COVID-19 IN SOUTH AFRICA: THE INCREASED SURVEILLANCE, COLLECTION AND STORAGE OF PERSONAL INFORMATION BY THE PUBLIC AND PRIVATE SECTORS

C19 Analysis Sub-Group

July 2021

CONTENTS

INTRODUCTION

We live in an era of Big Data, where vast amounts of information is produced at staggering speeds, thanks to ever-increasing computer processing power, expanding data storage capacity, and high-speed internet. Much of this information is personal. It includes people's names, identity numbers, contact details, addresses, employment information, medical records, consumer behaviour, web browsing habits, religious beliefs, sexual orientation, social media activity, and images of themselves, their loved ones and their possessions. With this onslaught of information, new technologies have developed, creating fresh opportunities for both commercial and government surveillance, and the mass collection, storage and processing of personal data.

Also courtesy of our digital world, is the vast amount of location data generated about our everyday activities by the phones, computers, websites and applications we use to communicate, interact, socialise, and work. Added to that, are the ever-proliferating networks of high-definition internet-based surveillance cameras in public spaces, capable of generating petabytes of quality footage that can be analysed to reveal the activities of millions of citizens in granular detail.

It is within this surveillance landscape that the Covid-19 pandemic has raged across the globe, bringing with it new applications and opportunities for manufacturers of surveillance technology. Globally, both governments and the private sector have been eager to explore and exploit this new technology. New developments range from facial recognition applications that can detect when social distancing regulations are broken, to digital vaccine passports that could spell segregation for many who are unwilling or unable to be vaccinated. This has brought with it new ethical issues compounding the complex moral dilemmas that were already plaguing the surveillance and data privacy landscape long before the pandemic.

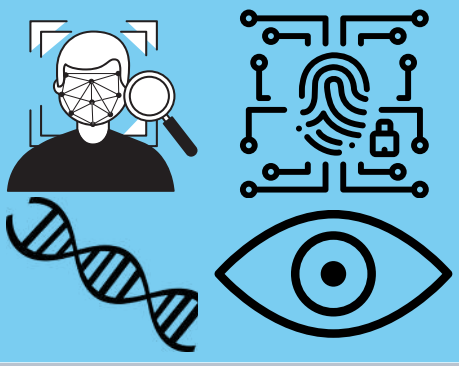
This brief guide takes a look at some of the most prominent surveillance technologies available today, and how Covid-19 has impacted their use. We discuss facial recognition technology, licence plate recognition cameras, mobile phone data and tracking, social media monitoring, and Covid-19 vaccine passports. For each technology, a brief overview of its workings and purpose is provided, as well as its uses globally and in South Africa. The impact of Covid-19 on the use of the technology is discussed, as well as the current human rights and legal context within which the technology functions. Following this, recommendations for further actions are made.

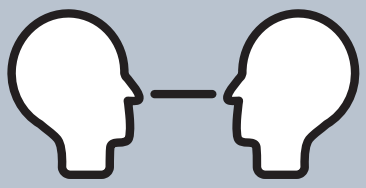
We hope that this guide will provide you with an accessible, convenient look at some of the most widespread surveillance and personal data analysis methods available, as well as the legal vacuum that exists for many of these technologies both globally and in South Africa.

FACIAL RECOGNITION TECHNOLOGY

WHAT IS IT?

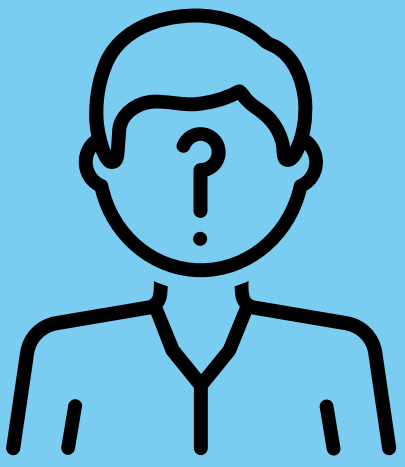
Your face is a biological trait that uniquely identifies you. It's a biometric, just like fingerprints, DNA, irises, palm prints, and even the way you walk. Facial recognition technology (FRT) includes a range of software products that measure facial features for various purposes. These include verification and identification, emotion recognition, and many more.



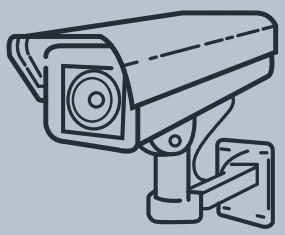


Facial recognition technology can be used to verify if a person is who they claim to be. For instance, when a traveller passes through customs, a camera can be used to scan their face, and facial recognition software can compare this new image to the ID photo in their passport. If there is a match between the two, the person's identity is verified. Because a new facial photo is compared to the ID photo, this is known as a one-to-one comparison.

Facial recognition technology can also be used to identify an unknown individual. Globally, police are increasingly using this software. A facial photograph of an unknown person can be compared to an indefinite number of known people (like mugshots in a criminal database, or ID photos of citizens in a population register). If there is a match, it links the identity in the database to the photo of the unknown person. Since one image is compared to a number of images, this is also known as a one-to-many comparison. This is similar to how police use fingerprints found at a crime scene to search for unknown suspects against a database of known criminals' fingerprints.



One-to-many facial recognition can also be applied to footage or images of an uncooperative subject (in other words, a person who is not voluntarily facing a camera to have their photo taken). This use of facial recognition is especially suited to situations where surveillance cameras film public spaces where persons move about freely. These can include public transport (like trains and roadways), schools, and office buildings. This presents a new opportunity for authorities to track people's movements, since public video surveillance systems are proliferating and, unlike fingerprints, one's face is on public display.



