Oma plains by Jane Hoggard

AUGUST 2022

AI GUIDES

AI & FACIAL RECOGNITION TECHNOLOGY

Although facial recognition technology has been around in various forms for decades – the last few years have been marked by the rapid evolution of the technology and increased adoption rates around the world.

Today, facial recognition technology not only authorises your entry into some countries but unlocks your phone, helps locate criminals and, although not strictly recognition, if you are looking for work, may be used to analyse your job interview.

However, as the mainstream adoption of facial recognition technology by both government and private entities grows, questions are being increasingly raised around the world (by government, media and individuals alike) as to whether facial recognition technology should be used and, if so, in what situations.

BUT FIRST... WHAT IS FACIAL RECOGNITION TECHNOLOGY?

Facial recognition technology can be described as technology that can detect and analyse biometric data (for example mapping the underlying bone structure of a face or facial expressions) and reach conclusions based on that analysis. Two of the most common uses are:

a. verification (or authentication) of a known individual's identity via "one to one" matching. For example, SmartGates at Australian airports utilise facial recognition technology to undertake a biometric match of a person's facial features (when they are in front of the camera at the gate) with the information contained in that person's ePassport chip;[1] and

b. identification (or matching) of a potentially unknown individual via "one to many" matching. For example, law enforcement use this method to identify offenders and victims by matching faces to a database of images it has collected.

IS THE USE OF FACIAL RECOGNITION TECHNOLOGY LEGAL?

Whether you can legally use facial recognition technology depends on who you are and how you are using it. In Australia, users can be divided into groups.

The first is government users bound by 'specific' legislation relating to the collection and use of biometrics and facial recognition (such as the *Migration Act 1958* (Cth)).

The second is government and commercial users bound by 'general' legislation relating to either the data that is collected, used and disclosed (such as the *Privacy Act 1988* (Cth)) (**Privacy Act**) and/or the decisions that are made as a result of using facial recognition technology (such as restrictions on automated decision making and discrimination laws).

Internationally, a third category has been emerging – the commercial user bound by general and specific legislation. For example, some US States (such as Illinois, Texas and Washington) have specific biometric laws that limit how companies can collect, use and disclose biometric data. In 2021, New York City placed limits on how companies can collect biometric information, including requirements such as notices mandatory for establishments collecting biometric information from customers.

HOW DOES THE AUSTRALIAN PRIVACY ACT REGULATE FACIAL RECOGNITION SOFTWARE?

The information used by facial recognition systems will be sensitive information for the purposes of the Privacy Act (as it will involve use of biometric information for automated verification or identification purposes and/or the creation of biometric templates). As a result, organisations utilising facial recognition technology must comply with the stricter use and disclosure obligations that apply to this type of information under the Act. This will include ensuring that:

- they have consent from the individuals whose personal information is being processed (unless a narrow exception, such as public safety, applies) and that the information is reasonably necessary for one or more of the organisation's functions or activities; and
- only use the personal information for the purpose for which it was collected or for a directly related purpose.

Organisations who do not comply strictly with these requirements run the risk of complaints and investigations by the Australian privacy regulator, the Office of the Australian Information Commissioner (**OAIC**), in addition to public reputation risks. This is a real rather than theoretical risk – facial recognition is an active area of focus for the OAIC. For example:

- in October 2021, the OAIC determined that a customer survey tool used by 7-Eleven involved the collection of biometric information that was not reasonably necessary for its functions and that the information was collected without consent and without adequate notice;[2]
- in November 2021, the OAIC ordered Clearview AI (who scrapped biometric information from the web for the use of a facial recognition tool) to cease collecting facial images and biometric templates from individuals in Australia, and to destroy existing images and templates collected from Australia;[3] and
- in July 2022, the OAIC commenced an investigation into Bunnings and Kmart use of facial recognition technology in their retail stores following a report from consumer advocacy group, CHOICE.[4]

In some cases, the use of facial recognition technology will also be governed by surveillance laws. These laws differ between each State and Territory. Some jurisdictions also have laws specific to workplace surveillance, which may impose additional obligations on employers who use facial recognition technology on their workforce.

[1] See, for example, https://www.abf.gov.au/entering-and-leaving-australia/smartgates/arrivals.
[2] See the OAIC's public announcement, *OAIC finds against 7-Eleven over facial recognition* (14 October 2021) available here: https://www.oaic.gov.au/updates/news-and-media/oaic-finds-against-7-eleven-over-facial-recognition.
[3] See the OAIC's public announcement, *Clearview AI breached Australians' privacy* (3 November 2021) available here: https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy.
[4] See the OAIC's public announcement, *OAIC opens investigations into Bunnings and Kmart* (12 July 2022) available here: https://www.oaic.gov.au/updates/news-and-media/oaic-opens-investigations-into-bunnings-and-kmart.

WHY ARE PEOPLE (AND GOVERNMENTS) RAISING QUESTIONS ABOUT THE USE OF FACIAL RECOGNITION TECHNOLOGY?

