OVIC
Office of the Victorian
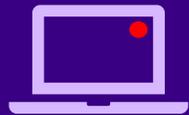Information Commissioner

Victorian Privacy Network

March 2026

A reminder – Today's session is being recorded.

# Acknowledgment of Country

Anthony Corso
Acting Privacy and Data Protection
Deputy Commissioner

We acknowledge the Wurundjeri people of the Kulin Nation as the Traditional Owners of the land from which we are presenting today.

We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.
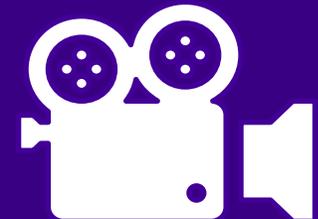
Housekeeping - What to be aware of
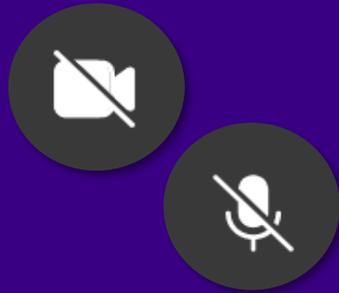
Cameras and mics have been muted for attendees**.**
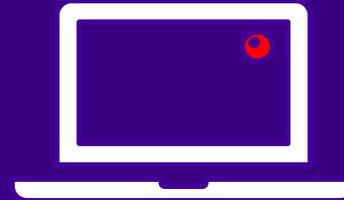
Today's session **is being recorded.**

A copy of the **recording** will be made available on our Vimeo website.

Housekeeping – How to engage

If you want to ask a **question,** type your question into the **Teams Q&A channel**.

Please leave us some **feedback** at the end of the meeting!

Today's agenda

Uplifting your privacy program
Felicity Wright
Transport Accident Commission

Use of Facial Recognition Technology in public spaces with insights from OVIC's regulatory action team
Cara O'Shanassy
Office of the Victorian Information Commissioner

Uplifting your privacy program

Felicity Wright, Information and Privacy Manager

Transport Accident Commission

Privacy Function Uplift

Victorian Privacy Network | 10 March 2026

TAC
Transport
Accident
Commission

Outline

1. Background

2. Purpose & Scope of Functional Uplift

3. Uplift Activities

- Policies & Work practices

- Third party risk management
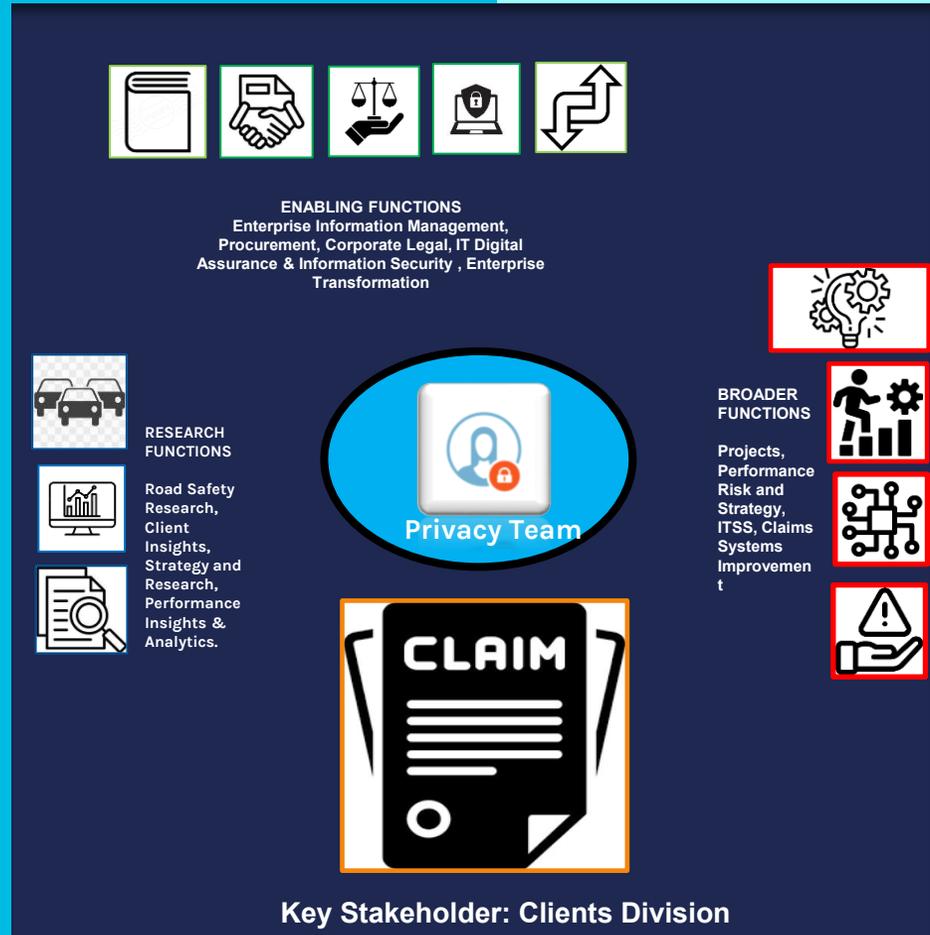
- Privacy Risk Tracking