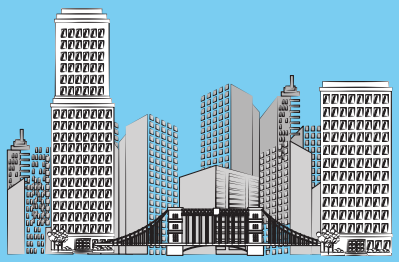
FACIAL RECOGNITION TECHNOLOGY

GLOBAL USE

By 2020, the global market value of the facial recognition industry was estimated at USD 3.8 billion. Facial recognition is used in policing, airports, banks, places of employment, retail, smartphone security, and many more. The global market is expected to reach a value of USD 8.5 billion by 2025. Government agencies are the main drivers behind this growth.

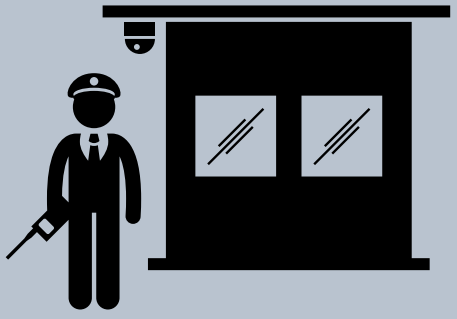
USE IN SOUTH AFRICA

The national Department of Home Affairs (DHA) is currently developing an Automatic Biometric Identification System (ABIS) that will allow for both identification and verification through the use of fingerprints, facial recognition, and other biometrics like palm prints, iris scans, and even DNA. The South African Police Service will be able to use ABIS to conduct one-to-many identification searches for criminal suspects with both fingerprints and facial images. In this scenario, a mugshot of a wanted person could be compared to ID photos of all South Africans in order to identity a suspect. This effectively puts the faces of all citizens in a criminal database.



Facial recognition technology looks set to be adopted for use with surveillance cameras in public spaces. By November 2020, 6% of the 2 345 cameras in the City of Cape Town's surveillance network were equipped with facial recognition. Other municipalities have also been planning to use facial recognition with their street surveillance cameras. These include the Johannesburg Metropolitan Police Department and Ekurhuleni Municipality. The eThekwini Municipality announced in December 2019 that some of their city's 432 cameras were equipped with facial recognition, although the city did not specify a number.

In Johannesburg, a private security company called Vumacam had rolled out over 5 000 surveillance cameras in public streets by June 2021. Private security companies patrolling a certain area pay a monthly fee to access the feed from Vumacam's cameras in that area. The security company must have a monitoring room to which Vumacam then sends the video feed. The system is internet-based, and Vumacam's cameras are connected via the fibre network. It is possible to use facial recognition software with Vumacam's cameras. Private security companies can choose whether or not they will use FRT. Currently, there is no law prohibiting this, and it is not known if any of these security companies are using FRT.

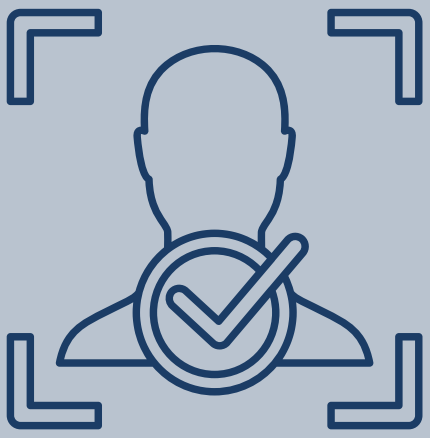


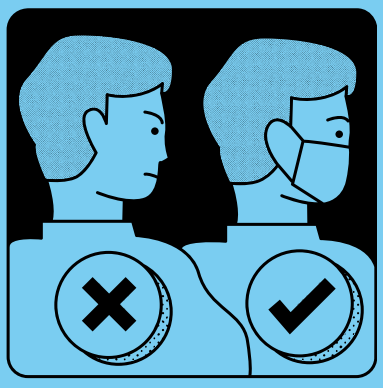
FACIAL RECOGNITION TECHNOLOGY

COVID-19 IMPACT

COVID-19 is thought to be a major contributor to the projected growth of the global facial recognition market, since FRT provides a number of uses to curb the spread of the pandemic.

Facial recognition allows for so-called touchless verification of identity. Technology allowing people to avoid physical contact of potentially contaminated surfaces are projected to see an increase in demand. Using FRT at places of employment or residential estates to verify identity means that people will not have to provide a fingerprint, swipe a keycard, or key in a pin code, all of which may require physical contact with a communal surface. Scientists have been quick to adapt facial recognition algorithms that can identify an individual even when they are wearing a mask.





No mask, no entry.

Facial recognition technology can be employed in a public space to detect if someone is wearing a mask. Face detection analysis (an algorithm that simply detects the presence of a face in an image, without necessarily identifying the person) is also being used to detect when too many people are gathered within a certain space, or if people are too close together. If the camera detects this, it can send an alert to authorities or venue managers that social distancing protocols are not being adhered to.

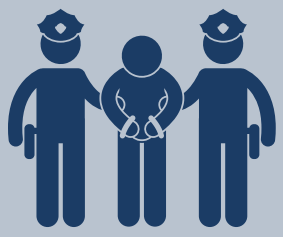
Facial recognition has been employed to enforce quarantine measures and COVID-19 safety protocols. In Russia, authorities have reportedly used facial recognition to identify persons who leave the home and fail to self-isolate. Chinese authorities have used the technology in the same manner, and have also used it to identify persons not wearing masks.Thus far, South African authorities are not using facial recognition technology to monitor COVID-19 safety protocol adherence. This could change, as there is a global drive by facial recognition vendors to profit by selling the technology to governments in order to enforce adherence to COVID-19 restrictions. Vumacam, the country's biggest private surveillance company, is already envisioning the use of analytical software to enforce mask detection and social distancing.

