Should Australia introduce mass facial recognition surveillance?

What they said…

'[These services] will help protect Australians by making it easier for security and law enforcement agencies to identify people who are suspects or victims of terrorist or other criminal activity'

Julie Bishop, Former Australian Foreign Minister, referring to the value of facial recognition technology

'It changes the world we're in. It's this idea that you can be watched anytime'

Professor Toby Walsh, a Fellow of the Australian Academy of Science and an Artificial Intelligence expert

The issue at a glance

On March 22, 2020, it was reported that governments around the world were using new and expanded forms of facial recognition technology to help prevent the spread of coronavirus. https://www.ifsecglobal.com/asia/can-cctv-help-contain-coronavirus/ Advocates have stressed the huge gains in individual accountability and community safety such technology can provide. Critics fear these developments will exacerbate the erosion of personal liberties.

On July 31, 2019, the Morrison government put before the parliament bills which would allow government agencies, telcos and banks to use facial recognition technology to collect and share images of people across the country.
https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd021
The government's identity-matching bills, Identity-matching Services Bill and the Passports Amendment Bill, aim to set up a national database of images captured through facial recognition technology and other pieces of information used to identify people, such as driver's licenses, passports, and visa photos. https://theconversation.com/why-the-governments-proposed-facial-recognition-database-is-causing-such-alarm-125811

On October 24, 2019, the plan was temporarily blocked when the Parliamentary Joint Committee on Intelligence and Security (PJCIS) handed down an extensive report calling for significant changes to the legislation to ensure stronger privacy protections and other safeguards against misuse. https://www.theguardian.com/australia-news/2019/oct/24/committee-led-by-coalition-rejects-facial-recognition-database-in-surprise-move

Background

A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database. It is also described as a Biometric Artificial Intelligence based application that can uniquely identify a person by analyzing patterns based on the person's facial textures and shape.
https://en.wikipedia.org/wiki/Facial_recognition_system#Commonwealth

While initially a form of computer application, it has seen wider uses in recent times on mobile platforms and in other forms of technology, such as robotics. It is typically used as access control in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.[2] Although the accuracy of facial recognition

system as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless and non-invasive process.[3] Recently, it has also become popular as a commercial identification and marketing tool.[4] Other applications include advanced human-computer interaction, video surveillance, automatic indexing of images, and video database, among others.
https://en.wikipedia.org/wiki/Facial_recognition_system#Commonwealth

Some current applications of facial recognition technology
The Commonwealth
https://en.wikipedia.org/wiki/Facial_recognition_system#Commonwealth
The Australian Border Force and New Zealand Customs Service have set up an automated border processing system called SmartGate that uses face recognition, which compares the face of the traveller with the data in the e-passport microchip. All Canadian international airports use facial recognition as part of the Primary Inspection Kiosk program that compares a traveler face to their photo stored on the ePassport. This program first came to Vancouver International Airport in early 2017 and was rolled up to all remaining international airports in 2018-2019. The Tocumen International Airport in Panama operates an airport-wide surveillance system using hundreds of live face recognition cameras to identify wanted individuals passing through the airport.
Police forces in the United Kingdom have been trialling live facial recognition technology at public events since 2015. However, a recent report and investigation by Big Brother Watch found that these systems were up to 98 percent inaccurate.
In May 2017, a man was arrested using an automatic facial recognition (AFR) system mounted on a van operated by the South Wales Police. Ars Technica reported that "this appears to be the first time [AFR] has led to an arrest".
Live facial recognition has been trialled since 2016 in the streets of London. It will be used on a regular basis from Metropolitan Police from beginning of 2020.

United Stateshttps://en.wikipedia.org/wiki/Facial_recognition_system#Commonwealth
The U.S. Department of State operates one of the largest face recognition systems in the world with a database of 117 million American adults, with photos typically drawn from driver's license photos. Although it is still far from completion, it is being put to use in certain cities to give clues as to who was in the photo. The FBI uses the photos as an investigative tool, not for positive identification. As of 2016, facial recognition was being used to identify people in photos taken by police in San Diego and Los Angeles (not on real-time video, and only against booking photos) and use was planned in West Virginia and Dallas.
In recent years Maryland has used face recognition by comparing people's faces to their driver's license photos. The system drew controversy when it was used in Baltimore to arrest unruly protesters after the death of Freddie Gray in police custody. Many other states are using or developing a similar system however some states have laws prohibiting its use.
The FBI has also instituted its Next Generation Identification program to include face recognition, as well as more traditional biometrics like fingerprints and iris scans, which can pull from both criminal and civil databases. The federal General Accountability Office criticized the FBI for not addressing various concerns related to privacy and accuracy.
In 2019, researchers reported that Immigration and Customs Enforcement uses facial recognition software against state driver's license databases, including for some states that provide licenses to undocumented immigrants.

China https://en.wikipedia.org/wiki/Facial_recognition_system#Commonwealth

As of late 2017, China has deployed facial recognition and artificial intelligence technology in Xinjiang. Reporters visiting the region found surveillance cameras installed every hundred meters or so in several cities, as well as facial recognition checkpoints at areas like gas stations, shopping centers, and mosque entrances. In 2020, China provided a grant to develop facial recognition technology to identify people wearing surgical or dust masks by matching solely to eyes and foreheads.

The Netherlands https://en.wikipedia.org/wiki/Facial_recognition_system#Commonwealth
The Netherlands has deployed facial recognition and artificial intelligence technology since 2016. The database of the Dutch police currently contains over 2.2 million pictures of 1.3 million Dutch citizens. This accounts for about 8 percent of the population. Hundreds of cameras have been deployed in the city of Amsterdam alone.

Attempts to extend the application of facial recognition technology in Australia
The Morrison government has sought to introduce laws which would allow Home Affairs to maintain centralised databases of facial images from government-issued documents (for example, passports and driver's licences) and other identity markers such as address and birthplace. https://www.afr.com/politics/federal/mass-surveillance-the-facial-recognition-bill-explained-20191029-p5358t
The Home Affairs department would then be able to use and transmit this information to perform a range of "identity-matching services" for other government agencies and non-government contractors. https://www.afr.com/politics/federal/mass-surveillance-the-facial-recognition-bill-explained-20191029-p5358t
The most general of these functions is identifying an unknown person by cross-referencing their image (say, from a CCTV screenshot) against the pictures in the database. But there are also more specialised services such as facial recognition to detect whether a person has multiple driver's licences. https://www.afr.com/politics/federal/mass-surveillance-the-facial-recognition-bill-explained-20191029-p5358t
The scope of activities for which the department could authorise the use of identity-matching services is expansive. Besides national security and law enforcement, it encompasses "community safety" and "road safety" activities, as well as "verifying identity".https://www.afr.com/politics/federal/mass-surveillance-the-facial-recognition-bill-explained-20191029-p5358t

