The Australia Institute
Research that matters.
Centre for Responsible Technology

Government’s forced rollout of facial recognition for home quarantine needs strict limits and protections

Discussion Paper

Jordan Guiao
Research Fellow, Centre for Responsible Technology

September 2021

About The Australia Institute

The Australia Institute is an independent public policy think tank based in Canberra. It is funded by donations from philanthropic trusts and individuals and commissioned research. We barrack for ideas, not political parties or candidates. Since its launch in 1994, the Institute has carried out highly influential research on a broad range of economic, social and environmental issues.

About the Centre for Responsible Technology

The Australia Institute established the Centre for Responsible Technology to give people greater influence over the way technology is rapidly changing our world. The Centre will collaborate with academics, activists, civil society and businesses to shape policy and practice around network technology by raising public awareness about the broader impacts and implications of data-driven change and advocating policies that promote the common good.

Our philosophy

As we begin the 21st century, new dilemmas confront our society and our planet. Unprecedented levels of consumption co-exist with extreme poverty. Through new technology we are more connected than we have ever been, yet civic engagement is declining. Environmental neglect continues despite heightened ecological awareness. A better balance is urgently needed.

The Australia Institute's directors, staff and supporters represent a broad range of views and priorities. What unites us is a belief that through a combination of research and creativity we can promote new solutions and ways of thinking.

Our purpose – 'Research that matters'

The Institute publishes research that contributes to a more just, sustainable and peaceful society. Our goal is to gather, interpret and communicate evidence in order to both diagnose the problems we face and propose new solutions to tackle them.

The Institute is wholly independent and not affiliated with any other organisation. Donations to its Research Fund are tax deductible for the donor. Anyone wishing to donate can do so via the website at https://www.tai.org.au or by calling the Institute on 02 6130 0530. Our secure and user-friendly website allows donors to make either one-off or regular monthly donations and we encourage everyone who can to donate in this way as it assists our research in the most significant manner.

Level 1, Endeavour House, 1 Franklin St
Canberra, ACT 2601
Tel: (02) 61300530
Email: mail@tai.org.au
Website: www.tai.org.au
ISSN: 1836-9014

Summary

As states around Australia plan for life after lockdown, home quarantine is being hailed as a potentially significant part of our pandemic management infrastructure.

In order for home quarantine to work, governments need the ability to monitor individuals and prove that they are complying with the quarantine.

The South Australian and Western Australian governments have used a combination of facial recognition and global positioning system (GPS) technology to police these individuals. NSW and Victoria have also announced trials using the same technology.

Facial recognition is of particular concern, with the technology proving to have systemic weaknesses and limitations, including errors in identifying female faces and people of colour, and risks of privacy and ethical abuses.

The Australia Institute's Centre for Responsible Technology does not support the use of facial recognition technology for home quarantine and general pandemic monitoring.

If governments insist on using this technology, we call on them to develop strict limits and protections for its use. We recommend that, at a minimum, the following be developed as part of the rollout of facial recognition technology:

1) **Constrain facial recognition to a single use with strict limits** - for home quarantine purposes and nothing else, using only 'one-to-one' verification, with data expiry on image captures and proper consent obtained from the public.

2) **Update State privacy legislation** in line with the federal Privacy Act which lists facial recognition and biometric information as sensitive information requiring privacy protections.

3) **Develop strong human rights protections in law** to guard against misuse of facial recognition and biometric technology, regulating future uses of facial recognition technology.

4) **Establish an Artificial Intelligence ethics advisory group** of academics, civil society and industry to properly scrutinise the effects and implications of biometric technology like facial recognition given the increased interest in and use of this technology.

Introduction

Facial recognition software uses image capture devices like a smartphone camera to analyse an image and create a faceprint – a biometric marker used to identify and verify an individual's identity.