FACIAL RECOGNITION TECHNOLOGY

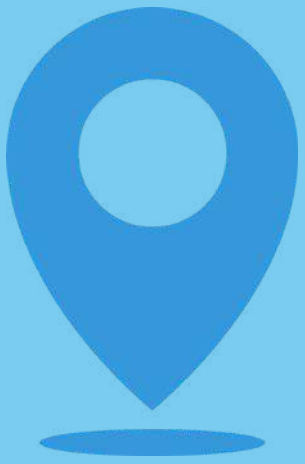
HUMAN RIGHTS AND THE LAW

Facial recognition is increasingly meeting with opposition in democratic countries. A common problem is that facial recognition algorithms are less accurate when identifying persons of colour and females. FRT has mostly been developed by white males, and works best on white male faces. Objective studies have found that demographic traits impact the accuracy of the majority of FRT software programmes.

This bias and inaccuracy poses a problem for both identification and verification. If a person is falsely identified as a criminal, they could land in jail with a criminal record. If a person's identity verification fails, they can be denied access to, for instance, the workplace or ports of entry.



Another aspect of facial recognition that advocacy groups have warned against, is the potential for identifying and tracking individuals in public spaces (such as roads, sidewalks and public transport). Because one's face is on public display, and because public space surveillance is becoming so widespread, facial recognition has introduced a new opportunity for authorities to track people as they go about their daily business. Given the improvements in facial recognition driven by COVID-19, it could become even more difficult for people to escape such tracking. This could have a chilling effect on people's privacy, freedom of movement and association, and right to protest.



In South Africa, the Criminal Procedures Act of 1977 has been amended to allow the police to do searches for suspects against databases of fingerprint and facial photographs of any and all government bodies. This includes the national population register. Alarmingly, the Department of Home Affairs' draft identity management policy makes provision for authorities to search biometrics contained in the Automatic Biometric Identification System without a court order. There are no specific, legally binding regulations in place to govern the identification of individuals through the use of public space surveillance cameras coupled with facial recognition software. We also do not know if the Protection of Personal Information Act (POPIA) will protect us from FRT, since safety is often held up as a justification for invading privacy. If the current status quo is allowed to continue, both state and private agencies could potentially develop the ability to track people's movements with facial recognition.

LICENCE PLATE RECOGNITION TECHNOLOGY

WHAT IS IT?

Licence plate recognition (LPR) software is utilised with surveillance cameras for both private and commercial purposes. It is used for billing purposes in parking lots, average speed enforcement, and traffic management. It allows a camera to scan and record all passing vehicles' registration numbers. For law enforcement, a licence plate scanned by an LPR camera can be checked against an existing database of suspicious vehicles. If there is a match, the system alerts police about the vehicle.

Licence plate recognition systems can also be used to map vehicle movements on a massive scale. LPR cameras are fixed in a single location, and each time a vehicle registration number is recorded, that image is time-stamped. This means that the time it was photographed is recorded electronically, and this record is unalterable. Special software can be used to analyse collections of millions of licence plate number scans taken over prolonged periods. Such software can accurately track the movements of vehicles as long as they remain within the coverage area of the camera network. This can be done in real-time as the vehicle is on the move, or movements can be mapped retrospectively.

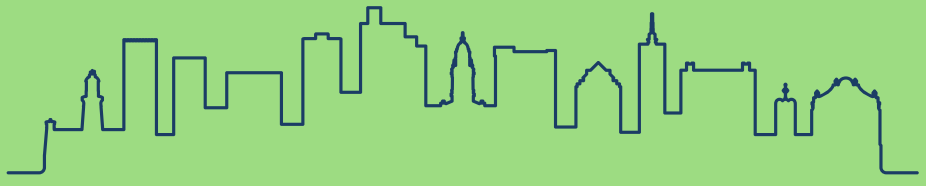
GLOBAL USE

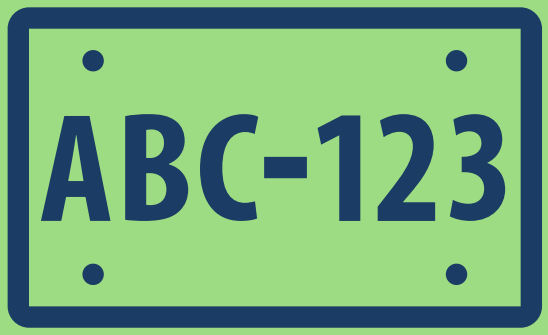
LPR is a relatively old technology, and has been in use since the 1970s. Globally, these systems are commonly used for law enforcement purposes on every major continent, particularly in major economies (including China, Japan, the United States, the United Kingdom, Australia, and Middle Eastern and European economies).

The industry is also growing in developing nations in Africa and South America. Estimates of the market size vary. By one estimate it is expected to grow to USD 3.8 billion by 2025. Major drivers for market growth include the increased adoption by governments for law enforcement purposes.

USE IN SOUTH AFRICA

Cape Town and Johannesburg have seen the biggest uptake of LPR technology in South Africa. By 2018 the City of Cape Town had just over 500 cameras with LPR capabilities monitoring major roads, intersections and freeways.