Internet information

On March 22, 2020, IFSEC Global published a report titled ‘Can CCTV help contain the Coronavirus?’ which examined the use of facial recognition technology around the world in a bid to control the spread of coronavirus.
The full text can be accessed at https://www.ifsecglobal.com/asia/can-cctv-help-contain-coronavirus/

On March 13, 2020, Forbes published an article by Bernard Marr author of Artificial Intelligence in Practice: How 50 Companies Used AI and Machine Learning To Solve Problems. The article is titled ‘Coronavirus: How Artificial Intelligence, Data Science And Technology Is Used To Fight The Pandemic’
It presents some of the ways in which technology is being used around the world to combat the coronavirus.
The full text can be accessed at
https://www.forbes.com/sites/bernardmarr/2020/03/13/coronavirus-how-artificial-intelligence-data-science-and-technology-is-used-to-fight-the-pandemic/#37349a565f5f

On March 9, 2020, The Hill published a comment by Adonis Hoffman titled 'Facial recognition could stop terrorists before they act' which argues for the benefits of this technology.
The full text can be accessed at https://thehill.com/opinion/technology/486570-facial-recognition-could-stop-terrorists-before-they-act

On February 22, 2020, Gizmodo published an article titled 'Moscow Using Facial Recognition to Enforce Coronavirus Quarantine Of 2,500 Travellers From China' The item explains the use of this technology to prevent the spread of the coronavirus in Russia.
The full text can be accessed at https://www.gizmodo.com.au/2020/02/moscow-using-facial-recognition-to-enforce-coronavirus-quarantine-of-2500-travelers-from-china/

On February 17, 2020, Biometric Update,com published a report titled 'Advancing facial technology to fight identity fraud through liveness detection' which details the manner in which increasingly sophisticated facial recognition technology is being used to protect against identity theft.
The full text can be accessed at https://www.biometricupdate.com/202002/advancing-facial-technology-to-fight-identity-fraud-through-liveness-detection

On February 14, 2020, the ABC published an RMIT/ABC Fact Check titled 'Is facial recognition technology worse at identifying darker-skinned faces than lighter ones?'
The fact check concluded that a number of studies have demonstrated significant biases in the systems most commonly in use.
The full text can be accessed at https://www.abc.net.au/news/2020-02-04/fact-check-facial-recognition-darker-skin/11781192

On January 27, 2020, The Information Technology & Innovation Foundation published an article titled 'The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist nor Sexist'
The article explains that facial recognition technology is no longer prone to the biases that once distorted its results.
The full text can be accessed at https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms

On January 19, 2020, the Sydney Morning Herald published a report titled 'Australian police using face recognition software as privacy experts issue warning'
The article presents the way in which facial recognition technology is currently being deployed by police forces in Australia and the concerns of some privacy advocates.
The full text can be accessed at https://www.smh.com.au/national/australian-police-using-face-recognition-software-as-privacy-experts-issue-warning-20200119-p53ssj.html

On December 27, 2019, Sky News carried a report titled 'Govt urged to increase facial scans to counter increasing threats of terrorism'
The full text can be accessed at https://www.skynews.com.au/details/_6118302406001

On December 26, 2019, the Chicago Tribune reprinted from The New York Times an article titled 'Many facial-recognition systems are biased, says U.S. study' which explains the ethnically- and gender-based biases inherent in most facial recognition technology.

The full text can be accessed at https://www.chicagotribune.com/consumer-reviews/sns-facial-recognition-bias-20191226-cldfnnmqbzf6lp5w622jnw7oga-story.html

On November 1, 2019, The Saturday Paper published a report by Mike Seccombe outlining the concerns of privacy experts regarding the Morrison government's proposed changes to the law around the use of facial recognition technology. The article is titled 'Dutton's plan for a surveillance state'
The full text can be accessed at https://www.thesaturdaypaper.com.au/news/law-crime/2019/10/26/duttons-plan-surveillance-state/15720084008972?cb=1585819622
Please note: The Saturday Paper gives limited access to this publication to non-subscribers

On October 31, 2019, the Financial Review published an analysis titled '"Mass surveillance"? The facial recognition bill explained' which outlines a range of concerns that have been raised regarding the proposed legislation governing the use of facial recognition technology.
The full text can be accessed at https://www.afr.com/politics/federal/mass-surveillance-the-facial-recognition-bill-explained-20191029-p5358t

On October 25, 2019, The Conversation published an article by Sarah Moulds, lecturer of law at the University of South Australia, titled 'Why the government's proposed facial recognition database is causing such alarm' which examines the privacy and administrative issues raised by the proposed database.
The full text can be accessed at https://theconversation.com/why-the-governments-proposed-facial-recognition-database-is-causing-such-alarm-125811

On October 2, 2019, the Law Council of Australia made a submission titled 'Review of the Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019' which outlines in detail a number of the shortcomings of the proposed legislation.
The full text can be accessed at https://www.lawcouncil.asn.au/docs/3ceb93a3-3de6-e911-9400-005056be13b5/3692%20-%20Review%20of%20the%20IMS%20Bill%20and%20Passports%20Bill.pdf

On September 29, 2019, The Guardian published an article titled 'Plan for massive facial recognition database sparks privacy concerns' which outlines some of the criticisms made regarding the proposed expansion of Australia's use of facial recognition technology.
The full text can be accessed at https://www.theguardian.com/technology/2019/sep/29/plan-for-massive-facial-recognition-database-sparks-privacy-concerns

On July 26, 2019, Sydney Criminal Lawyers published on their website a comment titled 'Australia's Future Is Nationwide Facial Recognition Surveillance' which criticises the legal and human rights implications of the proposed facial recognition technology legislation.
The full text can be accessed at https://www.sydneycriminallawyers.com.au/blog/australias-future-is-nationwide-facial-recognition-surveillance/

On May 11, 2019, NBC News published an article presenting the manner in which facial recognition technology is becoming common practice among United States police. The article is titled 'How facial recognition became a routine policing tool in America'
The full text can be accessed at https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251

On May 3, 2018, the Australian Human Rights Commission published its arguments against Identity-matching Services Bill and the Passports Amendment Bill. The full text can be accessed at https://www.humanrights.gov.au/about/news/identity-matching-bills-threaten-our-rights

On July 27, 2017, Computer World published a report titled 'Government awards $22.5m facial recognition contract for airports' which reported on Australia's use of facial recognition technology for security purposes at airports.
The full text can be accessed at
https://www.computerworld.com/article/3470860/government-awards-22-5m-facial-recognition-contract-for-airports.html

Arguments in favour of Australia's Identity-matching Services Bill and the Passports Amendment Bill