4. Challenges

5. Outcomes

Background

Positives

- Relationships with key business stakeholders

- Relationships with enabling functions

- Annual Privacy Training and Privacy Awareness Week

- Privacy Incident reporting function

- Privacy Impact Assessment (PIA) processes

Opportunities

- Privacy 'Cultural Awareness' in key areas

- Formalising consultation processes with Privacy Function

- OVIC Standard 8 – VPDSS Audit (Third party risk management)

- Privacy Risk Tracking

- Policy and work practice updating

ENABLING FUNCTIONS
Enterprise Information Management, Procurement, Corporate Legal, IT Digital Assurance & Information Security , Enterprise Transformation

RESEARCH FUNCTIONS
Road Safety Research, Client Insights, Strategy and Research, Performance Insights & Analytics.

Privacy Team

BROADER FUNCTIONS
Projects, Performance Risk and Strategy, ITSS, Claims Systems Improvement

CLAIM

Key Stakeholder: Clients Division

Purpose & Scope of Functional Uplift

With a new CEO and Executive Leadership Team, in 2024 TAC began an ambitious uplift in its enterprise technology. The Privacy Function needed to uplift to meet the needs of the business and provide support to this program of work.

Privacy Governance

► TAC's Privacy framework and supporting policies were out of date. We needed to ensure they were in alignment with the requirements outlined in the 10 Information Privacy Principles and TAC Organisational Objectives.

Third Party Risk Management

► The Privacy team needs to ensure we are engaged for all new third-party contract arrangements, including new system implementations or major system upgrades.

Communication and Training

► Privacy training programs – do these need to be enhanced/extended beyond current audience (e.g. to high-risk roles at TAC and/or third-party service providers)