The Johannesburg metropolitan police department had 500 surveillance cameras in total by 2018. It is not known how many of these have licence plate recognition capabilities. Over the past five years, numerous reports have surfaced that the city's surveillance system is not fully functional. Other major municipalities like eThekwini and Mangaung have also started rolling out licence plate recognition systems.

LICENCE PLATE RECOGNITION TECHNOLOGY

USE IN SOUTH AFRICA

Most high-income neighbourhoods in Cape Town have privately funded and operated LPR camera systems, and control centres are located within neighbourhoods. Neighbourhood networks are connected to each other, and control rooms can share information and alerts about suspicious vehicles.

One company's roll-out of licence plate recognition cameras by far exceeds that undertaken by any other government and private entity. By June 2021, the private surveillance company Vumacam had an over 2000 licence plate recognition cameras in place throughout Johannesburg.This number is continuously increasing.

COVID-19 IMPACT

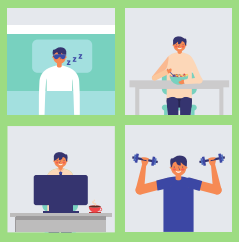
COVID-19 has generated new uses for LPR, particularly for enforcing COVID-19 self-isolation and quarantine measures. In the UK, police in the Devon and Cornwall used LPR to monitor whether residents were making unnecessary trips during the lockdown period. Police in India and Australia have also employed LPR to monitor movements of citizens and enforce lockdown measures. In China, the technology was used to track citizens and identify potential contact with the virus. Police then contacted drivers to order them to self-isolate.

Civil rights activists have warned that the increased use in LPR surveillance during the COVID-19 lockdown could endure well after the emergency measures introduced to curb the pandemic have been lifted.
In South Africa, LPR technology has not been used to monitor people's movements in order to enforce lockdown rules. The different LPR networks in the country are isolated from each other, and operated by a mix of government and private bodies. The lack of infrastructure and coordination has likely contributed to a decreased likelihood that LPR will be used to enforce Covid-19 regulations on a country-wide scale in the near future.

HUMAN RIGHTS AND THE LAW

Licence plate recognition has evolved into an accurate tracking mechanism. Yet even in countries where the use of LPR by law enforcement is well-established, legislation has lagged behind. In Britain, automatic LPR has been in use since 1997. But blanket LPR tracking was only ruled illegal in 2013. In the United States, only 16 states have laws expressly governing licence plate recognition use by police.

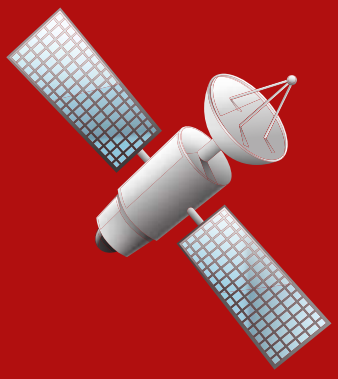
In South Africa, there are no laws governing LPR. Advocates for LPR argue that number plates are there to aid law enforcement, making the collection, storage and processing of licence plate numbers exempt from the Protection of Personal Information Act (POPIA). Thus, there's a danger that POPIA will fail to protect citizens from LPR technology.



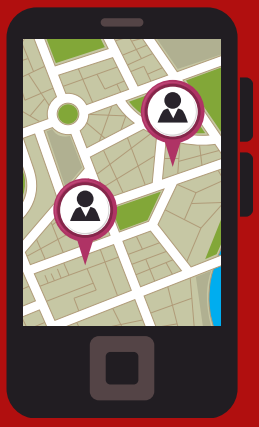
LPR poses a major threat to privacy, even if the cameras record movements in public places. Analytical software gives police and private entities access to other personal information: by tracking people's movements on public roads, it is possible to find out where a person works, lives, socialises, goes to church, and much more.

MOBILE PHONES AND LOCATION DATA

WHAT IS IT?



A smartphone can be used to track its owner in different ways. One method is through GPS. The Global Positioning System is a collection of satellites orbiting the earth and owned by the United States government. The GPS satellites emit radio waves that can be received by smartphones because they are equipped with GPS receiver chips. If a smartphone can receive the signals of at least 4 GPS satellites, it can calculate the phone's position to within 4 metres, although accuracy usually varies between 10 and 100 metres. GPS is less effective if obstructions like cloudy weather conditions or buildings come between satellites and the receiving smartphone.



Smartphones can also be tracked through location data generated by Wi-Fi network connection devices (such as a modem), since smartphones are also equipped with a Wi-Fi chip. The chip receives signals emitted by Wi-Fi connection devices. When a phone receives signals from a number of such devices, it can calculate its location based on the varying signal strengths of the different devices.

The more Wi-Fi access devices there are emitting signals, the more accurately a smartphone can calculate its position. This geolocation method works best in urban areas where there are typically an abundance of Wi-Fi access devices. It can determine location within a few feet.

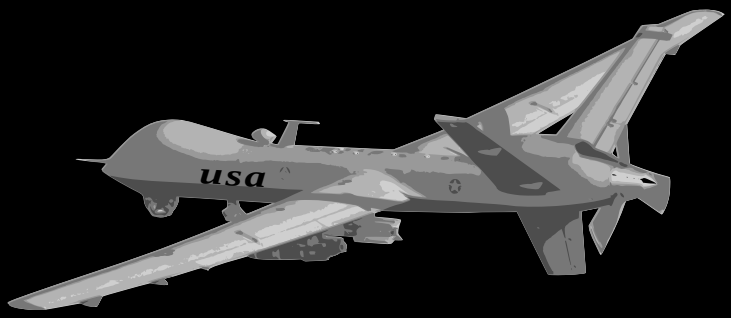
GLOBAL USE

GPS and Wi-Fi tracking are often used in conjunction by applications on smartpohones to determine position (E.g.: Ride-hailing apps, navigation apps (like Google Maps), delivery apps, and weather forecast apps). This data can also be used to track an individual's movements in detail. An app need not necessarily require a person's location information to function (such as a weather app), but a condition of its use may be to allow it access to the phone's location data. This data can in turn be sold to third party companies who may use it, for instance, to target the smartphone owner with advertisements based on the locations that they visited. Globally, marketers use location data to target consumers likely to be susceptible to their advertisements.