1. An expanded use of facial recognition technology will help protect Australia against terrorist attacks

The Morrison government's primary motivation for an expanded use of facial recognition technology across Australia has been to reduce the likelihood on terrorist attacks.
On December 12, 2019, it was reported that the department of Home Affairs had warned the government the greater use of biometric facial recognition technology was needed to counter increasing threats of terrorism. In a detailed brief handed to Home Affairs Minister Peter Dutton - and obtained by the Australian under Freedom of Information laws - the department laid out a case for upgrading its capabilities in facial scans and said the department's IT systems are ageing and failing. https://www.skynews.com.au/details/_6118302406001
On February 12, 2018, the South Australian government produced a policy statement on the measures necessary in order to protect Australia from terrorist incursions. It stated, 'Since September 2014, there have been five attacks and 14 major disruption operations in relation to imminent terrorist attack planning in Australia. Australia is not immune to terrorists who are targeting vulnerable people, including youth, and attempting to radicalise them to commit acts of violence. Intelligence also indicates there are Australians currently fighting or engaged with terrorist groups overseas where they are gaining specialist knowledge and skills. While not all will return to Australia, any who do would pose significant threat to our safety and security.' https://www.asial.com.au/documents/item/1277
The policy statement further argues, 'Identity crime is a key enabler of terrorism…To combat this… the Commonwealth and other jurisdictions [need] to implement facial recognition capability. This will allow law enforcement and national security agencies to identify criminals earlier, including potential terrorists, by matching peoples' images with those on government record such as passports or drivers' licences.'
https://www.asial.com.au/documents/item/1277
Former Australian Foreign Minister, Julie Bishop, has stated, '[These services] will help protect Australians by making it easier for security and law enforcement agencies to identify people who are suspects or victims of terrorist or other criminal activity.'
https://www.sbs.com.au/news/debate-begins-on-facial-recognition-laws
In July 2017, while announcing the introduction of facial recognition technology at Australian airports, the Minister for Home Affairs, Peter Dutton, stated, 'Australia is committed to being a world leader in the use of biometrics at our border to facilitate legitimate travel, protect our community and prevent the activities of potential terrorists…'

https://www.computerworld.com/article/3470860/government-awards-22-5m-facial-recognition-contract-for-airports.html
Defenders of the use of facial recognition technology at Australian airports have drawn attention to the number of thwarted terrorist attacks that have been attempted. It has been noted that there have been foiled several planned attacks by radicalised locals, most notably in July 2017 when federal police arrested and charged several men who attempted to smuggle an explosive device onto a plane departing Sydney Airport. The Minister for Home Affairs, Peter Dutton, has stated, 'These terrorist plots showed a very real and disturbing danger.' https://www.reuters.com/article/us-australia-politics-budget-security/australia-to-spend-a300-million-to-upgrade-airport-security-amid-heightened-terror-fears-idUSKBN1I911M
Separately from the rollout of biometrics for traveller processing, the government has been building out the National Facial Biometric Matching Capability. A key part of the system, the Face Verification Service (FVS), went live in November 2016.
https://www.computerworld.com/article/3470860/government-awards-22-5m-facial-recognition-contract-for-airports.html
On March 9, 2020, Adonis Hoffman the chief executive officer of The Advisory Counsel, Inc, advised that governments in the United States, state and federal, need to adopt the type of facial recognition surveillance technology being considered in Australia. He stated, 'Our world is becoming more dangerous every day. As we stand on the doorstep of this new frontier, policymakers should err on the side of public safety…While AI cannot undo the terrorism of the past, it could mean the margin between success and failure, life and death, security and danger for us all in the future.' https://thehill.com/opinion/technology/486570-facial-recognition-could-stop-terrorists-before-they-act

2. An expanded use of facial recognition technology will help to guard against identity theft
Proponents of an expanded use of facial recognition technology in Australia argue that it will reduce the incidence of identity theft in Australia. When introducing the Passports Amendment Bill to federal parliament, the Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs, David Coleman, stated, 'The services will…contribute to preventing and detecting identity fraud…' https://migrationalliance.com.au/immigration-daily-news/entry/2019-08-australian-passports-amendment-identity-matching-services-bill-2019.html
Identity crime is one of the most common crimes in Australia. According to the Australian Institute of Criminology (AIC), the annual economic impact of identity crime exceeds $2 billion. A survey by the AIC found that identity crime 1 in 4 Australians have been a victim of identity crime at some point in their lives. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-crime
Misuse of personal information and identity crime remains an ongoing concern for Australians, with almost all respondents to the AIC's most recent survey (96.9%) indicating that misuse of personal information was, in their view, 'very serious' or 'somewhat serious'. Stolen and fraudulent identity credentials continue to be highly sought after by criminals, with a large amount of personal information obtained illegally online, by email, social media or through scams or data breaches. Identity crime is rarely an end in itself but is an important element in a wide range of other criminal activities. These include credit card fraud, superannuation and other financial frauds against individuals and welfare, tax and other frauds against government agencies.
Personal information is often obtained other than through the internet, with telephone and face-to-face methods being the two most prevalent methods employed. Although large numbers of identity crimes are reported officially, only a relatively small proportion of incidents result in police investigation and prosecution.

The impact of identity theft upon individuals can range from inconveniencing to highly distressing depending on how successful the identity thieves are in gaining private information and accessing sensitive accounts, such as bank accounts. The AIC study noted, 'Identity thieves can steal a person's personal identification information and access email and bank accounts very easily. This became quite apparent to a family in Sydney, who had their mobile phone details, Facebook account, email account and bank details accessed and changed by identity criminals within one hour.'

In an article published in Biometric.com on February 17, 2020, Sarah Amundsson, an international expert in digital identity verification, noted that governments and private businesses were increasingly adopting biometrics, including facial recognition technology, to enhance the security of those who have entrusted their data to government or corporate databases. These technologies rely on unique physical markers such as facial features, retina patterning or fingerprints to prevent fraudsters accessing valuable, private data. https://www.biometricupdate.com/202002/advancing-facial-technology-to-fight-identity-fraud-through-liveness-detection

Amundsson acknowledges that facial recognition technology may need to be developed even further to guard against hackers. She observes, 'As businesses rely heavily on digital onboarding, there's a need to introduce advanced AI-powered facial recognition technology that could help fight against criminals and enhancing facial recognition with 3D liveness detection provides a foolproof security solution.'

https://www.biometricupdate.com/202002/advancing-facial-technology-to-fight-identity-fraud-through-liveness-detection

On April 24, 2019, Peter Trepp of FaceFirst noted, 'Increased accuracy using hundreds of thousands of points of measurement has made facial recognition extremely reliable.' Trepp also explained the 'liveliness' measures that are in use to prevent thieves using photographs to replicate the individual whose data they were attempting to access.

