Members' Viewpoints: The Use of Facial Recognition in Publicly Accessible Places

Version Public | 4 July 2025

Introduction

Over the years, the Biometrics Institute has engaged in the discussion on the responsible use of facial recognition through regular meetings of its global membership. In 2021, we published a paper asking the question: Should we ban facial recognition? following calls in the UK and USA to ban facial recognition (Ada Lovelace in 2025 and in 2022 , Electronic Frontier Foundation in 2022 and Center for Democracy and Technology in 2022).

In November 2024, the Office of the Australian Information Commissioner (OAIC) published Facial recognition technology: a guide to assessing the privacy risks which stimulated discussions amongst the Biometrics Institute members how this guidance will be implemented in practice.

More recently, in January 2025, the UK Minister of State for Crime, Policing and Fire of the United Kingdom, Dame Diana Johnson, started a programme of engagement about the use of live facial recognition (LFR) by police in the absence of a single law to give the police the power to use the technology. The Institute had the opportunity to participate in this debate and collected viewpoints from its diverse membership on the issue summarised in the Members' Viewpoints: Use of Facial Recognition in Policing.

The Institute organised an *On the Pulse Conversation* on the issue of the use of facial recognition in publicly accessible places in February 2025 followed up by a discussion session during the Asia-Pacific Conference in May 2025 in Sydney. The events presented a proposal to take one small step at a time to address the question of practical guidance and a way forward with facial recognition by presented standardised signage for the use of facial recognition in publicly accessible spaces.

The Institute will be attending a workshop held by the OAIC on the 2 July discussing facial recognition. In the lead-up to the workshop we have surveyed our members on the issue and will be publishing "Members' Viewpoints" in order to raise awareness about the following:

- The Biometrics Institute promotes the use of biometrics but only if used responsibly and ethically
- Biometrics are complex, different use cases present different levels of risk which need to be assessed, planned and managed carefully
- Missteps erode trust including those from other countries as the public suspect all such technology systems operate in the same way
- Using biometrics responsibly, requires informed decision-making, clear communication and transparency. Therefore, it's important that operations are fully transparent and are developed following the Institute's *Three Laws of Biometrics*, and *Good Practice Framework (GPF)*
- The Institute is well placed to provide these tools and accompanying guidance as the independent and impartial international membership organisation representing a diverse multi-stakeholder community from around the world, including law enforcement agencies and technology evaluation agencies, whose own experience and advice is useful

Key points

- Citizens are using their phone cameras to record faces and potentially submit these images to the police? Or they conduct their own facial recognition (Facebook). They are not seeking consent
- Police have conducated manual (human) facial regognition for decades. However, humans are generally worse at recognising people than facial recognition technology (*Diverse types of expertise in facial recognition* (2023)). Why are we so worried about automated (machine) facial recognition?
- Do retailers have a right to protect their staff from becoming future victims of attacks in stores? What about their basic human right to be safe?
- How are watchlists being created? There is no clear goverance around this. How does a person get added to that list? How can they be removed? How are the images stored securely? Who are the images being shared with?
- What about a retailers creating a "wall of shame" with pictures of known suspects? How does that impact on the privacy of individuals?
- It is clear that a consistent approach to the use of FR technology is critical, and its application through well-constructed policy and process
- The *Three Laws of Biometrics* have to be front of mind: Policy first, followed by process and then the technology. We can put all the right policies in place and test the technology but we require safeguards (processes) that ensure things are managed well when something goes wrong.

Biometrics Institute Members' viewpoints

The Biometrics Institute asked its members and stakeholders to provide their views on the responsible use of facial recognition. Their responses have been amalgamated below. Please note that the submissions have not been peer reviewed to confirm whether all the details submitted are factual and correct.

Lack of clarity and definition of what general considerations for FRT entail

The OAIC recently introduced its facial recognition technology (FRT) guidance, stating it outlines only "general considerations" for private sector organisations. However, the guidance **fails to clearly define what those considerations entail**, nor does it explain in what contexts FRT might fall outside such generalities.

As the Biometrics Institute has articulated in its *Members' Viewpoint Paper*, facial recognition can be deployed in a wide range of commercial and retail scenarios - across both public and private settings, and for live or static analysis – each presenting very different levels of privacy risk and requiring different mitigation strategies.

Point 1: The OAIC's decision not to acknowledge this complexity or to even cite the Biometrics Institute's well-established work on risk differentiation represents a significant regulatory oversight.