MOBILE PHONES AND LOCATION DATA

GLOBAL USE

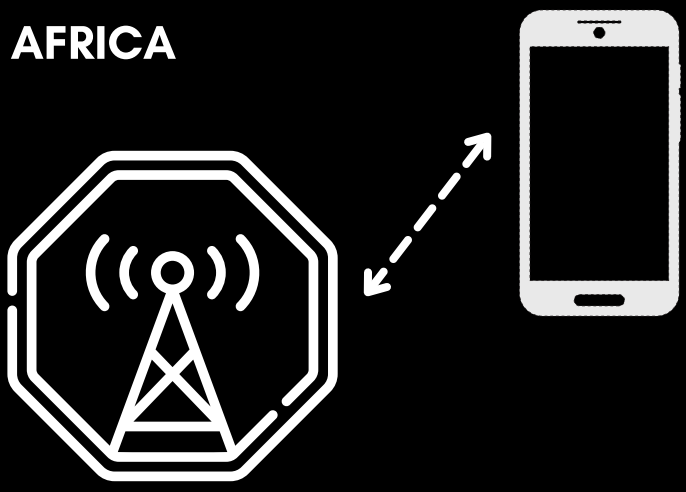
Although the use of the geolocation tracking is largely commercial, reports have surfaced of governments using location data generated by smartphone apps to track citizens. In November 2020 Vice news reported that the United States military was purchasing location data generated by a Muslim prayer app that had 98 million downloads. The location data from the app was being sold by private companies.



In March 2021, it emerged that the Iowa National Guard bought such app location data to assist it in conducting more precise drone strikes. Police in the United States have also made use of so-called geofencing warrants: the court can issue a warrant allowing police to request location data for all smartphones within a certain geographic area and timeframe. Google receives the majority of these requests.

USE IN SOUTH AFRICA

In the private sector, mobile phone tracking is commonly used for employers who want to keep tabs on workers out in the field. Applications are installed on the smartphones of employees. An employee could use the app to sign in or out of work, log lunch breaks, and indicate their location. GPS tracking apps for employees who frequently drive for work purposes can measure their speed and pinpoint their location. Such software can allow employers to keep track of workers in real-time. A primary aim of this software is to prevent workers from wasting time on the job, and in the case of field workers it provides the employer with proof that the worker did indeed visit work sites.



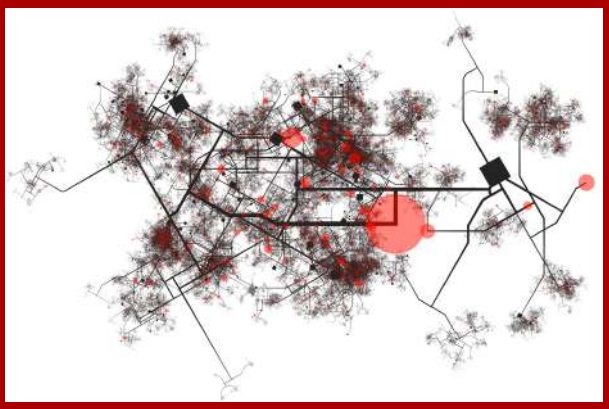
Police commonly use section 205 of the Criminal Procedures Act to compel cellular service providers to provide them with the location data generated when mobile phones connect to cell towers. This is known as tower data, and is typically contained in the billing records of a cell phone company's customer. When a mobile phone detects a signal from a nearby cell tower, that data is recorded. Based on the location of the tower, police can estimate a person's whereabouts. Upon receipt of a court order, a cellular service provider will have to hand over to police the location data of a phone (recorded over a specific and limited time period stipulated in the court order). This location data is, however, not as accurate in tracking individual movements as GPS and Wi-Fi geolocation.

MOBILE PHONES AND LOCATION DATA

COVID-19 IMPACT

Globally, countries have made use of smartphone location data in an attempt to curb the spread of Covid-19.

In South Korea, a tracking app that citizens installed on their smartphones sent data to a central database, which in turn created maps showing where persons infected with Covid-19 had been. People were then warned to avoid those places. In Taiwan, authorities used geolocation data generated by phones to alert police if people ordered to isolate at home left their homes during the isolation period. In Iran, the government notified the public to download an app on their smartphones that could assist them to perform a Covid-19 self-diagnosis by answering certain questions. The app also harvested personal information like names, birthdays, addresses, and people's location data.



In Israel, the government removed the warrant requirements for intelligence services to monitor people's movements through their phone location data. In Singapore, the government made the installation of their track-and-trace app mandatory for citizens who wanted to access venues such as shops and workplaces. It later emerged that the data had been made available to police for criminal investigations.

In the United States, the varying responses to track-and-trace app development from different states and and private technology companies led to a fractured approach that ultimately failed to stem the tide of the pandemic. The British government's first tracking app was scrapped after poor performance in a trial run. A second application was developed and launched in September 2020. It worked with Bluetooth technology, measuring the distance between phones that had the app installed on them, and calculating risk of infection between people. If someone was potentially exposed to the virus for long enough, the app would send an alert to tell the person to self-isolate. App use was voluntary, and it did not collect personal data such as names, addresses and locations.