Trepp advocates for the sort of biometric indicators that Australia's proposed expansion of its facial recognition network would rely upon. He states, 'Think about how easy it is to steal a key fob, a car key, a plane ticket or a social security number. It doesn't take a great deal of skill, planning or training to pull it off. Consider how a driver's license or credit card can be replicated. Then consider how much damage can be done with that data. By contrast, biometric identifiers such as facial templates… are incredibly difficult to replicate, and biometric template keys are extremely hard to spoof. Almost anything that prevents identity theft is ultimately a victory for personal privacy.' https://www.facefirst.com/blog/face-recognition-the-future-of-personal-identity-management/

3. Facial recognition technology can be used to help protect the community against a wide range of conventional crimes

In addition to its benefits in preventing some types of cybercrime, such as identity theft, advocates of the proposed facial recognition technology system proposed for Australia argue that it will be of great benefit in protecting the Australian community by discouraging more conventional crime.

Proponents of the new legislation point to the successful use of facial recognition technology as a crime fighting tool in other jurisdictions. United States police have emphasised the program's benefits, with the technology having already helped authorities solve a wide range of cases, from shoplifting to child abuse. In 2017, Indiana State Police were able to utilise Clearview AI technology to identify a killer who had been caught on video shooting a man in the stomach. The killer's identity was uncovered within 20 minutes of the Clearview AI search taking place. https://www.holmanwebb.com.au/blog/ai-facial-identification-technology-clearview

Currently, Amazon has given its facial recognition system to United States police departments to trial. An NBC News report published on May 11, 2019, gave an overview of some of the ways in which facial recognition technology is being used by United States police. In Colorado, local investigators foiled credit-card fraudsters, power-tool bandits and home-garage burglars and identified suspects in a shooting and a road-rage incident. In San Diego, officers snapped pictures of suspicious people in the field who refused to identify themselves. The technology has led to the capture of a serial robber in Indiana, a rapist in Pennsylvania, a car thief in Maine, robbery suspects in South Carolina, a sock thief in New York City and shoplifters in Washington County, Oregon. Currently the technology is being used as an investigative tool to help identify potential suspects; it is not recognised in courts and needs to be supplemented by other forms of evidence and police work. https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251

Facial recognition technology is also being used by the United States Federal Bureau of Investigation (FBI). The FBI can now search databases with more than 641 million photographs. Formerly, fingerprint analysis was the most widely used biometric technology for positively identifying arrestees and linking them with any previous criminal record. Beginning in 2010, the FBI started to replace the Integrated Automated Fingerprint Identification System (IAFIS) with Next Generation Identification (NGI), which not only includes fingerprint data from IAFIS and biographic data, but also provides new functionality and improves existing capabilities by incorporating advancements in biometrics, like face recognition technology. https://www.securitymagazine.com/articles/90332-fbi-using-more-facial-recognition-to-fight-crime

Agents with the FBI and Immigration and Customs Enforcement (ICE) have access to state driver's license databases and are able to scan through millions of Americans' photographs in order to detect criminals. There is regular use of facial recognition to track down suspects in low-level crimes, including cashing a stolen check and petty theft. https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ In 2017 the FBI used facial recognition technology to locate a gang member suspected of murder. Their apprehension of the man, later convicted of the crime, was assisted by using facial recognition technology to identify and locate his girlfriend. The crime had been committed six years earlier and the suspect was on the FBI's Ten Most Wanted Fugitives List. https://www.npr.org/2019/08/21/752484720/how-a-tip-and-facial-recognition-technology-helped-the-fbi-catch-a-killer

In January 2020, New South Wales and Victorian police confirmed that they use facial recognition technology as part of police work. A spokesperson for New South Wales Police Minister David Elliott said in a statement, 'Face Matching Services are being implemented to provide law enforcement with a powerful investigative tool to identify people associated with criminal activities.' A Victoria Police spokeswoman confirmed that Victoria Police are using a facial recognition system called iFACE to identify criminal suspects at 85 police stations. https://www.smh.com.au/national/australian-police-using-face-recognition-software-as-privacy-experts-issue-warning-20200119-p53ssj.html

4. Facial recognition technology can be used to prevent the spread of contagious diseases and advance public health

Since the advent of the coronavirus pandemic, advocates of facial recognition technology and its deployment by centralised agencies have noted the capacity of these systems to assist in the maintenance of public health.

A report from Reuters has indicated that facial recognition technology is currently being used to detect cases of coronavirus in China and help contain the spread of the outbreak. The report highlights one case study, indicating that authorities were able to track a resident from Hangzhou who had recently taken a trip to nearby Wenzhou – an area that has been affected by the virus – via the use of facial recognition cameras. The individual was subsequently instructed to stay indoors for two weeks. https://www.ifsecglobal.com/asia/can-cctv-help-contain-coronavirus/ It has also been reported that Guangzhou City is using thermometers on its city buses and employing facial recognition to scan passengers to quickly identify any symptoms of the virus. Some surveillance cameras have the ability to recognise low-grade fevers, and therefore may even be used to detect cases of the Coronavirus.

The Chinese industry ministry has reportedly since sent a message to the country's AI companies and research bodies to help identify new ways of containing the outbreak. According to reports, the thermometers can scan passenger foreheads in one second, sending an alert to the driver if an anomaly is detected. https://www.ifsecglobal.com/asia/can-cctv-help-contain-coronavirus/

Initially, as these reports surfaced, it was thought that the face masks many are wearing as part of protective measures may hinder the facial recognition technology. However, a company in China has outlined that the technology exists to identify people who are even wearing masks. https://www.ifsecglobal.com/asia/can-cctv-help-contain-coronavirus/

AI-powered interactive graphs are tracking the virus' migration across China, with the company working on creating an alert system, whereby users will be able to receive information about whether an infected individual has traveled within their vicinity. These graph models are also being used by the Chinese Government to find infected individuals and provide medical resources to them. https://www.ifsecglobal.com/asia/can-cctv-help-contain-coronavirus/

China has also indicated how it is using this technology to track travelers. The government has tracked arrivals later suspected to pose a risk and used facial recognition technology to locate their contacts. The same technology has also been used to track and monitor individuals who were originally given a false negative after being tested for the virus. https://www.gizmodo.com.au/2020/02/moscow-using-facial-recognition-to-enforce-coronavirus-quarantine-of-2500-travelers-from-china/

The Chinese government has developed a monitoring system called Health Code that uses big data to identify and assesses the risk of each individual based on their travel history, how much time they have spent in virus hotspots, and potential exposure to people carrying the virus. Citizens are assigned a color code (red, yellow, or green), which they can access via the popular apps WeChat or Alipay to indicate if they should be quarantined or allowed in public. https://www.forbes.com/sites/bernardmarr/2020/03/13/coronavirus-how-artificial-intelligence-data-science-and-technology-is-used-to-fight-the-pandemic/#2d2263dd5f5f