Actions | Privacy Governance: Policies & Work practices

Align Privacy framework to OVIC requirements and update or publish key policies & work practices…
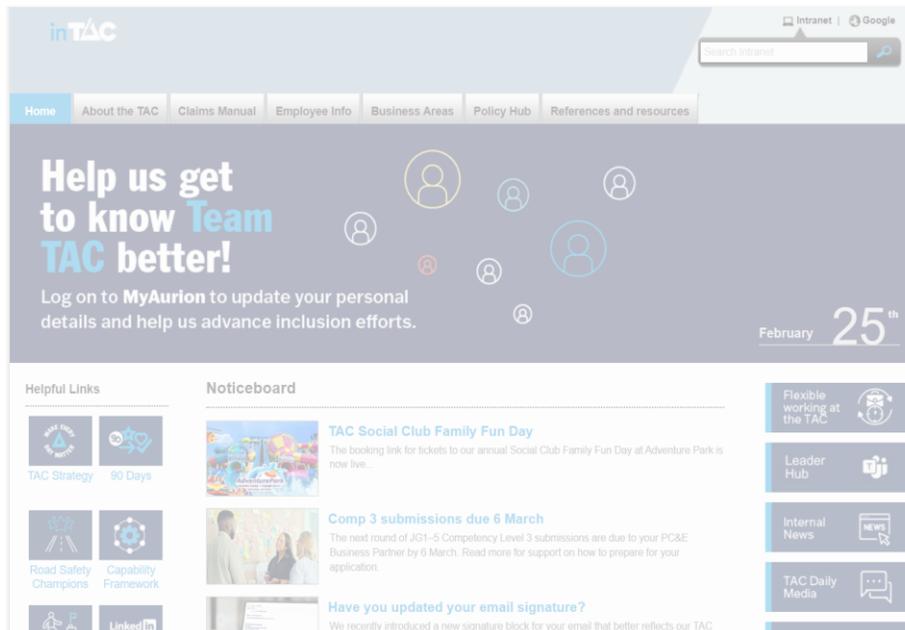
#	Document Name
1	TAC Privacy Strategy at 2016 - Outdated
2	Privacy Management Framework FW v2 DRAFT
3	2019-2022 - Privacy Strategy Framework - DRAFT TEXT
4	Website Privacy policy - TAC
5	TAC General Public Facing Privacy Policy (webpage)
6	TAC Workplace Monitoring Policy FINAL (Not Published)
7	TAC Workplace PRIVACY Policy - FINAL (Not Published)
8	TAC Data Privacy Policy v8.7 - Approved not published
9	TAC Data Privacy Procedures & Work Practices Directory v1.6 - Approved not published
10	TAC Data Breach Management & Notification Protocol - DRAFT
11	TAC Records & Information Management policy
12	Data Quality Policy
13	Privacy Incident Work Practice
14	Definitions
15	Principle 1 – Collection of Information
16	Principle 2 – Use and Disclosure of Information
17	Principle 3 – Keeping Information accurate and up to date
18	Principle 4 – Keeping Information Secure
19	Principle 5 – Openness use and disclosure of information
20	Principle 6 – Access and Correcting Information
21	Principle 7 – Identifying your claim
22	Principle 8 - Anonymity
23	Principle 9 – Transborder data flows
24	Principle 10 – Sensitive Information
25	Privacy Complaint Work practice
26	Information and Data Security Policy
27	TAC De-identification Policy
28	TAC Data Sharing Policy
29	When do you need to consult with the privacy team

Privacy Team

Performance Insights & Analytics
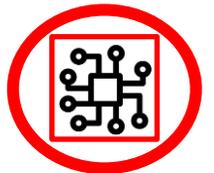
IT Digital Assurance & Information Security

Enterprise Information Management

Actions | TAC Service Providers: Third Party Risk Management

TAC's Procurement and Evaluation Plan & Project - Management Framework to include minimum, mandatory consultation requirements with Privacy Team.

Outline risk tiering process (inclusive of pre and post contract privacy questionnaire) and ongoing privacy assurance process for TAC Vendors.

Review TAC list of all third-party service providers handling PI/SI to confirm whether they had been assessed by the privacy team.

Review privacy training provided to TAC staff. Determine whether TAC needs to provide this (or specialised) training to any third-party service providers or TAC staff in high-risk roles.

Actions| Privacy Risk Tracking

Uplift tracking of Privacy team advice, identified risks and risk mitigation activities.
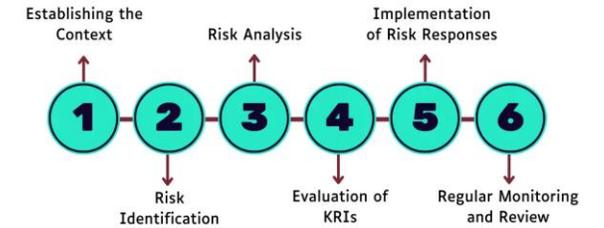

Update Privacy Risk Register and develop guidance on risks to be included.