The South Australian government's home quarantine app trial using facial recognition is the latest proposal in the tricky balance Australia must navigate between managing the effects of the COVID-19 pandemic with the help of technology, and this same technology increasing incursions into the public's privacy and individual rights.[1]

A similar app has been already been used in Western Australia.[2] The NSW government has also announced trial of a similar app[3] and the Victorian government has also followed suit.[4] The South Australian app is intended to be the national model to be copied once trials are deemed successful.

All the apps being trialled use geolocation and facial recognition software to track and identify individuals subject to home quarantine. The app prompts verification at random moments, and users are required to prove that they are at home using their devices using the facial recognition feature (as shown in Figure 1).

The South Australian app allows up to 15 minutes to use facial recognition to verify their identity,[5] while the Western Australian app only allows 5 minutes.[6]

GPS is then used to verify those people/their devices are within their listed residences.

[1] Doherty (2021), *Controversial facial recognition technology could be the key to opening Australia's borders,* https://www.sbs.com.au/news/controversial-facial-recognition-technology-could-be-the-key-to-opening-australia-s-borders/5451e07c-47c4-41bd-a9b1-4a48b8e8aefc

[2] Ferguson (2021), *WA's Covid-19 home quarantine system 'waterright' and ready: police*, https://www.theaustralian.com.au/nation/politics/was-covid19-home-quarantine-system-watertight-and-ready-police/news-story/17444569dd6d104d6bad1a14f7c9d9a0

[3] NSW Government (2021), *NSW to run home quarantine pilot program,* https://www.nsw.gov.au/media-releases/nsw-to-run-home-quarantine-pilot-program

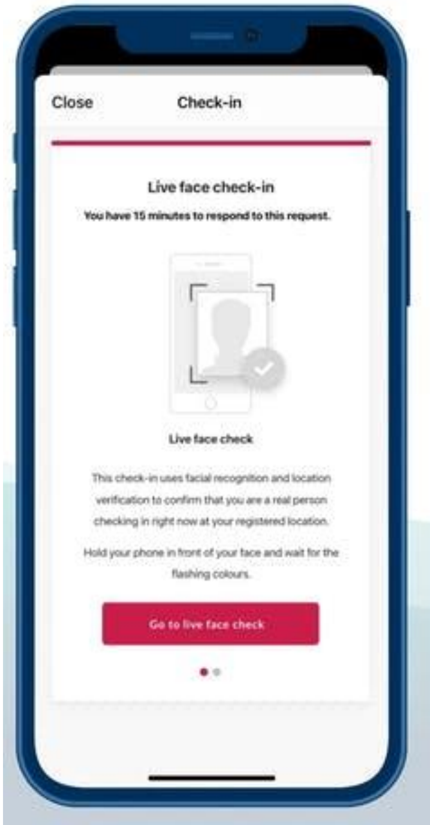
[4] SBS News (2021), Victoria to trial home quarantine app as 867 new local COVID-19 cases recorded

[5] Garcia & McClaren (2021), *How will South Austraila's home quarantine trial work?* https://www.abc.net.au/news/2021-08-23/how-will-south-australias-home-quarantine-trial-work/100398878

[6] WA government, *COVID-19 coronavirus: G2G Now frequently asked questions,* https://www.wa.gov.au/organisation/department-of-the-premier-and-cabinet/covid-19-coronavirus-g2g-now-frequently-asked-questions

The South Australian app is currently voluntary, while the Western Australian app is already mandatory for arrivals from high risk areas.

Figure 1: Screenshot of the South Australian home quarantine app using facial recognition software to identify users.



Live face check-in

You have 15 minutes to respond to this request.

Live face check

This check-in uses facial recognition and location verification to confirm that you are a real person checking in right now at your registered location.

Hold your phone in front of your face and wait for the flashing colours.

The main reason provided for the app's use is to ease the requirement for providing hotel quarantine and to give people the option to quarantine at home instead. The facial recognition and GPS elements assist with compliance and monitoring.

However, facial recognition technology is riddled with issues and privacy challenges, and has known technical errors and limitations.