The tone and framing of the OAIC's material suggest a guideline designed primarily to justify a singular enforcement action – specifically its decision in the Bunnings case. The language, including claims such as *"FRT significantly interferes with the privacy of individuals,"* appears aimed more at deterring uptake than at fostering responsible, case-by-case adoption of facial recognition in lawful contexts. We note with interest the recent determination by the New Zealand Privacy Commissioner, who found that the use of FRT in a supermarket context – for the purposes of preventing and investigating unlawful conduct – was conducted lawfully and was proportionate. We can cite many other cases around the world where the use of FRT can be used lawfully without consent.

Point 2: Our company questions whether the OAIC has fully considered that FRT is not always used as a surveillance tool – **that it is also increasingly being used within compliance and safety-enhancing technologies**. In our case, it is deployed to enforce consent, reduce human error, and protect vulnerable individuals, especially children. As our CEO reminds us daily: "A spade is a tool. It can be used to plant a tree, or it can be used to cause harm. What matters is not the tool itself, but how it is used, and for what purpose." The ethical application of FRT can be a force for good—not just a risk.

Point 3: As a company deeply committed to advancing privacy-by-design principles, we have made every effort to align our technology with the OAIC's guidance, yet, despite this alignment, **we often feel as though we are working in isolation – pushing forward without the regulatory support needed to truly protect children.** While we strive to innovate responsibly, the lack of practical guidance or acknowledgement of best practice use cases by the OAIC leaves a gap – particularly when it comes to enabling privacy technologies that directly mitigate risk for vulnerable young people.
Point 4: As an organisation that provides compliance technology designed to operate effectively at scale within schools, **we respectfully emphasise that consent should not be viewed as the sole lawful basis for processing.** There are established alternative legal bases, such as where processing is reasonably necessary, appropriate, and proportionate, that support a legitimate and clearly justified purpose, particularly where the goal is to uphold legal obligations, protect individuals, and enable organisational compliance. We urge the OAIC to recognise the importance of balancing individual privacy rights with collective safeguarding interests, especially in contexts where vulnerable populations - such as children - may face serious risks if protections are not applied consistently and automatically.
In Conclusion
We are a locally owned and internationally recognised company in data protection operating across Australia, the United States and the UK. We have invested millions into building a **privacy-by-design platform** that aligns with OAIC guidance and regulatory best practices. Our hope is that this submission encourages the new Privacy Commissioner and the OAIC to take a forward-looking approach: one that supports innovation in privacy-enhancing technologies, including the responsible use of facial recognition, where it is used to uphold lawful compliance, minimise human error, reduce administrative burden, and protect children from harm.
The stakes are real. When privacy technology designed for safeguarding is discouraged, banned or delayed, the consequences are not theoretical – real people (children and adults) are placed at real risk. In some cases, lives are lost because these tools are not being used where they should be.
We thank the Biometrics Institute for the opportunity to provide this input and would welcome further discussion or clarification as required from the OAIC.

A challenge of passive versus reactive governance

The fundamental problem is passive and reactive governance, not just in Australia but internationally. The Institute has developed good practice guidance in all areas relating to biometric technologies and this, or something similar, should form the basis of a **proactive licensing regime** rather than the continual **'catch up' process currently employed by governments and regulators**.
The procedure should be 'Plan, do, review' but at the moment we are trying to manage with 'Do, review, plan.' The cart is firmly in front of the horse and the goal posts are continually moving.
Commercial companies should be free to innovate and introduce new technologies and use cases but these should be approved before implementation. Therefore, the types of issues that are going to be discussed at the Workshop should have been addressed when companies applied for permission to introduce a biometric system in a public space - not afterwards. The thorny topics such as consent, signage, individuals' right of redress etc. should be explored with the regulatory body during the planning stage and then, once approved, it would be the duty of the regulator to audit the system in operation to confirm compliance.
Currently, we are trying to make it all up as we go along - hence the Workshop. I would, therefore, recommend to them that they adopt a new proactive approach to biometrics to support its expanding use but, at the same time, prevent foreseeable problems of the sort that are under discussion.
The Institute's good practice guidance is an ideal benchmark for all regulators and could form an excellent basis for licensing new and emerging biometric technologies. Citizens' PII and sensitive data is worth protecting, no less than civil aviation standards, or safety in nuclear power facilities so maybe this is the time to seriously consider licensing as an essential concept in the 21st century. We need a system that is both fair and transparent for suppliers, regulators and, above all, those directly affected by biometric systems.