We are increasingly seeing media and regulatory focus on the use of facial recognition technology spurred by the ethical and legal questions including:

a. should facial recognition technology be allowed at all (especially when combined with CCTV and other surveillance technologies (such as drones) that can produce a form of "live" monitoring of individuals)?

b. if so, should there be restrictions on who can use facial recognition technology? Should it be used for law enforcement by the police? Should it be used by retailers or other private sector organisations for security purposes?

c. should different types of facial recognition technology be treated the same? Is it the same if a retailer is using facial recognition technology for customer profiling and not security purposes?

d. can individuals adequately consent to the collection of their biometric information for facial recognition technology? Can customers give free and informed consent if they do not understand how their biometric information is going to be used?

e. is facial recognition technology sufficiently accurate to avoid incorrect and discriminatory, impacts? What happens if there are racial and/or gender bias in the datasets used for training the underlying technology? What happens if there is inadequate testing resulting in an unacceptable error rate (a particular issue in one-to-many applications where a 'false positive' match can have serious consequences for the underlying data subject)?

With the Australian Human Rights Commission making a public call for a temporary government mortarium on facial recognition in high-risk decision making;[5] the European Union (**EU**) under pressure to strengthen proposed restrictions on facial recognition technology in the draft Artificial Intelligence Act;[6] the Australian Government considering whether to introduce additional restrictions on facial recognition as part of the ongoing Privacy Act review;[7] the upcoming release of model laws on facial recognition technology as part of the UTS Facial Recognition Model Law Project;[8] and the current OAIC investigation into retailers use of facial recognition technology[9] – this is a space to watch!

WHAT DOES THIS MEAN FOR COMMERCIAL USES OF FACIAL RECOGNITION SOFTWARE?

Although we are currently waiting to see how the law in this area plays out – this does not mean that organisations cannot use facial recognition technology. Rather, it means that if an organisation wishes to utilise facial recognition technology, they must carefully assess the legality of the proposal and the expectations of the broader community.

To undertake such an assessment, it is recommended that organisations undertake a privacy impact assessment (also known as a PIA). Although not (currently) mandated for organisations in Australia, undertaking PIA's is considered best practise and aligns with regulatory requirements in the UK and EU (where the General Data Protection Regulation requires organisations to undertake "Data Protection Impact Assessments") and the requirements on Australian agencies. In the context of facial recognition technology, a PIA is fundamental to organisations considering "*the impact on privacy, the community's expectations and the need to comply with privacy law*" and "*whether they can achieve their goals in a less privacy intrusive way*".[10] Importantly, conducting a PIA will help avoid obvious compliance issues that may prompt complaints or investigations, and it will also help to be able to demonstrate compliance in the event that an investigation is conducted.

[5] See, e.g., page 111 of the Australian Human Rights Commissions Final Report on Human Rights and Technology (https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2021_Final_Report.pdf).
[6] See, e.g., https://www.europarl.europa.eu/doceo/document/CJ40-PR-731563_EN.pdf.
[7] See, e.g., https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.
[8] For more information, see the University of Technology Sydney's Facial Recognition Model Law Project page available here: https://www.uts.edu.au/partners-and-community/initiatives/social-justice-uts/centre-social-justice-inclusion/research-support/facial-recognition-technology-towards-model-law.
[9] See the OAIC's public announcement, OAIC opens investigations into Bunnings and Kmart (12 July 2022) available here: https://www.oaic.gov.au/updates/news-and-media/oaic-opens-investigations-into-bunnings-and-kmart.
[10] See the OAIC's public announcement, *Retailers must ensure compliance with privacy laws* (16 June 2022) available here: https://www.oaic.gov.au/updates/news-and-media/retailers-must-ensure-compliance-with-privacy-laws.

KEY CONTACTS

MICHAEL SWINSON

PARTNER
MELBOURNE

TEL +61 3 9643 4266
MOB +61 488 040 000
EMAIL michael.swinson@au.kwm.com

BRYONY EVANS

PARTNER
SYDNEY

TEL +61 2 9296 2565
MOB +61 428 610 023
EMAIL bryony.evans@au.kwm.com

KENDRA FOURACRE

SENIOR ASSOCIATE
MELBOURNE

TEL +61 3 9643 4105
MOB +61 437 959 826
EMAIL kendra.fouracre@au.kwm.com

KAI NASH

SOLICITOR
BRISBANE

TEL +61 7 3244 8157
MOB +61 401 250 434
EMAIL kai.nash@au.kwm.com

ABOUT KING & WOOD MALLESONS

A firm born in Asia, underpinned by world class capability. With over 2000 lawyers in 30 global locations, we draw from our Western and Eastern perspectives to deliver incisive counsel.

With 30 offices across Asia, Europe, North America and the Middle East we are strategically positioned on the ground in the world's growth markets and financial centres.

We help our clients manage their risk and enable their growth. Our full-service offering combines un-matched top tier local capability complemented with an international platform. We work with our clients to cut through the cultural, regulatory and technical barriers and get deals done in new markets.

JOIN THE CONVERSATION

SUBSCRIBE TO OUR WECHAT COMMUNITY.
SEARCH: KWM_CHINA

Asia Pacific | Europe | North America | Middle East
King & Wood Mallesons refers to the network of firms which are members of the King & Wood Mallesons network. See kwm.com for more information.

www.kwm.com