KING&WOOD MALLESONS
金杜律师事务所

AI Guides

AI and 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 main stream adoption of facial recognition technology by both government and private entities grows – questions are being increasingly raised around the world (including in prominent newspaper articles) 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 facial 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. Often used in law enforcement – this technology has received significant media attention in 2020 with the rise of ClearView AI - a research tool for law enforcement to identify both offenders and victims by matching faces to a database of images it has collected.[2]

So 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 the following groups:

(a) government users bound by 'specific' legislation relating to the collection and use of biometrics/ facial recognition (such as the *Migration Act 1958 (Cth)*); and

(b) 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)*) and/ or the decisions that may be made as a result of using facial recognition technology (such as restrictions on automated decision making and discrimination laws).

Internationally, there is also a third category rapidly emerging– the commercial user bound by both '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 and, since January 2020, employers in Illinois who wish to use facial recognition technology as part of their recruitment process must comply with the *Artificial Intelligence Video Act, Illinois HB 2557*. It is likely that additional regulation will be introduced in this space – a move that is publicly supported by the very companies who are currently pushing the boundaries of the technology.

So why are people (and governments) raising questions about the use of facial recognition technology?

The use of facial recognition technology raises a number of ethical and legal questions relating to:

(a) the use of facial recognition technology – especially when combined with CCTV and other surveillance technologies (such as

drones) that can produce a form of "live" monitoring of individuals. For example, in May 2019, San Francisco reacted to concerns around how it was using facial recognition (including by law enforcement) by banning the use of facial recognition by government agencies (although the ban has since been amended to allow some use of facial recognition, including phones that are unlocked using facial recognition);[3]

(b) access and disclosure of facial biometric data – for example, in 2019 the Australian government tabled the '*Identity-matching Services Bill 2019* and *Australian Passports Amendment (Identity-matching Services) Bill 2019* which (among other things) would have facilitated the sharing of facial images and other identify information between Commonwealth, State and Territory governments pursuant to the objectives of the Intergovernmental Agreement on Identity Matching Services agreed by COAG in 2017. However, upon review it was sent back for re-drafting to ensure that any such scheme is built around privacy, transparency and robust safeguards;[4]

(c) whether an individual has adequately consented to the collection of their biometric information – especially where an individual may not even know that facial recognition technology is being used and/or may not have a true ability to opt out; and

(d) whether the facial recognition technology is even accurate – for example, there are a swath of recent examples of facial recognition technology exhibiting racial and/or gender bias as a result of training datasets being used that are not sufficiently diverse. Where facial recognition technology is used to inform decisions about individuals, this may result in incorrect, and discriminatory, impacts

With public concerns, and the technology itself, evolving at rapid speed – it is important to ensure that any decision to use facial recognition technology is made on a case by case basis – taking into account legality, privacy and reputational risk.

1 See, for example, https://www.abf.gov.au/entering-and-leaving-australia/smartgates/arrivals

2 See, for example, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; https://clearview.ai/

3 https://sfgov.legistar.com/LegislationDetail.aspx?ID=4134650&GUID=35F4C6CB-4DC8-4CB6-9C34-B7A239F77823&Options=&Search=; https://sfgov.legistar.com/View.ashx?M=F&ID=7977061&GUID=DB0A925F-D942-4216-ACC5-CF6BE5E47CC7

4 https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024343/toc_pdf/AdvisoryreportontheIdentity-matchingServicesBill2019andtheAustralianPassportsAmendment(Identity-matchingServices)Bill2019.pdf;fileType=application%2Fpdf

The AI Guides are authored by:

John Swinson
Partner, Brisbane
T +61 7 3244 8050
john.swinson@au.kwm.com

Rebecca Slater
Senior Associate, Brisbane
T +61 7 3244 8147
rebecca.slater@au.kwm.com

Kendra Fouracre
Senior Associate, Melbourne
T +61 3 9643 4105
kendra.fouracre@au.kwm.com