Similarly, the Dubai World Trade Centre recently announced it was taking extra-precautionary measures to control and monitor access to its Sheikh Rashid Tower and 'ensure the wellbeing of all our tenants and visitors'. In a message sent out to its customers, it stated: 'You will be passing through the thermal cameras/scanners and/or will be referred to be medically checked by medical professionals (if required).'

https://www.ifsecglobal.com/asia/can-cctv-help-contain-coronavirus/

In Moscow, a network of 100,000 cameras equipped with facial recognition technology are being used to make sure anyone placed under quarantine stays off the streets. The cameras are controlled from a purpose-built coronavirus control centre. Images and personal details of those under quarantine are put on a database so they can be recognised by the cameras. https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine

South Korea has also been using surveillance cameras, mobile phone location data and credit card records to track movements of coronavirus patients.
https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine
There has also been consideration given in Australia to the use of this technology to control the spread of the coronavirus. In recent weeks, Australian transport staff have been disinfecting tap on points at public transport entry and exit points. Facial recognition could do away with the need for the touch or 'tap' element in travel entirely. Some Australian governments are considering facial recognition trials in their transport networks with a view to future use. It has been claimed that the pandemic is likely to see these plans fast-tracked.
https://www.nec.com.au/insights/blog/facial-recognition-option-we-look-coronavirus-answers

5. Facial recognition technology is a reliable means of identification
Facial recognition technology has seen a range of advances that have largely overcome concerns regaining its accuracy.
In 2017 in his book Effective Physical Security Dr. Thomas J. Rzemyk wrote, 'Facial recognition technology has had several enhancements over the past decade post 9/11. In the mid-21st century, facial recognition was limited to characteristics related to the eyes, ears, nose, mouth, jawline, and cheek structure. Several private organizations have released updated technologies to both government and the public.
Newly enhanced technologies permit both verification and identification (open-set and closed-set). Facial recognition technology today uses complex mathematical representations and matching processes to compare facial features to several data sets using random (feature-based) and photometric (view-based) features.'
https://www.sciencedirect.com/topics/computer-science/facial-recognition
Advances in facial recognition technology are now reaching human recognition levels of accuracy. Facebook researchers are currently developing algorithms called 'DeepFace' to detect whether two faces in unfamiliar photographs are of the same person with 97.25% accuracy, regardless of lighting conditions or angles. As a comparison, humans generally have an average of 97.53% accuracy.
https://www.forbes.com/sites/amitchowdhry/2014/03/18/facebooks-deepface-software-can-match-faces-with-97-25-accuracy/#31e1987554fc
DeepFace creates a simulated neural network to work out a numerical description of the reoriented face to determine if there are similar enough descriptions from the two images. This network involves over 120 million parameters using locally connected layers. The DeepFace team trained the network using a dataset of 4 million facial images belonging to around 4,000 people. https://www.forbes.com/sites/amitchowdhry/2014/03/18/facebooks-deepface-software-can-match-faces-with-97-25-accuracy/#31e1987554fc These developments indicate that with expanded sources of photographic data from which to construct the database and with advances in technology automated facial recognition can operate with near-human accuracy.
In an article published in TNW on February 9, 2019, Christopher Shiostu explained the conditions necessary to create highly reliable facial recognition systems. Shiostu stated, 'The accuracy of a neural network depends on two things: your neural network and your training data set. The neural network needs enough layers and compute resources to process a raw image from facial detection through landmark recognition, normalization, and finally facial recognition. There are also various algorithms and techniques that can be employed at each stage to improve a system's accuracy. The training data must be large and diverse enough to accommodate potential variations, such as ethnicity or lighting.'

https://thenextweb.com/contributors/2019/02/09/facial-recognition-tech-sucks-but-its-inevitable/
It is also possible to lift the 'confidence level' of a facial recognition system so that only matches with a very high degree of correspondence are registered. A higher confidence threshold leads to fewer false positives and more false negatives. A lower confidence threshold leads to more false positives and fewer false negatives. However, raising confidence levels when judging how to act upon apparent 'matches' would help to ensure that law enforcement officers and others behaved in a manner that was appropriate to the level of confidence. https://thenextweb.com/contributors/2019/02/09/facial-recognition-tech-sucks-but-its-inevitable/
Shiostu concluded, 'Focusing on the quality and size of data used to train neural networks could improve the accuracy of facial recognition software. Simply training algorithms with more diverse datasets could alleviate some of the fears of misprofiling minorities.' https://thenextweb.com/contributors/2019/02/09/facial-recognition-tech-sucks-but-its-inevitable/
On January 27, 2020, it was reported, 'The [United States] National Institute of Standards and Technology (NIST) recently released a report that examined the accuracy of facial recognition algorithms across different demographic groups. The NIST report found that the most accurate algorithms were highly accurate across all demographic groups.' https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms

Arguments against Australia's Identity-matching Services Bill and the Passports Amendment Bill

1. The Bills have an excessively wide scope
It has been claimed that that the Bills expanding Australia's use of facial recognition technology do not make it sufficiently clear who can access the data drawn on and the matches obtained. This, it is claimed, allows for misuse of the data and an ongoing expansion of its use in ways not stipulated by the proposed legislation.
Microsoft president Brad Smith warned in December 2019, 'The facial recognition genie, so to speak, is just emerging from the bottle. A government … could follow anyone anywhere, or for that matter, everyone everywhere. It could do this at any time or even all the time. This use of facial recognition technology could unleash mass surveillance on an unprecedented scale.'
In an opinion piece published in The Conversation on October 25, 2019, Sarah Moulds, Lecturer of Law at the University of South Australia, stated, 'Much of the detail about precisely who can access the system and what limits apply is not set out in the bills. This will be determined through government regulation or subsequent intergovernmental agreements.' https://theconversation.com/why-the-governments-proposed-facial-recognition-database-is-causing-such-alarm-125811
Dr Moulds explained further, 'Legal bodies have argued that amendments are needed to tighten the boundaries of who can access the identity-matching services and for what purposes. They note that as currently drafted, the proposed laws give too much discretionary power to government officials and actually create opportunities for identity theft.' https://theconversation.com/why-the-governments-proposed-facial-recognition-database-is-causing-such-alarm-125811
The Law Council of Australia has stated there is a need to 'ensure that identification information produced in response to a request for an identity-matching service is not used for any purpose other than establishing or verifying the identity.'