Privacy & Risk Teams to confirm appropriate risk matrix to assess privacy risks.

RISK MONITORING PROCESS

Establishing the Context — 1
Risk Identification — 2
Risk Analysis — 3
Evaluation of KRIs — 4
Implementation of Risk Responses — 5
Regular Monitoring and Review — 6

Project Risk Register Template

Smartsheet Inc. ©2025

5x5 Risk Matrix Example

Impact
Measures the potential severity of the risk's consequences.

Probability — Measures how likely it is that a risk will occur.

	Insignificant (1)	Minor (2)	Significant (3)	Major (4)	Severe (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Moderate (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Rarely (1)	1	2	3	4	5

Challenges| Mitigations |

1. Time & Resourcing

Significant processes, frameworks, polices and work practices required development, drafting or reviewing – privacy BAU work still needed to be supported. Significant consultation across the business with other enabling functions and stakeholders.

How we did it: Information & Privacy Manager went 'offline' to support uplift. External consultant was engaged to review/produce as many artefacts as possible. Internal Project management supported.

2. Consistent Risk Analysis

Historical inconsistencies of opinion around application of TAC Corporate Risk matrix. Resolution has interdependencies with other matrices.

How we did it: Prioritise workshops to resolve Corporate Risk matrix application questions. Agree on an interim position in lieu of interdependencies.

Still to come

1. Data Governance documents

• *Data Privacy Policy*   • *De- identification Policy*
• *Data Privacy Procedures & Work Practices*   • *Data Sharing Policy*
• *Data Quality Policy*

Have recently been completed in consultation with Data Governance under the oversight of a committee.

2. Workplace policies

• *Workplace Monitoring Policy*

• *Workplace Privacy Policy*

Require engagement with TAC staff & the CPSU

Outcomes

Privacy Governance

► Most artefacts drafted, revised and published. TAC Privacy Function Intranet content updated (setting out when and how to engage with Team).

Third Party Risk Management

► Predictive Risk Tiering Assessment of Vendors to target high risk outsourcing implemented. Consultation processes with Procurement, Corporate Legal, Enterprise Transformation, Digital Security, Contract Management and Projects put in place and documented. Training program outline and funding for targeted third-party service providers approved.

Risk Tracking

► Data Protection Risk Matrix finalised and implemented. Privacy Risk Register updated. PIA Recommendation tracking process updated & documented. Protecht tool to be used to track all Privacy related risks and recommendations enterprise wide.

TAC Transport Accident Commission

Thank you

For more information

Felicity Wright | Information & Privacy Manager

Felicity_Wright@tac.vic.gov.au

TAC Transport Accident Commission

Use of Facial Recognition Technology in public spaces with insights from OVIC's regulatory action team

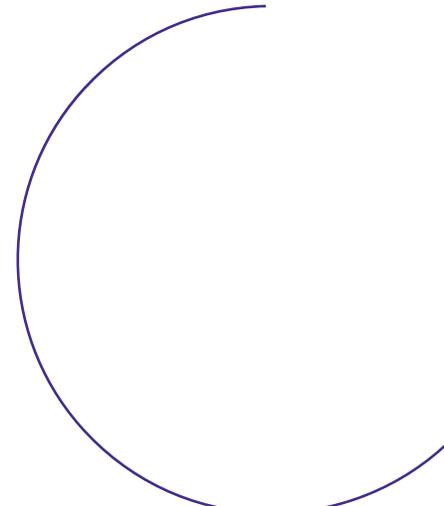Cara O'Shanassy, Chief Investigations and Compliance Officer

