JUTA
POPIA PORTAL

ISSUE NO 10 • PUBLIC CCTV SURVEILLANCE AND POPIA • NOVEMBER 2022

PUBLIC CCTV SURVEILLANCE AND POPIA – HOW DO THESE TWO WORK TOGETHER?

1. OVERVIEW

Governments' surveillance of their citizens has seen a massive uptick in recent years (especially with Covid-19). There is an extreme example of mass public surveillance in China. However, many police departments in other countries, such as the US, the UK, Canada, and the EU, have all come under fire for using CCTV cameras in public spaces to monitor crime and other security concerns (such as terrorism). With the various privacy concerns around the use of CCTV surveillance (e.g. the use of facial recognition technology, bias, profiling and general privacy infringement) and POPIA coming into effect – the question remains: how do you use CCTV to monitor the public in compliance with POPIA?

Photo: Rich Smith Unsplash


Photo: iStock

2. HOW IS CCTV USED FOR PUBLIC SURVEILLANCE GLOBALLY?

The extremity ranges from country to country, of course. For example, in cities across the US, Canada, the UK and the EU, many police departments have deployed CCTV cameras and monitored the public on these from centralised police command stations or 'real time crime centres'. The CCTV cameras provide a live feed actively monitored by police, enabling them to respond to crime and security threats 'in real time'. Using licence plate readers and the more controversial facial recognition technology can also come into play. China seems to have taken this to the extreme. For example, according to a report by the *New York Times*, Chinese law enforcement has reportedly requested to install CCTV cameras equipped with facial recognition technology inside private spaces, like residential buildings, karaoke lounges and hotels. The same *New York Times* report also details how these facial recognition CCTV cameras feed footage into 'powerful analytical software that can tell someone's race, gender and whether they are wearing glasses or masks'. Many of these facial recognition CCTV cameras are also starting to be equipped with recording capabilities for around a 300-foot radius. This is so that a person's 'voice pr int' can also be captured and added to Chinese law enforcement's profile of that person.

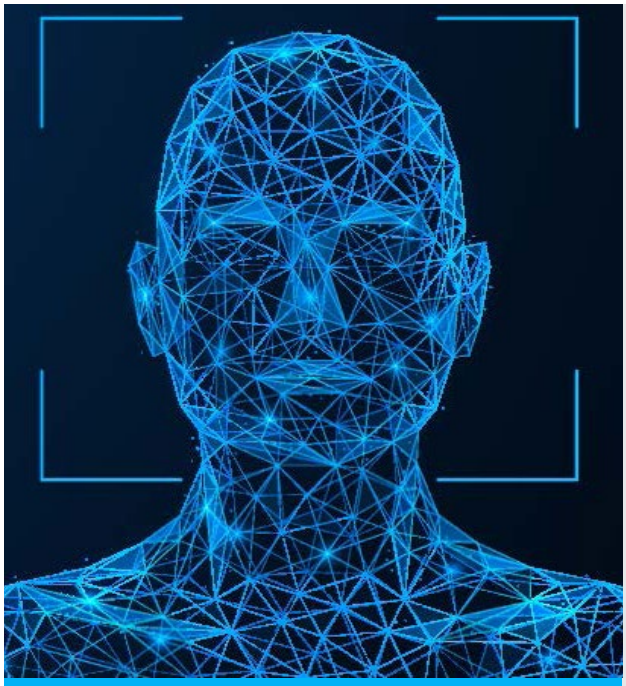

Photo: iStock

3. WHAT IS HAPPENING IN SOUTH AFRICA?

In South Africa has not been immune to these trends. For example, over the past several years, a private company called Vumacam have been rolling out CCTV cameras across urban centres such as Johannesburg and Durban. These CCTV cameras are fibre-connected to Vumacam's data centre. For a monthly fee, private security companies and government law enforcement agencies can access live video streaming from the CCTV cameras they choose. While Vumacam's street CCTV cameras are not enabled with facial recognition technology, they are enabled with features such as licence plate recognition services.

Vumacam's CCTV cameras have been the subject of criticism from privacy advocates locally and abroad, and even the subject of a 2020 High Court case against the Johannesburg Roads Agency('the JRA'). Vumacam maintain that their service is POPIA compliant, and you can read their CCTV POPIA Policy here.

Recent South African developments in the facial recognition technology space include some reports that a local security company is using a platform called 'Scarface' to do this. Scarface is a platform which links high-resolution cameras to technology which uses Artificial Intelligence ('AI') algorithms to identify 'persons of interest' by scanning images against a database. It has been used, for example, to combat illegal mining.

The Department of Home Affairs (DHA) is also updating its national population register system. The current system includes only fingerprints and photographs of all South Africans with a national ID. The DHA plans for the update to eventually include more biometric data points such as 'iris recognition technique, facial recognition and palm print'. In 2020, the DHA released their draft Official Identity Management Policy for public comment. One of the major criticisms against this draft policy has been that it proposes linking CCTV surveillance footage equipped with facial recognition technology to the national population register system in one single interface. SAPS will be allowed access to all this information in a single interface for crimefighting purposes.

4. SO, HOW DOES THIS WORK UNDER POPIA?

For public bodies using CCTV cameras (with or without facial recognition technology), they can choose to rely on section 11(1)(*e*) of POPIA as their legal basis ('processing is necessary for the proper performance of a public law duty by a public body'). Depending on the context, POPIA may not even apply to a wide range of scenarios because POPIA does not apply to processing done by a public body:

Photo: iStock

'which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or

the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information.'

It is important to note that facial recognition technology has been a subject of much legal debate in Europe for several years. In May 2022, the European Data Protection Board (the EU's information regulator) called for a ban on the use of facial recognition technology in certain contexts.

Private bodies like shopping centres or sectional title schemes, for example, who use CCTV to monitor the public or common areas, can choose to rely on section 11(1)(*f*) of POPIA (legitimate interest).

5. FURTHER READING

You can read more about mass public surveillance and the associated privacy issues in Chapter 15. You can read more about exemptions to POPIA's application in Chapter 3 and the legal justifications for processing personal information under POPIA in Chapter 6.

juta