The Curious Case of Digital Double Standards: A Reality Check on FRT Logic

I write to express my bewilderment at the seemingly paradoxical position regarding facial recognition technology that has emerged in contemporary privacy discourse. After careful consideration, I find myself questioning whether we've perhaps gotten our regulatory wires crossed in ways that would make even Lewis Carroll's Mad Hatter tip his hat in confusion.

The Great Digital Paradox

Let me present what appears to be a fundamental logical inconsistency: we live in a world where recording someone's face digitally in public spaces is not only acceptable but ubiquitous. Every smartphone wielder, security camera, and tourist can capture, store, and share facial images without seeking consent. These digital images can subsequently be converted into any proprietary biometric template by any third party with the appropriate software—yet this raises nary an eyebrow from privacy advocates.

However, the moment we suggest performing this same conversion process in real-time for legitimate security purposes, suddenly we're told consent is required. This strikes me as rather like saying it's perfectly acceptable to leave your front door unlocked, but requiring permission to notice that it's unlocked.

The Template Mythology

The current discourse seems to suffer from a fundamental misunderstanding of how biometric systems actually function. There appears to be an almost mystical fear surrounding biometric templates, as if converting a facial image into a mathematical representation somehow makes it more invasive than retaining the original, reversible digital photograph. This is rather like arguing that a recipe is more dangerous than the actual cake—when in reality, the template is simply a mathematical abstraction. It is near-impossible to reverse-engineer it back into the original image.

If we're genuinely concerned about privacy invasion, shouldn't we be more worried about the permanent storage of high-resolution facial photographs than their conversion into irreversible mathematical representations?

The Human vs. Machine Paradox

Perhaps most perplexing is the apparent double standard applied to human versus automated recognition. A security guard can scan faces against a mental database of known troublemakers, banned individuals, or persons of interest without anyone questioning the need for consent. This human operator can make identification decisions based on facial recognition—often with far less accuracy than modern systems—and we consider this perfectly reasonable.

Yet when a machine performs the same task with superior accuracy, consistency, and without the potential for human bias or fatigue, suddenly we require explicit consent. This seems to suggest that inferior human judgment is somehow more palatable than superior machine precision—a position that defies both logic and public safety considerations.

The Watchlist Confusion

The current framework appears to conflate fundamentally different applications of FRT. Certainly, there are legitimate concerns about placing individuals on watchlists without probable cause—whether they're labeled as VIPs, persons of interest, or otherwise. However, comparing someone's image against an existing watchlist of individuals with legitimate law enforcement interest is an entirely different proposition.

This is analogous to the difference between adding someone's name to a no-fly list versus checking whether someone attempting to board a flight is already on that list. The former requires justification and due process; the latter is simply prudent security practice.

A Modest Proposal for Rational Discourse

I would suggest that our regulatory approach has become somewhat untethered from both technological reality and common sense. We've created a system where:

- Recording facial images is fine, but analysing them in real-time requires consent
- Storing reversible photographs is acceptable, but creating irreversible templates is invasive
- Human facial recognition is unquestioned, but more accurate machine recognition is problematic
- Checking legitimate watchlists somehow requires the consent of those being checked

Perhaps it's time to step back from this regulatory Alice in Wonderland and ask ourselves: what exactly are we trying to protect, and are our proposed solutions actually achieving those objectives?

Conclusion

I respectfully submit that the current discourse around FRT regulation has become divorced from both technological understanding and practical reality. Rather than reflexively requiring consent for every application of facial recognition technology, perhaps we should focus on ensuring appropriate oversight of watchlist creation, proper data handling practices, and transparent policies about retention and use.

After all, if we're going to regulate the Mad Hatter's tea party, we should at least understand what's actually in the teapot.

The governance, maintenance, and sharing of watchlists

My concerns are regarding the governance, maintenance, and sharing of watchlists, particularly where these lists are used in facial identification (1:many) systems in commercial or semi-public environments.

Key points for consideration:

- Watchlist Accuracy & Oversight: There is currently little public transparency around how individuals are added to or removed from watchlists. Criteria for inclusion are often vague or undisclosed, raising risks of unfair targeting or bias.
- Shared Watchlists: The sharing of watchlists across commercial entities or between private operators and law enforcement introduces serious privacy and accountability concerns. There is limited clarity on legal authority, chain of custody, data minimisation, and redress mechanisms when such sharing occurs.
- Proportionality & Purpose Limitation: In retail and commercial contexts, there is a risk that watchlists are used for purposes beyond their original intent, such as broader surveillance or profiling unrelated to legitimate security needs.
- Governance Frameworks: There is an urgent need for independent oversight and clear governance structures—defining responsibilities, access controls, audit mechanisms, and rights of affected individuals. How do people know they are on a watch list and is there a right to appeal?