https://www.lawcouncil.asn.au/docs/3ceb93a3-3de6-e911-9400-005056be13b5/3692%20-%20Review%20of%20the%20IMS%20Bill%20and%20Passports%20Bill.pdf
The Australian Privacy Foundation has further argued that the proposal is highly invasive, as the system could be integrated into a number of other systems that collect facial data, including closed-circuit television.
The Foundation has stated, 'We are on our way to automated and real-time surveillance of public spaces.' https://www.theguardian.com/technology/2019/sep/29/plan-for-massive-facial-recognition-database-sparks-privacy-concerns
Dr Moulds has pointed to two additional related concerns, stating, '[Unregulated expansion of access to the surveillance] is particularly problematic when coupled with the potential for the rapid spread of facial recognition technology in Australian streets, parks and transport hubs…Another concern is that it could be used by a wide range of agencies to confirm the identity of any Australian with government-approved documentation (such as a passport or driver's license), regardless of whether they are suspected of a crime.'
https://theconversation.com/why-the-governments-proposed-facial-recognition-database-is-causing-such-alarm-125811
This last apprehension Dr Moulds voices relates to the difference between a system which searches for a particular individual suspected of significant wrongdoing and one which conducts searches with far less obvious justification. The concern Dr Moulds raises is that because a system can be used it will be with the potential for ever-greater intrusions into people's lives.
The Law Council of Australia has stated that there is a need to 'limit the use of [facial identification technology] to the detection, investigation or prosecution of offences that carry a maximum penalty of not less than three years' imprisonment.'
https://www.lawcouncil.asn.au/docs/3ceb93a3-3de6-e911-9400-005056be13b5/3692%20-%20Review%20of%20the%20IMS%20Bill%20and%20Passports%20Bill.pdf
The Law Council of Australia has also stated, 'To ensure that there are more clearly defined limits on the legitimate and proportionate use of identity-matching services proposed in the IMS Bill, as well as greater oversight and transparency, the Law Council recommends that the [Bills] be amended to introduce…safeguards for when [facial recognition] is accessed by local government and non-government organisations [and that] notice…be given to individuals about the collection and use of their identifying information.'
The Council has also noted that there is currently no provision for 'mandatory training of empowered individuals within local government or non-government organisation about permitted uses.' https://www.lawcouncil.asn.au/docs/3ceb93a3-3de6-e911-9400-005056be13b5/3692%20-%20Review%20of%20the%20IMS%20Bill%20and%20Passports%20Bill.pdf

2. The Bills undermine civil liberties, especially the right to privacy
There has been concern expressed that these Bills and the systems they would allow represent a substantial risk to the liberties of Australian citizens.
The Australian Human Rights Commission stated in its most recent submission to the federal Parliament, 'The Commission continues to hold serious concerns that the Bill would impinge on a number of human rights…Rights that are particularly likely to be limited are the right to privacy, freedom of movement, the right to non-discrimination, and the right to a fair trial, though this is not an exhaustive list.' https://which-50.com/human-rights-groups-sound-alarm-on-governments-facial-recognition-laws/
Arthur Moses SC, president of the Law Council of Australia, has stated, 'Misuse of this technology would undermine the rights of individuals, as well as the community's trust in the

system and its operation.' https://www.afr.com/politics/federal/facial-recognition-bill-knocked-back-20191024-p533s6

Angus Murray, junior vice-president of the Queensland Council of Civil Liberties (QCCL), has stated, 'The question for society is whether this is technology we can or should be using. It's a slippery slope to a place that's probably irretrievable if we end up with technology like this around all the cities of Australia. We may decide this isn't the way we want to go – the concept of privacy and freedom of association disappears fairly rapidly.' https://www.afr.com/technology/your-face-is-about-to-end-your-privacy-how-do-you-feel-about-that-20190130-h1anyy

Human Rights Commissioner, Edward Santow, has claimed that the two proposed bills are 'unprecedented' in their impact on Australians' privacy. He notes that the Department of Foreign Affairs and Trade anticipates processing thousands of identity-matching requests a day if the bills are passed – compared to a few hundred per year currently. https://www.afr.com/technology/your-face-is-about-to-end-your-privacy-how-do-you-feel-about-that-20190130-h1anyy

The Australian Privacy Foundation has argued the proposal is highly invasive, because the system could be integrated into a number of other systems that collect facial data, including closed-circuit television. A spokesperson for the Foundation has stated, 'We are on our way to automated and real-time surveillance of public spaces.' https://www.theguardian.com/technology/2019/sep/29/plan-for-massive-facial-recognition-database-sparks-privacy-concerns

The position put by the Australian Privacy Foundation has been elaborated by Professor Toby Walsh, a Fellow of the Australian Academy of Science and an Artificial Intelligence expert, who has observed, 'The widespread use of facial recognition is going to change the nature of our society. It changes the world we're in. It's this idea that you can be watched anytime. Even if no one is watching you, even if you never come to any harm, that [still] changes what you do because you don't have the privacy to question.' https://which-50.com/cover-story-australias-dangerous-foray-into-facial-recognition/

The apprehension appears to be that when people know themselves potentially to be under constant observation their freedom of action is diminished. They are no longer able to behave spontaneously or unselfconsciously as they consider themselves the object of ongoing judgement, even for their innocent or innocuous behaviour.

Professor Walsh has further stated, 'We're used to the idea that there are loads of CCTV cameras around. But that was before we had face recognition. In the past we knew no one was looking, there were too many cameras for people to be looking at … [CCTV] actually wasn't invading our privacy. And now we can just upgrade those cameras with software that will be invading our privacy. It will be able to identify people in real-time. It will be able to track you in real-time.' https://which-50.com/cover-story-australias-dangerous-foray-into-facial-recognition/

Similar concerns have been expressed by Christie Hill, Deputy Advocacy Director, American Civil Liberties' Union, San Diego, about the negative potential of facial recognition technology for individual's privacy. Hill has stated, 'We're living in an age when machines can collect information about nearly everything we do — from the places we go to the emotions we feel to the people we hang out with — and have the capability to transmit this data to each other and to our government.

When nearly any device can be turned into a hyper-powerful surveillance tool, it's up to us to ensure technology makes us more, not less, safe.' https://www.sandiegouniontribune.com/opinion/story/2019-09-06/facial-recognition-tool-civil-liberties

Privacy apprehensions regarding the use of facial recognition are widespread in numerous jurisdictions, including in the United States. An October 2018 survey in the United States conducted by the Brookings Institution found 42 percent of people thought facial recognition was an invasion of privacy, against 28 percent who disagreed – and 30 per cent who were unsure. https://www.afr.com/technology/your-face-is-about-to-end-your-privacy-how-do-you-feel-about-that-20190130-h1anyy

3. The technology is not failsafe

Opponents of the widespread use of facial recognition technology in Australia and overseas argue that it is not foolproof and that when errors are made the consequences can be dire for the individuals involved.

