Interactive Workshop: How to Risk-manage Facial Recognition Technology in Publicly Accessible Places

25 November 2025
12:30 – 17:30, Registration from 12:30
Canberra

WORKSHOP OUTLINE

Imagine: You are concerned about staff safety and theft. You decide to use a biometric like facial recognition to identify or record the actions of persistent customer miscreants. What advice would you give the board if they decide to proceed with facial recognition? (Biometrics Institute Privacy Guidelines)

The use of facial recognition technology (FRT) has been making headlines for many years now, gaining increased attention from regulators and enforcers and leading to an increasing public awareness over its use. This workshop, organised by the Biometrics Institute, will provide a better understanding of the responsible use of facial recognition technology and assess what good practice should look like. At a high-level it will address different use cases for FRT in publicly accessible places (retail, hospitality like sports ground, festivals, casinos, border e-gates), what they have in common and where they differ. It will then explore common risks and their mitigation by working through a risk-management methodology providing a series of questions. It will reveal how a change of a small criteria can change risk levels substantially and impact the question of proportionality of the use case.

By the end of the workshop, participants will have gained a much better understanding that there is not one-size-fits-all approach to facial recognition and should be able to apply the methodology to their own use case. This is also important for those who take over a biometric implementation and want to ensure that good practice has been applied. An added bonus will be that the Institute will use this workshop discussion to further shape its baseline "Go / No-go" questionnaire to assess whether to implement FRT for a specific use case. If you want to shape this thought process, this workshop is an absolute must-attend for the experienced biometric expert too.

Please note the workshop will take place on the day prior to the Biometrics Institute's Canberra *Showcase* (26 November).

For over 23 years, the Biometrics Institute has provided guidance and education on biometrics, helping its members to deliver on our mission of promoting the responsible, ethical and effective use of biometrics. The Biometrics Institute's *Three Laws of Biometrics* stresses that policy must come first, followed by process and then technology – which should be guided by policy and process. Most of our discussions have focused on government use of the technology, specifically in border management, law enforcement, policing and digital service delivery. Many of the lessons learnt on risk-managing FRT can be transferred to other use cases for example the retail, entertainment, hospitality and in-person service delivery sectors.

Attendees will take-away a better understanding of:

- What have different FRT use cases in publicly accessible places in common and how do they differ?
- What are common risks in using FRT?
- How can these risks be mitigated (to avoid any headlines)?
- How do I decide whether to use FRT? What are key considerations?
- What are base-line questions to ask to make the decision?
- Where can I get more information?

OVERVIEW

12:30 Registration and welcome coffee
13:00 Workshop sessions one to three
14:20 Coffee break and networking
14:40 Workshop session four to eight
16:30 Official workshop ends
16:45 Members-only discussion about recommendations and reporting
17:30 Close of workshop
Total learning time: 3 hours

AGENDA

12:30 Registration and welcome coffee

13:00 Workshop session one (90mins)

13:00 Welcome and introduction
Isabelle Moeller, Chief Executive, Biometrics Institute

13:05 Setting the scene (15mins)
- What are the Three Laws of Biometrics? How should they be used?
- Good Practice Framework – What does it look like?
- The *Use Case Matrix* and the three chosen use cases to be discussed

Isabelle Moeller, Chief Executive, Brett Feldon, Advisory Council Member, Biometrics Institute

13:20 SECTION ONE: Business goals of the project (20mins)
This first section will look at the chosen use cases and address questions outlined below. Participants are encouraged to contribute to the address the following questions:
- What are your business goals with this project?
- What exactly do you want to achieve?

Throughout the sections, participants will be able to discuss their own use case to test the very same questions to discover how they are similar or different.

13:40 SECTION TWO: Planning and management (20mins)
- What questions need to be answered now that you have decided on your business goals for this project?
- For example, the resources you need to plan, implement and manage the project?
- What are the upfront costs and the ongoing management and maintenance costs and resourcing?

14:00 SECTION THREE: Legal issues (20mins)
- Legal issues such as
    - the Australian Privacy Act (e.g. failure to protect the personal data base)
    - competition and consumer legislation relating to false advertising or
    - deprivation of liberty laws where someone is taken into custody as a result of the technology malfunctioning
    - the rights of redress such as defamation, due diligence and the failure to train staff properly so that they cause harm or distress

14:20 Coffee break and networking

14:40 SECTION FOUR: Policy and process (25mins)
- Data acquisition, enrolment and watchlist governance
- What is the process if there is a match?
- Human and machine – how good is the human? Who or what is the final decision maker?

15:05 SECTION FIVE: Privacy Impact Assessments (PIA) (20mins)
- The basics about conducting a PIA:
- What is a PIA?
- Why you need it
- What do you want to achieve (linking to goals discussed in section one)?