I believe the development of any guidance around FRT use in these settings must address these foundational risks, particularly when watchlists are used or shared outside strictly controlled, accountable frameworks.

Responses to the workshop agenda items

• specific issues and use cases giving rise to proposals to use FRT in retail or commercial settings.

Reflecting on the development of use cases in UK and US retail sectors there is the very real risk that a general approach is taken which leads to mission creep and blurring of lines. Surely they need to consider each sector and then each use case with a clear justification for use and value outcome – applying the Three Laws of Biometrics to ensure legality, proportionality and necessity?

• factors to be considered in a risk-based approach to deployment of FRT in common retail or commercial settings, particularly related to spatial context, technical functionality and consent.

There's much detail to be addressed in this category of they are to do it right, they need to get the fundamental right on how are they defining and then assessing 'risk'. We have seen significant imperfections in what authorities are classifying as their risk parameters and then the measures to address these. They also shouldn't be considered in isolation of risk again of mission creep, data use and exploitation and how these data holdings could then be utilised by the authorities – police, tax and immigration as examples.

• the threshold for a risk-based application according to categories of spatial context of common publicly accessible commercial spaces (such as retail complexes and supermarkets) and restricted, semi-public commercial spaces (such as stadiums, pubs and clubs, theatres, etc).

Again these sectors need keen attention to separation. Use at a prominent sports event what could attract specific security risks has a totally different authority regime and risk profile than a corner

shop who suffers from the odd shoplifter. We should not tolerate lowest common denominator here to make the assessors job easier.

• risk-based guidance on the use of FRT applications, depending on their functionality (such as facial verification (1:1), facial identification (1:many) or facial analysis).

Would love to see the Three Laws of Biometrics, Good Practice Guide and foundational training from the Biometrics Institute applied here to the sectors – so they approach the problem from a knowledgeable point of view – and then make use of the Procurement guidance we have published!

• models of consent which consider the elements of consent required by the Privacy Act 1988 and the practical challenges of implementing models of consent in a commercial or retail setting.

As above – legality, proportionality and necessity need to run through all this and then the attention to data, holdings, use, privacy and disclosure protocols both internally to their risk and assurance teams and to the authorities.

• areas in which the current Privacy Act framework might be enhanced to more effectively and proportionately address privacy harms and concerns related to FRT.

I haven't had time to go through it all – but noting this potential rapid expansion I would advise that they need enhanced monitoring mechanisms so that the rules / Act can be refined on an evidence based mechanism as it will be challenged in its suitability here.

• possible systemic impacts of increasing use of FRT in retail and similar contexts on the right to privacy.

Risk escalation – as we have seen elsewhere – increased violence to staff, criminal damage to cameras, use of masks and disguises, targeting of youth to commit crimes as they get treated less harshly than adults by the law etc, breaches of privacy rules, racial discrimination and bias.

• cooperation and information sharing between retail entities and law enforcement agencies.

As above strict protocols are required and forward thinking as to what's likely to come next – as an example in the UK certain Forces are now creating CCTV hubs piping all the feeds into their control rooms for FR scanning and response from the commercial partners – a significant leap.

Australian guidance on facial recognition – how to?

The problem with the OAIC guidance as it stands is that they give a roadmap of what to do, but they don't give firm guidance of how to achieve a successful/positive outcome that one can have confidence will stand up to 3rd party scrutiny.

- Suppose Retailer Bunnings does a PIA and contends their use is "necessary and proportional"
- Someone (eg Choice Magazine) challenges it
- OAIC upholds the challenge, media implies Bunnings has broken privacy laws
- Administrative Appeals Tribunal now has to judge who is right …

One size does not fit all

Level 1 = public space FR surveillance … everyone understands why it might be wise to ban this

Level 2 = retail

- it is reasonable that stores have a right to protect their staff, patrons, property?
    - especially when Bunnings video shows THIS IS an issue
- people don't want armed guards patrolling stores to achieve security
- Security at entrance cannot recognize people banned/trouble-causers country wide in a chain like Bunnings – only FR can do that
- Whenever anyone does a business case it needs to be holistic. And cost of providing is part of that calculation – you cannot ignore things like cost of security guards in every store no matter how much Privacy advocates would like you to