On August 29, 2019, Forbes published an article by Naveen Joshi, the founder and chief executive officer of Allerin, an engineering and technology solutions company. Joshi stated, 'No technology is 100 percent accurate and efficient; we all know that. And facial recognition tech is no different. There could be chances of this technology making false claims, which can then lead to undesirable consequences.'
https://www.forbes.com/sites/cognitiveworld/2019/08/29/the-implementation-of-facial-recognition-can-be-risky-heres-why/#1b5b17d77863

Joshi cites the recent case of Ousmane Bah who sued Apple for $1 billion for wrongfully accusing him of the theft of $1,200 worth of merchandise from an Apple store in Boston based on mistaken facial recognition identification. The potential for more damaging misidentifications has been stressed. Jay Stanley, a policy analyst at the American Civil Liberties Union, has stated, 'One false match can lead to missed flights, lengthy interrogations, watch list placements, tense police encounters, false arrests or worse.'
https://www.chicagotribune.com/consumer-reviews/sns-facial-recognition-bias-20191226-cldfnnmqbzf6lp5w622jnw7oga-story.html

Critics are concerned that misidentification via facial recognition technology could result in the death of an individual who has been inaccurately matched by the technology and whom law enforcers therefore mistakenly believed to be a dangerous criminal. It has been suggested that this is a particular risk given that racial minorities, who already attract a disproportionate amount of police attention, appear to pose a problem for programmers attempting to delineate their features algometrically with enough precision. Several studies have revealed that Artificial intelligence (AI) systems such as facial recognition tools rely on machine-learning algorithms that are 'trained' on sample datasets. If darker skinned groups within a given populations are underrepresented in benchmark datasets, then the facial recognition system will be less successful in identifying black faces. https://www.abc.net.au/news/2020-02-04/fact-check-facial-recognition-darker-skin/11781192

On December 29, 2019, The Chicago Tribune published an article explaining the potential for error when using facial recognition technology. The article cited a recently released report from the United States National Institute of Standards and Technology which observed 'The majority of commercial facial-recognition systems exhibit bias.' Among a database of photographs used by law enforcement agencies in the United States, the highest error rates came in identifying Native Americans. The Institute observed that the identification systems falsely identified African American and Asian faces 10 times to 100 times more than Caucasian faces. https://www.chicagotribune.com/consumer-reviews/sns-facial-recognition-bias-20191226-cldfnnmqbzf6lp5w622jnw7oga-story.html

Accuracy concerns have been raised regarding the technology to be expanded under the Morrison government's proposed legislation. Australian Human Rights Commissioner Edward Santow has stated, 'Errors are not evenly distributed across the community. So, in particular, if you happen to have darker skin, that facial recognition technology is much,

much less accurate. When you use that technology in an area where the stakes are high, like in policing or law enforcement, the risks are very significant.'
https://www.abc.net.au/news/2020-02-04/fact-check-facial-recognition-darker-skin/11781192
An ABC fact check published on February 14, 2020, noted 'Three leading software systems correctly identified white men 99 per cent of the time, but the darker the skin, the more often the technology failed.
Darker-skinned women were the most misidentified group, with an error rate of nearly 35 per cent in one test, according to…research…conducted by Joy Buolamwini, a computer scientist at the Massachusetts Institute of Technology's (MIT) Media Lab.'
https://www.abc.net.au/news/2020-02-04/fact-check-facial-recognition-darker-skin/11781192

4. The Bills allow for electronic surveillance without enough oversight of the process and those who request it
Critics of the two bills seeking expanded use of facial recognition technology in Australia are concerned that there are insufficient provisions to oversee how the technology is being used, allowing for misapplications that might never be detected. They object that access to databases can be obtained without an adequate review process and that there is no mechanism for checking that the surveillance and data access powers that the legislation would give government and some corporate bodies is being appropriately applied. Liberal MP Andrew Hastie, the chair of the bipartisan parliamentary joint committee on intelligence and security which scrutinised the two bills, warned the legislation lacked 'robust safeguards' and 'appropriate oversight mechanisms.' In making this statement the committee was echoing the views of a wide range of legal authorities and civil rights bodies.
https://www.thesaturdaypaper.com.au/news/law-crime/2019/10/26/duttons-plan-surveillance-state/15720084008972?cb=1585819622
The Law Council of Australia has stated, 'To assure that uses are reliably and verifiably legitimate and proportionate, controls and safeguards are reasonably required…it is critical to ensure that the legislation which enables the use of this type of technology does not permit a creep toward broad social surveillance in Australia.'
https://www.lawcouncil.asn.au/docs/3ceb93a3-3de6-e911-9400-005056be13b5/3692%20-%20Review%20of%20the%20IMS%20Bill%20and%20Passports%20Bill.pdf
The Law Council of Australia has further noted, 'The proposed limits on the number of images presented for matching to a participating authority does not in practice limit the number of images requested to those numbers because multiple requests may be made by a participating authority around the putatively matched image.'
https://www.lawcouncil.asn.au/docs/3ceb93a3-3de6-e911-9400-005056be13b5/3692%20-%20Review%20of%20the%20IMS%20Bill%20and%20Passports%20Bill.pdf
As proposed under the Passport Amendment Bill 'computer programs could automate the sharing of passport-related information without human oversight with the potential to negatively affect the individuals concerned. https://www.afr.com/politics/federal/mass-surveillance-the-facial-recognition-bill-explained-20191029-p5358t
Ben Seo writing for the Australian Financial Review in an article published on October 31, 2019, stated, 'Sceptics saw plenty of reasons for concern in the proposed laws because they…did not require warrants, and contained automated decision-making.'
https://www.afr.com/politics/federal/mass-surveillance-the-facial-recognition-bill-explained-20191029-p5358t
The bipartisan parliamentary joint committee on intelligence and security which scrutinised the two bills in October 2019 noted this lack of oversight and accountability. The committee argued enforcement agencies should be required to obtain a warrant before accessing certain facial recognition services. The committee was also concerned that where decision making

was automated, as is outlined in some of the provisions of the legislation there is no scope for within agency oversight even at the time a decision is being taken. The committee recommended that the bill be changed to ensure that automated decision-making can only be used for decisions that 'produce favourable or neutral outcomes for the subject'. This provision is intended to ensure that individuals cannot be harmed by surveillance and data matching operations undertaken without human oversight.
https://www.afr.com/politics/federal/mass-surveillance-the-facial-recognition-bill-explained-20191029-p5358t
The committee further claimed that the manner in which the bills have been drafted is neither sufficiently explicit nor transparent for citizens to be properly informed of the impact that the legislation, if passed in its current form would have on their lives. The committee's report concluded, 'A citizen should be able to read a piece of legislation and know what that legislation authorises and what rights and responsibilities the citizen has in relation to that legislation. This is especially important in the case of the IMS bill which has the potential to affect the majority of the Australian population…
It is clear that the Identity-matching Service Bill does not inform the citizen reader in this way.' https://www.afr.com/politics/federal/mass-surveillance-the-facial-recognition-bill-explained-20191029-p5358t