The increasing use of surveillance technology for compliance and monitoring is a troubling trend, and there are cases globally of it being abused. The normalisation of surveillance culture is also concerning given its potential for human rights abuses and overreach by authorities.

Issues with facial recognition

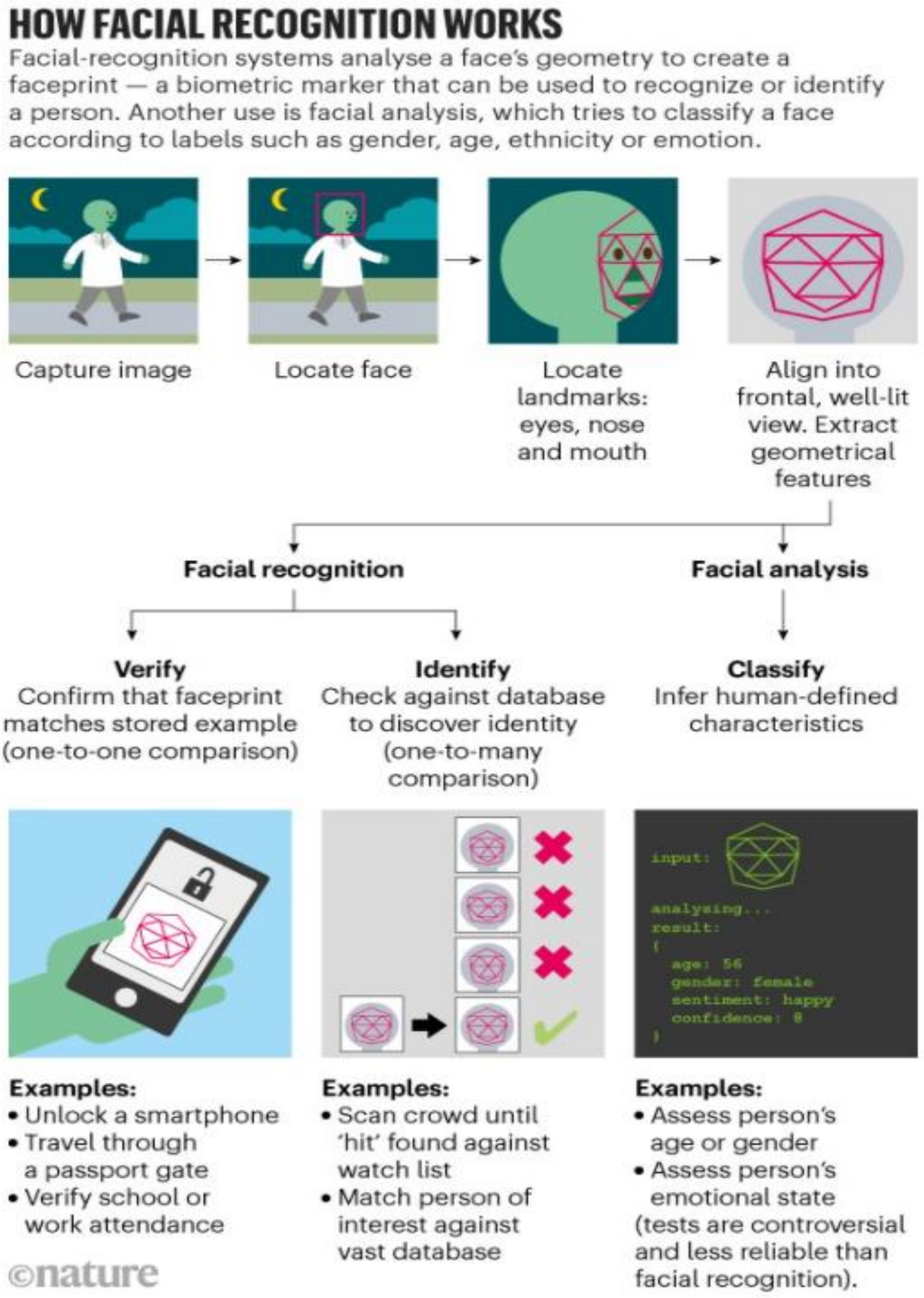
Black Boxes

One of the main issues with facial recognition technology is that they are often proprietary and provided by private companies. The Western Australian app was developed by Perth-based software company GenVis. The South Australian app was originally being built by GenVis also, but following performance issues this was discontinued and the app will be built by the South Australian government's digital team instead.[7]

Regardless, the technology is not transparent and issues with quality control or errors have not been made public. Facial recognition generally involves a multi-step process as outlined below.