Office of the Victorian Information Commissioner

Use of Facial Recognition Technology in Public Spaces

Victorian Privacy Network
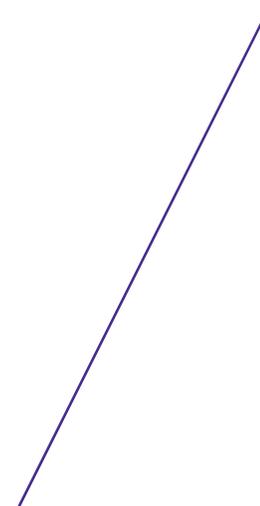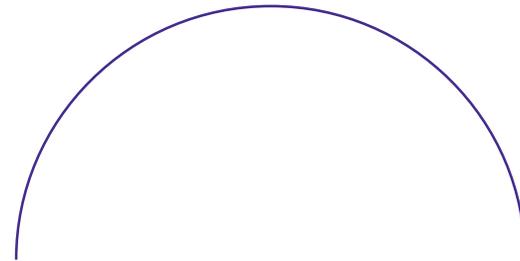
What is Facial Recognition Technology?

FRT in other Jurisdictions

OAIC, Bunnings and Kmart

OAIC original decision in the Bunnings case found the use of FRT by Bunnings contravened Australian Privacy Principles 1.2, 1.3, 3.3 and 5.1.

Bunnings appealed this decision. The Administrative appeals tribunal affirmed the OAIC's findings on APP 1 and 5. However the Tribunal found that the collection by Bunnings was permitted.

OAIC decision in Kmart found more transparency was needed for customers.

FRT in other Jurisdictions

New Zealand Privacy Commissioner

Supermarket ran a trial of FRT in some stores

Privacy Commissioner ran an inquiry alongside this trail of the FRT. The report found the use of FRT complied with the NZ Privacy legislation, though further improvements were recommended before permanently expanding the use of FRT in stores.

Key privacy issues that arise from FRT use

OVIC Office of the Victorian
Information Commissioner

Collection and Intrusiveness

IPP 1.1 – Collection must be necessary.

IPP 1.2 – Collection must not be unlawful,
unfair or unreasonably intrusive .

Consider

What is the purpose of collection?

Is there a less intrusive, alternative way to achieve that purpose?

Do I need all this personal information to achieve that purpose?

Transparency

IPP 1.3 – providing sufficient notice

Major consideration when implementing emerging technologies

Layered approach to collection

Consider

When is notice being provided?

Is notice accessible?