South Africa also opted for a less invasive tracking app called CovidAlert (after initially announcing that it would use location data from mobile service providers to track infections). The app, which works with Bluetooth, sends users notification if they have been in close contact with other app users who have confirmed their Covid-19 diagnosis. If an app user is diagnosed with Covid-19, they can use the app to anonymously inform other app users. The app then issues advice to users who have potentially been exposed to the virus long enough to become infected on the steps they need to take to protect themselves, their families and community members. All of this is voluntary, and not controlled by authorities.

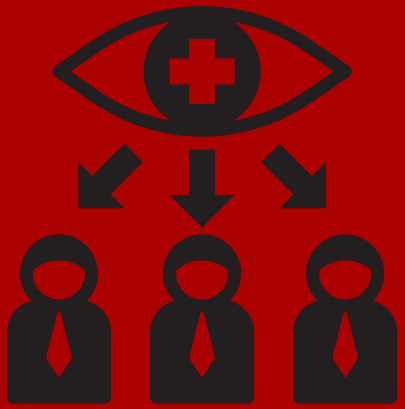
MOBILE PHONES AND LOCATION DATA

HUMAN RIGHTS AND THE LAW

In December 2019 the New York Times reported that they had been provided with the location data of over 12 million US citizens, amounting to over 50 billion location pings from their smartphones. The location showed a detailed picture of people's movements in US cities like New York, Washington, Los Angeles and San Francisco. The data was provided by an anonymous source from the private sector. The data did not originate from a telecom operator, technology company or government law enforcement agency. Instead, it was from a location data firm which collected information about people's movements through smartphone applications. This type of data collection is a global phenomenon and largely unregulated.

Once such data (which not only includes location data, but also other personal information like age, internet browsing habits, spending habits, and so forth) has been collected by the application, it can be sold to third parties or data brokers, who in turn resell it or use it to profile a smartphone user, predict behaviour, and target them with advertisements or other information (like political campaign advertisements). Smartphone users do not usually have a choice in whether or not this information is collected and resold. Usually, any data generated by smartphone apps, be it location or other data, can be legally sold to third parties, since the user of the app must agree to this before installing the app. That means that the third party can sell that data on to other customers, including the police. However, in April 2021, Apple was the first to announce that it would provide users with the option to refuse applications access to phone location data.

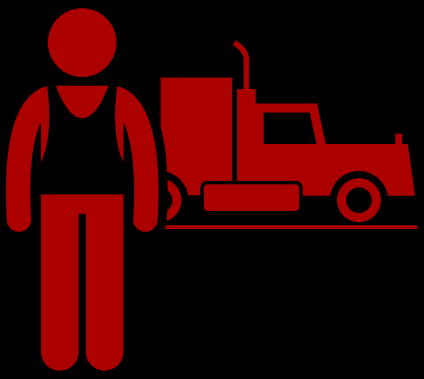
In countries where governments have employed invasive Covid-19 tracking apps using mobile phone location data, privacy advocates and researchers have been critical of the implications for individual privacy, warning that the surveillance may remain long after the pandemic has been brought under control.



MOBILE PHONES AND LOCATION DATA

HUMAN RIGHTS AND THE LAW

In South Africa, a specific privacy concern surrounds the tracking of employees through smartphone applications. The Protection of Personal Information Act (POPIA) compels employers to ensure that their collection, storage and analysis of location data logged by employees are in line with regulations, since location data is expressly mentioned as personal information in POPIA. Employers must, among other things, ensure that the data is secure, that employees have given permission to be tracked, and that measures are in place to stop other parties for using the data for anything other than the reason it was collected. Reasons for processing such data must also be sufficient.



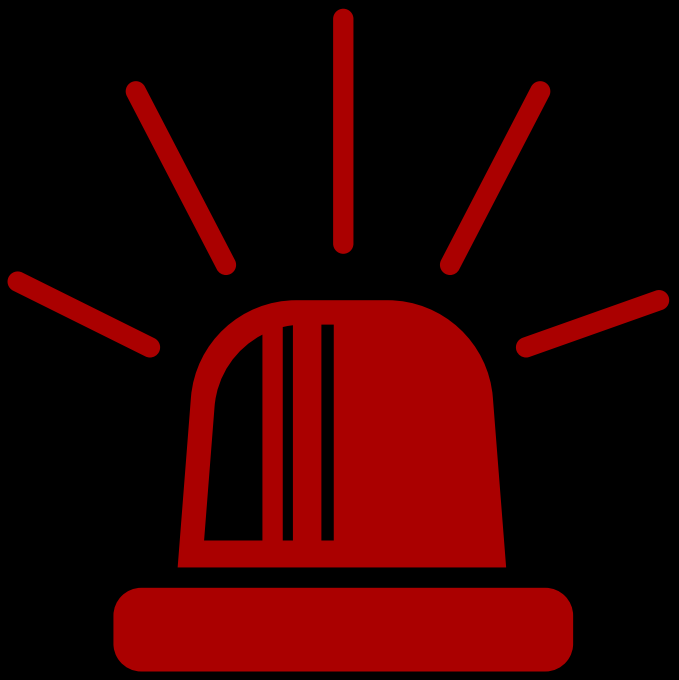
In terms of law enforcement, South African police appear to make minimal use of legal avenues that allow them to request location data from overseas companies who usually store application data. Although they can make use of a mutual legal assistance treaty to obtain such data from large organisations like Facebook or Google, this is a arduous process that requires the police to make its case to the South African National Prosecuting Authority and, following approval from the NPA, authorities in the United States. This approach seldom bears fruit. From July 2013 to December 2020, South African law enforcement agencies submitted 28 requests for information (not limited to location data) to Google, of which only four were granted.