15:25 SECTION SIX: Technology choice (20mins)
- Choose the technology: What is the design? Why chose FRT?
- Has it been tested in a credible environment with an appropriate test database of people that it will encounter in your use case?
- Do you intend to conduct a trial?
- What is the roll-out plan?
- How will you handle the upgrades and maintenance?

15:45 SECTION SEVEN: Communications strategy (20mins)

- Do you have both an internal and external communications strategy?
- What will the public fear and what do users and other stakeholders need to know? (Remembering that the public quite often ignores the original announcement but gradually catches up, often due to publicised controversies about the project)
- Do you have crisis responses?
- Do you build the communications strategy early in the life of the project in order to adjust the technology choice or business model?
- How "Biometrics in Operation Signage" could be a step forward

16:05 SECTION EIGHT: Useful resources and round-up discussion (25mins)

- For more detailed work, such as Privacy Checklist, the Privacy Guidelines, Three Laws and the Framework

16:30 Official part of workshop ends

16:45 Members-only session to agree on key recommendations and reporting

During this session, which is exclusive to members, we will review key recommendations and decide what input (if any) the Institute should provide to policy-makers, regulators and enforcers. If you want to shape the responsible use of FRT, then this session is a must. New members are welcome, to join, find out more about membership.

17:30 Close of workshop

What will you take-away?

This interactive workshop will help participants apply the *Good Practice Framework* methodology to a chosen use case. You will learn about key considerations for risk-managing a FRT implementation, discover what the common concerns and risks are and how to mitigate against them. For any biometric implementation it is essential to be able to provide evidence that you have risk-managed your use case and thought about the likely issues that could occur.

The workshop offers the opportunity to meet real expert practitioners in biometrics and engage in open dialogue about successful biometric implementations and how to get there.

The workshop will provide deeper insights into three important guiding documents:

- *Three Laws of Biometrics*
- *Good Practice Framework*
- *Privacy Guidelines*

PLUS: Be in the room where it happens – The workshop will finish with a members-only session during which we will discuss:

- What could a checklist or questionnaire look like that contained baseline questions to decide early on whether biometrics is the right choice?
- What are the key messages we should deliver to regulators, policy and decision-makers to help balance innovation and a responsible future of biometrics?
- How should we promote the "Biometrics/FRT in use" signage that we have developed?
- Are there other things we should do to ensure biometrics, and specifically FRT use cases, are future-proof?

Who should attend?

- Those **new** to biometrics who want to sell and/or implement a biometrics system
- Those who take over the management of an **existing biometric system** and want to ensure that good practice has been applied
- Those who have **experience** with biometric implementations and want to help shape recommendations on what good looks like
- **Regulators and policy makers** who want to gain a better understanding of risk management in FRT usage

From the following sectors:

- Government including citizen service delivery, border management, law enforcement, and policing
- Retail, hospitality and entertainment (for example, sports grounds and festival organisers, casinos, pubs and clubs)
- AI biometric technology suppliers and integrators

We offer a group discount to encourage you to bring your whole team to the workshop, the legal and policy team, the technology expert as well as the communication and project management. Email us to receive a quote.

WORKSHOP PRESENTERS

Terry Aulich is the Head of Privacy and Policy Expert Group (PEG) of the Biometrics Institute. The PEG is one of the oldest committees within the Institute and has been instrumental in facilitating the development of an Australian Privacy Code in 2006 which has now morphed into the Privacy Guidelines. Other pieces of guidance include a Privacy Awareness Checklist which is currently being updated. Terry has facilitated a range of Privacy Workshops for the Biometrics Institute.
Terry Aulich is also the chairman of Aulich & Co, strategic advisors, pollsters and market researchers since 1993. He was an Australian state minister and federal senator for over sixteen years.

Brett Feldon is a Biometrics Institute Advisory Council member and is Head of the Biometrics Institute's Digital Identity Expert Group (DIG). He was previously on the board of the Institute from November 2011 until March 2019 and is based in Sydney, Australia. Brett's professional experience includes management and oversight of deployments of voice biometrics solutions in Australia, New Zealand, Hong Kong and the US, across a range of industries and government departments. The DIG has worked on a range of topics with regard to biometrics and digital identity and helped release the *Digital Onboarding and Biometrics* guiding paper in 2021, the *Digital Identity and Biometric Authentication* paper in 2023, and the *Mitigating Biometric Vulnerabilities in Digital Identity – Executive Briefing* in 2024.

VENUE

Canberra

COST

Member – A$620 (incl. GST)
Non-Member – A$865 (incl. GST)

REGISTRATION

Register at our website.

IMPORTANT DISCLAIMER NOTIFICATION

The Biometrics Institute provides training and course material as a tool to help you conduct due diligence. While the Institute has used reasonable care to ensure the accuracy of the material and course, due to the content and variable inputs during and after the process of implementing biometrics, the Institute cannot be held accountable for outcomes or compliance. The material and course have been prepared for informational purposes only and are not intended to provide legal or compliance advice. You should consult your legal advisor should you require advice on the legal or compliance aspects of the material or course.