Figure 2: How Facial Recognition Works from the Nature Journal

[7] Hendry (2021) *SA govt trials home quarantine app with facial recognition, GPS tracking,* https://www.itnews.com.au/news/sa-govt-trials-home-quarantine-app-with-facial-recognition-gps-tracking-568979



HOW FACIAL RECOGNITION WORKS

Facial-recognition systems analyse a face's geometry to create a faceprint — a biometric marker that can be used to recognize or identify a person. Another use is facial analysis, which tries to classify a face according to labels such as gender, age, ethnicity or emotion.

Capture image
Locate face
Locate landmarks: eyes, nose and mouth
Align into frontal, well-lit view. Extract geometrical features
Facial recognition
Facial analysis

Verify
Confirm that faceprint matches stored example (one-to-one comparison)

Identify
Check against database to discover identity (one-to-many comparison)

Classify
Infer human-defined characteristics

```
input:

analysing...
result:
{
  age: 56
  gender: female
  sentiment: happy
  confidence: 8
}
```

Examples:
- Unlock a smartphone
- Travel through a passport gate
- Verify school or work attendance

Examples:
- Scan crowd until 'hit' found against watch list
- Match person of interest against vast database

Examples:
- Assess person's age or gender
- Assess person's emotional state

(tests are controversial and less reliable than facial recognition).

©nature

Given the sensitivity around the technology, there needs to be more transparency around its build, features and performance. Neither the Western Australian or South Australian governments have provided any details on their apps' technical capabilities.

Government's forced rollout of facial recognition for home quarantine needs strict limits and protections

‘One-to-one’ vs. ‘one-to-many’

There are two main ways that facial recognition technology is deployed: ‘one-to-one’ and ‘one-to-many’.

One-to-one recognition checks an image against a single, respective image to determine if they are the same person. This method is similar to using a password or key to prove one’s identity. For example, many smartphones have a feature where a user can unlock their phone just by looking at it. The phone checks whether the person who’s trying to unlock the phone matches a photo on file (usually one taken for this purpose).

One-to-many recognition checks an image against many images in a database containing many images of other people. An example is when Facebook tries to predict who should be tagged in a photo by comparing faces to other photos Facebook has on file. These databases can be very large repositories and therefore are much more subject to errors.

While one-to-one recognition has become very accurate, one-to-many recognition often results in false positives and misidentification. When used for law enforcement and individual profiling, it has resulted in innocent people being marked as suspicious, arrested or even wrongfully prosecuted.[8]

Given the risks of misidentification from one-to-many verification, one-to-one verification is the only appropriate method of facial recognition for home quarantine.

Bias against women and minorities

There is clear evidence of facial recognition technology having biases against women and people of colour.[9] The United Nations-backed treaty committee CERD (Convention on the Elimination of All Forms of Racial Discrimination 1966) concluded that:

> The accuracy of facial recognition technology may differ depending on colour, ethnicity, or gender of the persons assessed, which may lead to discrimination.[10]

This is in large part due to facial recognition datasets being trained using primarily white and male faces, creating more accurate readings from those type of faces.[11] Numerous groups

[8] Castelvecchi (2021), *Is facial recognition too biased to be let loose?* https://www.nature.com/articles/d41586-020-03186-4

[9] Ibid.