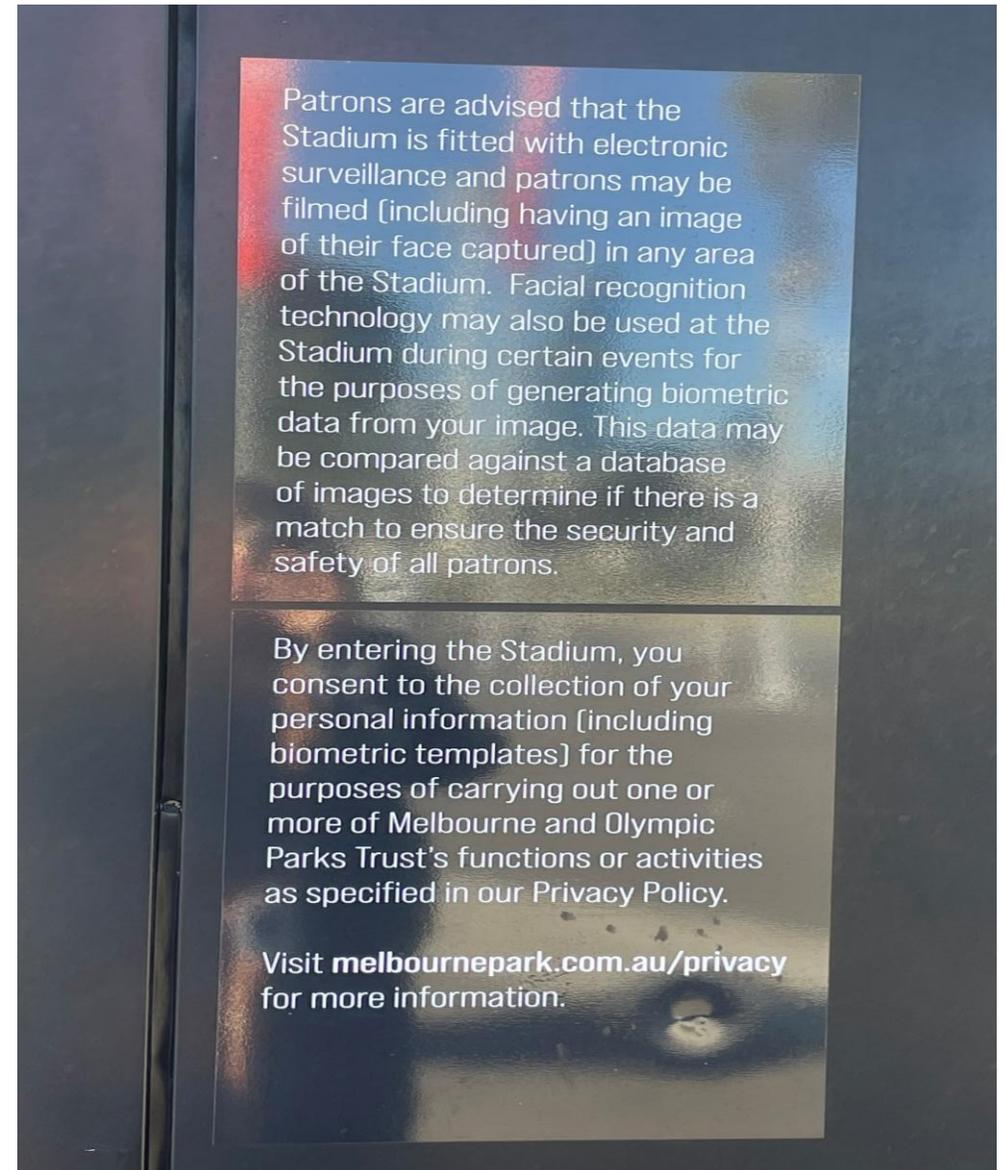*Does collection notice provide all details necessary*

Image provided by Melbourne and Olympic Parks Trust

OVIC Office of the Victorian Information Commissioner

Transparency

Layered approach to collection

Images provided by Melbourne and Olympic Parks
Trust

Patrons are advised that the Stadium is fitted with electronic surveillance and patrons may be filmed (including having an image of their face captured) in any area of the Stadium. Facial recognition technology may also be used at the Stadium during certain events for the purposes of generating biometric data from your image. This data may be compared against a database of images to determine if there is a match to ensure the security and safety of all patrons.

By entering the Stadium, you consent to the collection of your personal information (including biometric templates) for the purposes of carrying out one or more of Melbourne and Olympic Parks Trust's functions or activities as specified in our Privacy Policy.

Visit **melbournepark.com.au/privacy** for more information.

Disclosure to Third Parties

IPP 2.1 – Disclosure of information only where permitted

Consider

What was the purpose of collecting and what is the purpose of disclosing?

Why is disclosure occurring?

Who is this information being disclosed to?

Would an individual be aware of this disclosure?

Data Protection and Retention

IPP 4.1 – Reasonable steps to protect personal information for mishandling.

IPP 4.2 – Reasonable steps to destroy or permanently de-identify personal information.

Consider

Who needs access to this information?

Where is the information stored?

How could information be mishandled?

Does this information need to be retained?

What is the purpose of retaining the information?

How long does it need to be retained?

Key Takeaways

Proper due diligence can identify the key issues and risks when implementing a new process or technology.

A Privacy Impact Assessment can help with determining:

- Necessity
- Transparency
- Data Protection

Closing remarks

Anthony Corso, Privacy and Data Protection, Acting Deputy Commissioner

Office of the Victorian Information Commissioner

ⓘ For more information regarding this event or for any follow-up questions, please contact: **enquiries@ovic.vic.gov.au**

OVIC

www.ovic.vic.gov.au