5. An expansion of facial recognition technologies is not proportionate
Critics claim that the proposed legislation is an example of government and administrative over-reach seeking powers that are not necessary to address the problems offered as their justification. Critics further argue that most of these problems are already being tackled by other laws and enforcement practices.
The Law Council of Australia has expressed these concerns arguing that aspects of the Identity-Matching Services (IMS) Bill involve infringements on the right to privacy that are not justified by the supposed benefits to be gained. The Council has stated, 'As currently drafted, the IMS Bill will allow state and territory agencies to share and seek to match facial images and other biographical information for persons suspected of involvement in minor offences. The Law Council considers that this may not be a necessary or proportionate response.' https://www.lawcouncil.asn.au/docs/3ceb93a3-3de6-e911-9400-005056be13b5/3692%20-%20Review%20of%20the%20IMS%20Bill%20and%20Passports%20Bill.pdf
The Allens Hub for Technology, Law and Innovation, publicly launched on 14 March 2018, is an independent community of scholars based at University of New South Wales, Sydney. This group of academics has also argued that the proposed legislation is not proportionate, that is, that it is not required to address the problems in regard to which it has been proposed. The group has stated, 'The proposed system and legislation should be proportionate. This requires a demonstration that the legislation is reasonably necessary in pursuit of a legitimate objective and that its impact on fundamental individual rights are proportionate to this objective… [The]indiscriminate retention of biometric data of all people, with the broad ability to access and match images for any offences could be considered equally disproportionate.' https://www.allenshub.unsw.edu.au/sites/default/files/inline-files/Allens%20Hub%20Review%20Identity%20Matching%20Services%20Submission%202019%20for%20KB%20web%20upload.pdf
Looking particularly at the issue of protections against Australian nationals suspected to be terrorists who seek to return to Australia, critics of the proposed new laws argue that they are disproportionate as the country already has ample legislation in place for this purpose. In an opinion piece published in the University of New South Wales Newsroom, Sangeetha Pillai, Senior Research Associate at the University's Law School, argued, 'The government hasn't

explained why Australia's extensive suite of existing anti-terrorism mechanisms doesn't already adequately protect against threats posed by Australians returning from conflict zones.' https://newsroom.unsw.edu.au/news/business-law/there%E2%80%99s-no-clear-need-peter-dutton%E2%80%99s-new-bill-excluding-citizens-australia
Pillau went on to explain, 'Australia's 75 pieces of legislation provide for criminal penalties, civil alternatives to prosecution, expanded police and intelligence powers, and citizenship revocation. And they protect Australia from the risks posed by returning foreign fighters in a variety of ways.
For example, a person who returns to Australia as a known member of a terrorist organisation can be charged with an offence punishable by up to 10 years' imprisonment. Where the person has done more – such as fight, resource or train with the organisation – penalties of up to 25 years each apply.' https://newsroom.unsw.edu.au/news/business-law/there%E2%80%99s-no-clear-need-peter-dutton%E2%80%99s-new-bill-excluding-citizens-australia
Pillau also argued that Australia already has a more than adequate capacity to protect citizens from suspected terrorists against whom there is insufficient evidence to bring charges. She explains, 'A control order may be imposed on a person in cases where they are deemed a risk but there is not enough evidence to prosecute. This restricts the person's actions through measures such as curfews and monitoring requirements.
Evidence shows the existing measures work effectively. Police and intelligence agencies have successfully disrupted a significant number of terror plots using existing laws…' https://newsroom.unsw.edu.au/news/business-law/there%E2%80%99s-no-clear-need-peter-dutton%E2%80%99s-new-bill-excluding-citizens-australia

Further implications

The coronavirus epidemic has prompted a recess of parliament and a focus on emergency provisions to deal with the health and economic exigencies it has caused. In this context it will be some significant time before the Morrison government amends and resubmits to the parliament its Identity-matching Services Bill and the Passports Amendment Bill.
When these Bills are resubmitted, it is difficult to predict the reception they will receive. They would allow a more extended use of facial recognition technology which is already being used in other parts of the world to help regulate the movement of people and so control the coronavirus. This might lead to their meeting a more favourable reception from the parliament than they have up to this point.
It is also possible that the community may be less sensitive about limitations being placed upon its freedoms for the common good. These have been a feature of the manner in which the federal and state governments have attempted to restrict population movement and so contain the spread of the disease. The result has, however, been severe restrictions on commonly accepted civil liberties. https://www.abc.net.au/news/2020-04-03/coronavirus-emergency-laws-and-civil-liberties/12114042
These have generally been accepted with minimal complaint. As Michelle Grattan wrote in an article published in The Conversation on April 2, 2020, 'In the main the clamps are working without creating outrage.' https://theconversation.com/grattan-on-friday-imagine-if-we-could-extract-a-permanent-vaccine-against-hyper-partisanship-from-covid-19-135450
Grattan has also noted that the crisis also seems to have generated an unusually high level of trust in the actions governments have taken so far. An Essential poll registered 56 percent trust in the federal government. Though this may in part come from early favourable signs in the battle to control the virus and popular support for the large level of financial assistance the government has made available, it also indicates that the population has largely accepted the restrictions imposed on its liberties. https://theconversation.com/grattan-on-friday-

imagine-if-we-could-extract-a-permanent-vaccine-against-hyper-partisanship-from-covid-19-135450
It os almost impossible to predict the future of this proposed legislation in the post-coronavirus world. If the government is not ultimately judged to have handled the virus well, then it will not survive politically. If it is seen as having dealt with the crisis as well as could be expected, then it will have a huge amount of political capital to spend and its proposed legislation is likely to be accepted by both the parliament and the Australian people.
Either way, the advance of this technology is likely to continue even without formal regulation. Government and privately controlled databases are growing exponentially. Already drivers' licence photographs and other data have been added to the federal governments vast biometric databases after an agreement was reached with the state and territory governments in January 2018 giving federal authorities access to this data. https://www.abc.net.au/news/2018-01-15/alarm-raised-as-drivers-licences-added-to-government-database/9015484 Much of the proposed legislation does little more than formalise arrangements that already exist.
Michelle Grattan has argued that 'When this is over, there must be a clear end to…incursions into civil liberties.' https://theconversation.com/grattan-on-friday-imagine-if-we-could-extract-a-permanent-vaccine-against-hyper-partisanship-from-covid-19-135450 With regard to facial recognition technologies and the way in which they are used, much of the populace may not even be aware that its civil liberties have been infringed.