[10] UN Committee on the Elimination of Racial Discrimination (2020), *General Recommendation No. 36, Preventing and Combating Racial Profiling by Law Enforcement Officials*

[11] Australian Human Rights Comission (2021), *Human Rights and Technology Final Report*

have called for suspension of this technology because of these flaws, including the Australian Human Rights Commission.[12]

Even the largest technology companies like Microsoft and Amazon have recognised flaws in their facial recognition technology and paused sales of these products for a time. Commercial digital platforms have tried to improve the technology so far failed to eliminate these persistent and systemic flaws.[13]

Not only do minorities face potential discrimination using this technology, they can also be subject to more deliberate and harmful targeting.

In 2020 it was revealed that Chinese telecommunications giant Huawei developed facial recognition technology to monitor and track China's ethnic Uighur population. Uighurs are an ethnic minority group of Muslims that have faced ongoing persecution by the Chinese government. Using facial recognition software through Huawei, Uighurs were able to be identified, targeted, and have their information sent on to Chinese authorities.[14]

The known and unresolved issues with bias in facial recognition as well as the potential for real abuses and injustices in its use should not be overlooked.

Privacy and Trust

Existing pandemic software has already been responsible for privacy abuses and breaches of community trust, with the Western Australian, Queensland and Victorian police using QR check-in data to progress unrelated crimes.[15]

GPS and geolocation software has proven to be easy to hack and manipulate.[16]

Vaccination passports are another example of pandemic technology potentially rife with privacy abuses.[17]

[12] Australian Human Rights Comission (2021), *Human Rights and Technology Final Report*

[13] Wiggers (2021), *Bias persists in face detection systems from Amazon, Microsoft, and Google,* https://venturebeat.com/2021/09/03/bias-persists-in-face-detection-systems-from-amazon-microsoft-and-google/

[14] Fernando (2020), *Advances in facial recognition technology could amplify the persecution of minorities, AI experts warn,* https://www.sbs.com.au/news/advances-in-facial-recognition-technology-could-amplify-the-persecution-of-minorities-ai-experts-warn/da16ed2b-daa4-4b04-80c7-89b730388f1b

[15] Grubb (2021), *Privacy tsar wants police blocked from COVID check-in app data,* https://www.innovationaus.com/privacy-tsar-wants-police-blocked-from-covid-check-in-app-data/

[16] Fisher (2021), *How to fake a GPS location on your phone,* https://www.lifewire.com/fake-gps-location-4165524

[17] Guiao (2021), *Please Check-In: A blueprint for a safe, fair and ethical vaccination 'passport',* https://d3n8a8pro7vhmx.cloudfront.net/theausinstitute/pages/3117/attachments/original/1630984184/P1145_Blueprint_for_a_safe_and_ethical_vaccination_passport.pdf?1630984184

Because facial recognition uses biometric information, the complexity and risks are even greater.

Given governments have failed to prevent privacy abuses in simpler pandemic-related technologies, they need to be more vigilant if they adopt facial recognition software.

Normalisation of Surveillance

Use of facial recognition and biometrics is concerning because it normalises surveillance culture.

While making home quarantine safe and compliant is a worthy goal, it is unclear whether governments trialling this technology have thought through the full implications and potential issues of facial recognition technology.

The most prominent case study for successful use of facial recognition to combat the pandemic comes from China, which should be taken with a grain of salt given the country's history of privacy abuses.[18]

The question should be asked of whether this surveillance focused technology is the best way to support Australians through the pandemic, or if there were other less intrusive ways that could have been developed, such as a federally-funded national quarantine system, and a faster, more effective rollout of vaccinations.

[18] Yuan (2020), *How China is using AI and big data to fight the coronavirus,* https://www.aljazeera.com/news/2020/3/1/how-china-is-using-ai-and-big-data-to-fight-the-coronavirus

Conclusion

Facial recognition software is the latest in Australia’s technological arsenal in its attempt to get the pandemic under control. However, privacy and human rights abuses have been found in other pandemic-related software already. Facial recognition, which is vastly more complex should be properly scrutinised and safeguards should be put in place to protect Australians from any abuses if the technology is to be rolled out nationally.