workstream

- In September 2024, the Department of Industry, Science and Resources (DISR) published a Voluntary AI Safety Standard (VAISS) which contains 10 voluntary AI guardrails to help organisations across the AI supply chain to develop and deploy AI systems safely and reliably.

- In October 2024, the OAIC provided a submission to DISR on the *Proposals paper for introducing mandatory guardrails for AI in high-risk settings*.

- The OAIC supports the mandatory guardrails and favours a framework approach to implementation (Option 2) which uplifts existing regulatory frameworks and supports coordination.

- In February 2025, the OAIC met with the National AI Centre (NAIC) to be consulted on extending the VAISS to give practical guidance to developers of AI models and systems.

- In October 2025, NAIC published *Guidance for AI Adoption* as an update to the VAISS that condenses the 10 voluntary AI guardrails into 6 essential practices for responsible AI governance. The OAIC provided NAIC feedback on privacy practices.

- The OAIC has given feedback to the Department of Finance on their forthcoming APS AI Plan to introduce generative AI, basic AI training, and an 'AI adoption champion' across the APS. This focused on privacy, record-keeping, and freedom of information implications of AI use by government.

- The OAIC has given privacy-focused feedback to the Digital Transformation Agency on their forthcoming AI impact assessment tool. This tool provides Australian Government agencies with systematic guidance to assess the impacts and risks of AI use cases against Australia's AI Ethics Principles.

- In September 2025, the OAIC made a submission to the Productivity Commission (PC) on the interim report *Harnessing data and digital technology*. The OAIC supports a fair and reasonable test in the Privacy Act to improve trust, privacy and productivity in the AI era. The PC's proposed alternative compliance pathway and best interest obligation risks undermining these outcomes and creating regulatory uncertainty.

- The final PC report is awaited.

Meta AI

- It has come to our attention some Australian Facebook users have received notifications about commencement of AI training on user data.
- The OAIC has been in contact with Meta regarding this and understand from Meta that these notifications are as a result of a technical issue and relate to Meta's activities in other jurisdictions.

- IF ASKED ABOUT INVESTIGATIONS: The OAIC does not comment on ongoing investigations.

Data scraping

- In October 2024 we issued a concluding joint statement with 16 international counterparts on data scraping.
- The joint statement outlined expectations for organisations to comply with privacy and data protection laws, to use and regularly review safeguarding measures and to ensure permissible data scraping is done lawfully.
- The joint statement is published on our website.

Multimodal Foundation Models

- Through the Digital Platform Regulators Forum (DP-REG), the OAIC has recently published a Working Paper 3: Examination of technology: Multimodal Foundation Models (September 2024).
- A multimodal foundation model (MFM) is a type of generative AI that can process and output multiple data types, such as text, images and audio.
- This paper, which is available on our website, examines the impact of MFMs on the regulatory roles of each DP-REG member.

Automated decision making

- In January 2025, the OAIC provided a submission to the Attorney-General's Department in response to its Consultation Paper for Automated Decision-Making reforms.

- Our submission noted the OAIC's support for the development of a consistent legal framework for the use of ADM.

- The submission considered the intersection of ADM reforms with information access and privacy rights whilst also making recommendations that ensure appropriate consideration and mitigation of potential risks. This included a recommendation to ensure that consistent transparency obligations apply to the use of ADM whether or not it involves the handling of personal information.

- The OAIC has begun implementing the ADM transparency obligation that was introduced in the *Privacy and Other Legislation Amendment Act 2024* and will publish an issues paper in early 2026. The obligation will come into force on 10 December 2026.

Select Committee on Adopting Artificial Intelligence

- On 9 May 2024, DP-REG made a joint submission to the Select Committee on Adopting Artificial Intelligence drawing attention to the recent work of DP-REG and its members.

- The Senate Select Committee on Adopting AI released its final report in November 2024, making 13 recommendations.

AI Scribes

- In 2024–25 OAIC staff met with various health focused agencies and regulatory bodies to discuss the uptake in AI scribes across the medical profession.

    - These stakeholders included the Australian Health Practitioner Regulation Agency, the Australian Commission on Safety and Quality in Health Care (ACSQHC), Therapeutic Goods Administration (TGA), Australian Digital Health Agency and the Royal Australian College of General Practitioners.

- The OAIC has reviewed AI guidance developed by ACSQHC and provided comments relating to privacy impacts. The OAIC is in the process of developing a joint statement of regulatory expectations on AI scribes in clinical settings with the TGA.

- We have met with AI Scribe providers to better understand potential privacy impacts resulting from use in a clinical setting.

I-MED and AI training cases

- On 27 September 2024, the OAIC commenced preliminary inquiries into I-MED Radiology Network Limited in relation to the alleged disclosure of medical scans to a third-party for the purpose of training a diagnostic AI model.

- Our inquiries focussed on APP 5 and 6.

- A report into our preliminary inquiries was published on 31 July 2025.

- The Privacy Commissioner was satisfied that the medical scans had been sufficiently de-identified so that it was no longer personal information for the purposes of the Privacy Act.

OAIC guidance

- The OAIC intends to publish a blog post on the use of AI tools in the workplace, specifically based on a case study on ChatGPT, on the week of December 1.

- In October 2024, we published guidance on:
    - Privacy and developing and training generative AI models
    - Privacy and the use of commercially available AI products

To support the safe and responsible use of GovAI/GovChat, the Guidance and Publications team is currently considering developing a short, tailored AI guidance for the APS about the privacy and information governance considerations of using different AI tools (to complement our existing AI guidance).