Level 3 = clubs & casinos – don't forget in Australia they (and pubs) all want FR and are all running scared now

- Where people have to provide ID to enter and you can therefore potentially enforce at that time that they and their visitors give consent to FR, or they don't come in. Same as no id, cannot come in.
- Duty of care to protect self-declaring problem gamblers – can only do that with FR on the entrance to the club or the gaming floor

- This could also apply to stadiums as part of the ticketing process

Level 4 = Government National Security, Borders etc

Importance of Biometric Template Protection. Differentiate between on- and off-device

1. Raw biometric templates have sensitive data and will always be at a risk of breach. To that end, OAIC should look into and endorse modern Biometric Template Protection (BTP) schemes as per ISO 30136. This helps keep all biometric data secure as the protected templates become cancellable, unlinkable, and irreversible.
2. The guidance can shed more light on the preference between on-device verification and cloud verification. On-device verification is much more secure for 1-1 and 1-few matching scenarios since biometric templates never leave the device. This drastically reduces the risk of attacks.

Further considerations

The following links may be of interest to gain an understanding of the work going on in other sectors/ countries and in particular LFR.

The Biometrics Institute *Good Practice Framework (GPF)*

In 2020 the Institute published the *GPF*, a first-of-its-kind good practice tool that outlines the stages of the strategic planning, procurement and operation of a biometric system or network. It is a risk management tool helping with the decision-making process when implementing biometrics.

As every biometric use case and related policy is different, we offer tailored in-house workshops. A specific use case or organisational context for biometrics will be reviewed against the GPF to determine questions and issues relevant for your circumstances.

The Institute offers a range of education and guidance tools and more information is available from our website.

Proposed signage for the use of FRT in publicly accessible spaces

It is not an easy task to manage consent for the use of biometrics in publicly accessible spaces and this important discussion is ongoing. As a step in the right direction, the Biometrics Institute believes that is in the interests of all stakeholders that there is a clear, unambiguous sign for entities to advise the public that biometrics are used, and that the public can rely on this sign being displayed wherever such usage occurs (with exceptions where so legislated).

The Institute proposes that an unambiguous sign in icon and text form is agreed upon. An icon allows people who do not read the local language to be aware of the use of biometric systems. Text in the local language is also included in case the icon is not familiar to all initially.

Because most biometric data in public areas is captured by camera, it is proposed that the sign displays a typical surveillance camera sign icon. The Institute has created draft versions of a sign and sought feedback from its global membership over the past few months. The sign should be designed and used in such a way, and agreed with local regulators, such that it constitutes appropriate notice to people entering the area. The discussion is ongoing and we are hoping to finalise the sign in the coming weeks.

CONNECT NEW YORK

This is a public safety programme enabling the people of New York City to help keep their community safe.

https://newyorkcityconnect.org/

Live Facial Recognition: How does it work? Metropolitan Police in the UK

https://www.youtube.com/watch?v=oRGu_aK9TEo

Implementation of DHS Directive 026-11: Use of Face Recognition and Face Capture Technologies in the US
https://www.dhs.gov/sites/default/files/2025-01/25_0117_cio_Report-Select-Use-Cases-2024_Final-508.pdf

Privacy Commissioner New Zealand – FRT Inquiry Report June 2025
https://www.privacy.org.nz/focus-areas/frt-inquiry-report/
And specifically their recommendations:
https://www.privacy.org.nz/assets/DOCUMENTS/20250603-Factsheet-using-facial-recognition-technology-well-A1083621.pdf

About the Biometrics Institute

The Biometrics Institute is the independent and impartial international membership organisation for biometric users and other interested parties. It was established in 2001 to promote the responsible, ethical and effective use of biometrics. It has offices in London and Sydney.

The Institute represents a global and diverse multi-stakeholder community of over 200 membership organisations from 43 countries. While a large proportion of the members are from government, other members include banks, airlines, biometric experts, privacy experts, suppliers, academics and 18 Observers representing United Nations agencies, IGOs and European Union institution.

The Biometrics Institute connects the global biometrics community. It shares knowledge with its members and key stakeholders and most importantly, develops good practices and thought leadership for the responsible, ethical and effective use of biometrics.

For more information, visit www.biometricsinstitute.org

Contact:
Isabelle Moeller
Chief Executive
Biometrics Institute
isabelle@biometricsinstitute.org
Tel +44 7887 414 887

Dated: 23 June 2025