

Media Release

Media outlets have recently contacted the [Office of the Information Commissioner WA](#) (OIC WA) about [WA Police Force's Overt Live Facial Recognition Trial](#). The OIC WA is aware of the trial but was not invited to participate in any formal consultation process with WA Police and did not provide input into the design of the trial.

The OIC WA takes a keen interest in emerging technologies, including the use of biometrics technology. Facial recognition is one type of biometric technology, which identifies patterns in images of peoples' faces and compares them against one or many stored images to see if they match. Facial images are sensitive personal information, which is subject to additional obligations under the Privacy and Responsible Information Sharing Act 2024 (WA) (PRIS Act).

Biometrics are a higher-risk category of personal information because, once compromised, they are not easy to change. This is in contrast to, for example, less permanent information, such as credit card numbers, which can be more readily changed or replaced.

We know the community has concerns about the use of biometric technology. The Office of the Australian Information Commissioner (OAIC) recently released the [Australian Community Attitudes to Privacy Survey](#) which gathers perspectives on contemporary attitudes to privacy. It found:

- “comfort with the use of biometric analysis remains generally low” (p.63).
- “Australians are most likely to view the collection of sensitive and intrusive information as excessive or unjustified in most situations, regardless of the organisation or purpose, including data such as ... biometric information (71%)” (p.56).
- 45% of those surveyed (up from 27% in 2023) consider the biggest privacy risk they face today is facial recognition technology (p.13).
- there is a higher level of comfort in public safety settings (by state and federal police), though this is on a declining trend (from 60% in 2023 to 57% in 2026) (p.65).

While the OIC WA recognises responsible use of biometric technology can have public safety benefits, it can also have significant privacy risks that need to be eliminated or mitigated. Transparency and accountability around these risks and how they are being managed is central to building public trust in emerging technologies.

OIC WA welcomes the work WA Police has done to date towards addressing privacy risks and harms as part of the trial.

The following are some of the important concepts members of the community and regulated entities should be aware of in the roll out of biometric projects with large-scale public impact.

Mass collection of personal information

The use of real-time biometric identification in public spaces involves the collection of large amounts of sensitive personal information. Even where this information is only held for a very short time, it is still a collection and obligations attach to that activity.

Collective privacy

By focusing on individual privacy risk, the broader societal impacts of surveillance technology (collective privacy harms) are often overlooked. People often adjust their behaviour and speech if they feel like they are being watched. It is important to assess broader collective privacy harms and how they shape our communities.

Scope creep

As projects grow and evolve over time, the impact on privacy also changes and creates new risks that need to be managed. This “scope creep” is a real risk with projects involving biometric technology. For example, increases in the deployments, a shift to the use of covert technology or fixed widespread use (for example, using existing CCTV cameras) would significantly increase privacy risks.

Data quality

The potential for false matches resulting in unwarranted interventions is a known risk with the use of biometric technology, especially where images are taken in variable conditions or of populations where there is an increased rate of false positives or false negatives.

Automated decision-making

The PRIS Act is the first law in Australia to regulate the use of personal information in the context of automated decision-making, which can include the use of biometric technology in making law enforcement decisions. Information Privacy Principle 10 (IPP 10) requires entities seeking to automate all or part of a decision-making process to assess the risks of bias, harm and discrimination and provide assurance they are being properly addressed.

Privacy impact assessments

The PRIS Act also requires an assessment of privacy risks (called a privacy impact assessment or PIA) to be completed for projects involving significant privacy risks. The OIC WA is developing guidance on PIAs including when the conduct of independent PIAs should be considered.

The OIC WA intends to work closely with WA Police and is monitoring and requesting information, so that it can inform any potential future projects involving biometrics and automated decision-making.

9 July 2026