GPA resolution and joint statement on AI

- The OAIC submitted a resolution which was passed at the 47th Global Privacy Assembly in September 2025 on the collection, use and disclosure of personal data to pre-train, train and fine tune AI models.
- The resolution set out a list of non-exhaustive data protection principles to be used to pre-train, train or fine-tune AI models, including:
    - Lawful and fair basis for processing
    - Purpose specification and use limitation
    - Data minimisation
    - Transparency
    - Accuracy
    - Data security
    - Accountability and privacy by design

    - Rights of data subjects
- A joint statement on AI was signed at the GPA. The joint statement was signed by 20 attendees including Australia and specifically addressed building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI.

Bilateral engagements for thought leadership and knowledge sharing

- On November 2025, the OAIC met with the Treasury Board of Canada Secretariat Access to Information Policy Centre to discuss approaches and implications around AI use for record keeping and freedom of information.

ESTIMATES BRIEF: MATTER

Subject: Vehicle privacy

Type: preliminary inquiries

Key details			
When did OAIC learn of matter?	s47E(d)		
Origin	Media reports		
Jurisdiction	General privacy - APPs		
Responsible Branch & team	Regulatory Action Division, Investigations Team		
Content author	s22	Phone	s22
Clearance by	Rowena Park	Phone	s22
Brief current at	**10 November 2025**		

Brief overview

- Connected vehicles use information and communications technologies to share data and communicate with drivers, other road uses, roadside infrastructure and other wireless services through in-built mobile or satellite network infrastructure.

- Media reports and other commentary have raised a range of privacy risks for connected vehicles, including:

    - broad collection of personal information
    - lack of transparency around collection, use and disclosure of personal information
    - absence of informed and meaningful consent
    - lack of individual control over their personal information, and
    - security of personal information.

- Several proposals in the Privacy Act Review may help address these risks, such as:
    - the introduction of a fair and reasonable standard for the collection, use and disclosure of personal information (proposal 12.1),
    - amending the definition of 'consent' to provide that consent must be voluntary, current, specific and unambiguous (proposal 11.1), and
    - requiring consent to handle precise geolocation tracking data and to trade personal information (proposals 4.10 and 20.4).

Current action and next steps

- The OAIC has identified 'new surveillance technologies such as location data tracking in apps, cars and other devices' within its 2025-26 Regulatory Priorities.
- From May to December 2024 OAIC made inquiries with select manufacturers to understand their Australian practices.
- The OAIC is not able to provide specific details about ongoing investigations.

Background: public matters only

Issues of note for OAIC

- A comprehensive study of connected vehicles' privacy practices was conducted by the Mozilla Foundation on the 25 major connected vehicle manufacturers' US-facing privacy policies.

- In March 2024 Reuters reported that the United States Commerce Department opened an investigation into whether Chinese vehicle imports pose national security risks due to concerns about the amount of 'sensitive data' being collected by connected vehicles.

- Dr Katherine Kemp of the University of NSW published the paper Driving Blind: The Unexamined Privacy Risks of Connected Cars on 19 November 2024. The report provides an in-depth analysis of privacy terms relevant to connected cars in Australia.

ESTIMATES BRIEF: OTHER

Subject: Children's Privacy Code

Type: Law Reform

Key details			
Jurisdiction	Privacy		
Responsible Branch & team	Privacy Reform Implementation Taskforce		
Content author	s22	Phone	s22
Clearance by	Marcel Savary	Phone	s22
Brief current at	21 November 2025		

Brief overview

- The Children's Online Privacy Code (the Code) will:
    - apply to social media and a wide range of other internet services likely to be accessed by children, including apps, websites and messaging platforms; and any APP entity specified in the Code
    - specify how these services must comply with the APPs and may impose additional requirements to the APPs, so long as the additional requirements are not contrary to, or inconsistent with the APPs.
- As Code developer, our objective is not to prevent children from engaging in the digital world, but rather to protect them within it through strengthened privacy protections.
- The OAIC must register the Code by 11 December 2026 and is on track to meet this deadline.

Current action

- OAIC have engaged AGS to provide legislative drafting service for the Code, legislative drafting commenced in November 2025.

- OAIC have ongoing engagement on the Code with:
    - International regulators (UK, Ireland, Canada)
    - the eSafety Commissioner (fortnightly), and
    - the Digital Platform Regulators Forum (DP-REG).

Recent developments

- Initial consultations with children, parents, child welfare organisations, civil society, academia and industry are **completed**:
    - Children, young people and parents were invited to share their views from 16 May–30 June 2025, with responses received from:
        - 161 primary school children, 74 high school children and 102 parents/carers.
    - In collaboration with Reset.Tech Australia:
        - National survey of 1,624 young people aged 13–17 (March 2025, YouGov)
        - Workshops with:
            - 57 young people in March and April, and
            - 70 attendees from academia and civil society, 7 April 2025.
    - 59 submissions to an Issues Paper.
    - OAIC convened 3 industry roundtables with 32 attendees across sectors.
    - The OAIC also met with several government agencies including:
        - National Children's Commissioner

        - National Commission for Aboriginal and Torres Strait Islander Children and Young People
        - National Indigenous Australians Agency.
- The OAIC released the 'Children's Consultation Report' in October 2025.
    - 70% of children do not like it when information about them is shared without their knowledge.
    - 45% percent of children do not want location tracking on by default and want to be notified when and why they their location is being tracked.
    - 60% of children want more control over their personal information through the right to access, update and delete.
- The OAIC met with 5Rights/Baroness Beeban Kidron and Commissioner Phillipe Dufresne, Privacy Commissioner of Canada (OPC) on 14 November 2025.

Expected next steps/dates

- OAIC expects to open consultations on the draft Code for public comment in early 2026.