However, there is no guarantee that South Africans will not be subjected to state surveillance through location data derived from mobile apps. It is not known if any South African government agencies have ever purchased, or planned to purchase, location data generated by smartphone apps. There is no law prohibiting this. Usually, any data generated by smartphone apps, be it location or other data, can be legally sold to third parties, since the user of the app must agree to this before installing the app. That means that the third party can sell that data on to other customers, including the police.

MOBILE PHONES AND LOCATION DATA

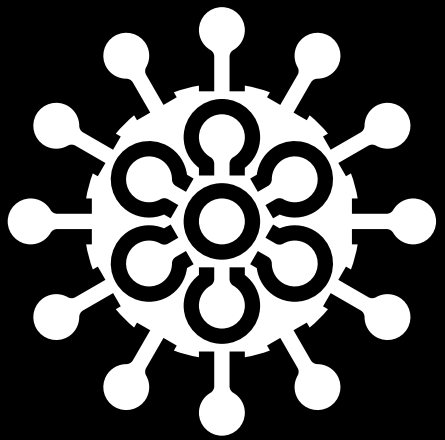
HUMAN RIGHTS AND THE LAW

Even if South African police do not use smartphone location data often, section 205 of the Criminal Procedures Act does give them access to a form of location data from people's personal mobile phones. Police frequently use this legislation to obtain cell phone records. In 2016, the Right2Know campaign obtained statistics from the four major mobile operators in South Africa showing that the courts ordered them to hand over the mobile billing information of more than 70 000 cell phone numbers per year. Included in these records, are the location of the cell phone towers to which the phones connect, the numbers they dialled, and the time and duration of the calls.



Location data obtained with a section 205 court order is less accurate than GPS or Wi-Fi tracking. However, police use software from IBM, known as i2 Analyst's Notebook, to analyse call records based on whom was dialled, how often, how long the conversations lasted, and where the caller and the callee were located. This gives police an accurate picture of the caller's movements and the people with whom they associate. Both smartphones and older cellular phones (that cannot connect to the internet) generate this data. Section 205 of the CPA is a well-established piece of legislation that has been tested in the Constitutional court. However, it is a method easily exploited by corrupt police who may want to obtain call data about innocent citizens.

Where Covid-19 is concerned, South Africans seem to have escaped government use of smartphone geolocation data to track potential exposures or the violation of quarantine and other preventative regulations. The CovidAlert app does not share personal information or location data with other app users or government authorities, and all personal data, including health data, is hidden from other users. Since it is based on Bluetooth technology, the app can register the proximity of other phones that have the app installed without connecting to any mobile networks. The government took great care to ensure that the app's functions adhere to the Protection of Personal Information Act, and state in the terms and conditions of the app that it cannot use GPS data to track phones, nor can the app be used by law enforcement to track individuals. It also cannot be used to access data, messages, or emails stored on the smartphone, nor for accessing people's identifying details and health information.



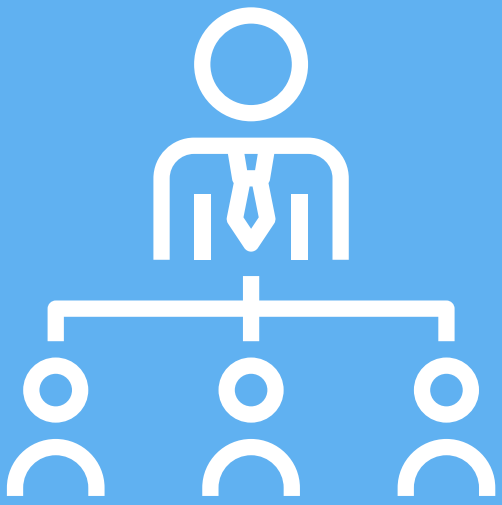
SOCIAL MEDIA MONITORING

WHAT IS IT?

Social media monitoring software is utilisedin to keep track of what people say and post on social media. It has commercial and law enforcement uses. The software allows the user to search for certain keywords across the web. In commerce, these words could relate to topics, specific products, brands, services, markets and so forth. Hashtag searches are also possible. Various platforms can be searched in this way, including Youtube, TikTok, Instagram, Facebook, and Twitter. Social media monitoring also covers websites, (such as news websites), discussion forums, and blogs – as long as the information is publicly available on the web.

GLOBAL USE

Social media monitoring is used globally for commercial purposes to assist marketers to gauge the attitudes, perceptions, sentiments and interest of customers or potential customers. Monitoring can be active, with keyword searches set up to listen out for specific brand names. It can also be passive, monitoring keywords showing people's general opinions and interests. This information can help marketers to find out what customers think about products and services, and if their advertising is reaching the intended target market.

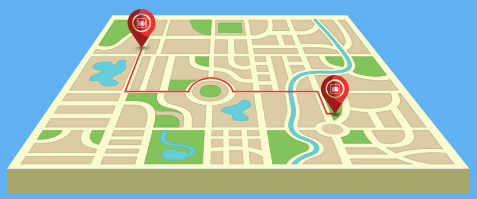


Another use for social media monitoring is found in the workplace. Employers are able to use the software to see what employees are saying through their private social media accounts. This practice is part of guarding against employees' social posts negatively impacting the company image. It also aims to ensure that workers do not lose productivity because of the time they spend on social media. In addition, it be used by companies to profile a potential employee, which would then assist in the decision to appoint that person.

SOCIAL MEDIA MONITORING

GLOBAL USE

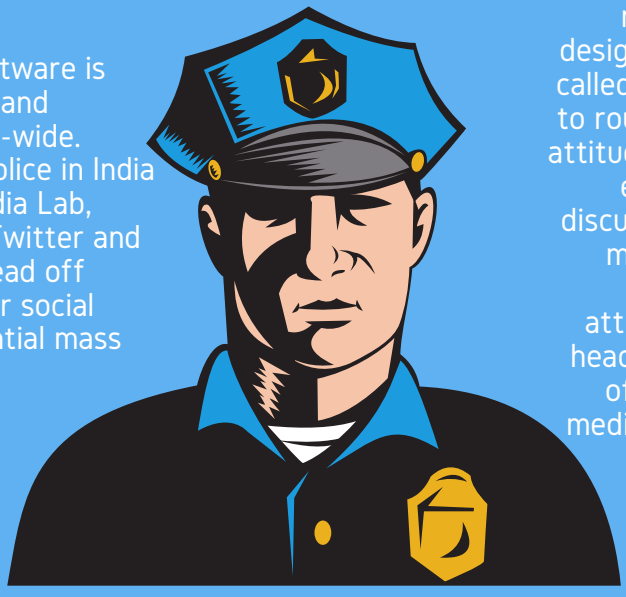
Social media monitoring software is utilised by law enforcement agencies to keep track of social media posts that may provide an indication of terror or criminal activities. The software allows law enforcement to monitor the public social media posts of citizens within a specific geographic area. Examples of social media platforms that can be monitored include Twitter, Facebook, Instagram, and Youtube.



Police can also use social media monitoring tools to identity suspicious individuals through their public social media posts. Police can use the software to, for example, receive alerts of any social media posts within a certain geographic area that mention keywords related to a protest that is in progress. The result is that people will land on the police's radar simply by mentioning these key words.

It is possible to monitor (in real-time) the posts of people taking part in a protest gathering by searching for posts made by people who are physically present at the gathering. This method uses GPS to demarcate the geographic area of interest, and is known as geofencing.

Social media monitoring software is utilised by both democratic and authoritarian regimes world-wide. For instance, the Mumbai police in India have a dedicated Social Media Lab, which monitors Facebook, Twitter and Google. The Lab aims to "head off unruly crowd sentiment over social media" and to predict potential mass gatherings.

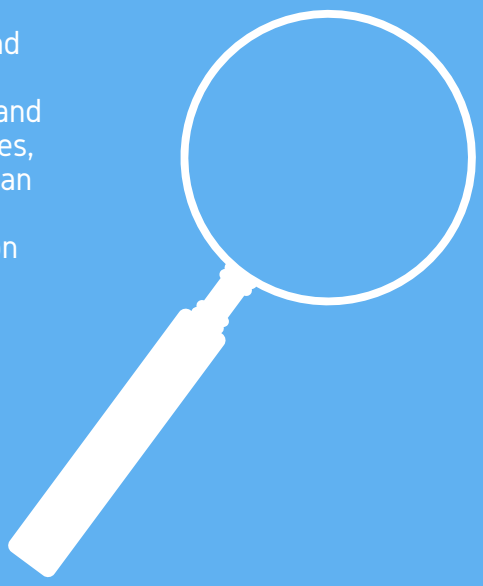


In the United States, a company by the name of OssaLabs offers software designed for law enforcement agencies called Social Impact Pro. It allows police to routinely harvest data on community attitudes and perception about local law enforcement and to monitor public discussions and conversations on social media. The software aims to "assist police to understand community attitudes before they become a news headline." Social Impact Pro is just one of many commercial software social media monitoring products available to police globally.

SOCIAL MEDIA MONITORING

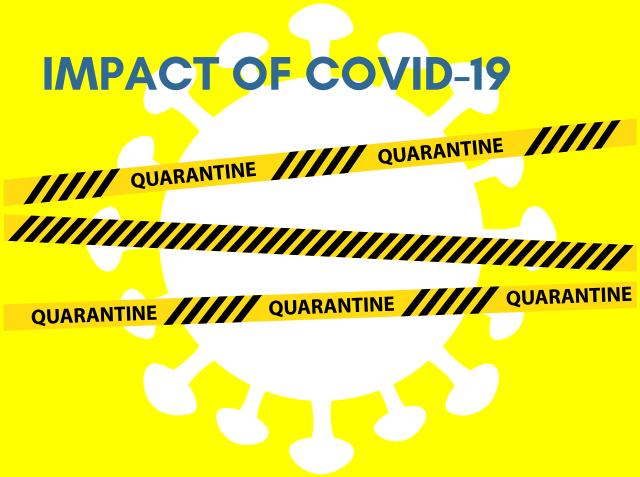
SOUTH AFRICA

Social media monitoring software is commercially available in South Africa, and there is nothing prohibiting government agencies or businesses from purchasing and utilising it. Alternately, government bodies, law enforcement, or private businesses can contract a private company to use the software to monitor social media posts on their behalf.



It is not known if police or intelligence services are currently using social media monitoring software to monitor protests or predict criminal activity. In 2016, SAPS obtained quotations for the purchase of monitoring software from a company by the name of RIPJAR. RIPJAR provides powerful web-based data analysis software, including social media monitoring software. However, it appears that SAPS has not been using the software, and that the eventual purchase of RIPJAR was fraudulent.

IMPACT OF COVID-19



Some countries have turned to social media monitoring to enforce Covid-19 regulations. In September 2020, Philippine police announced that they would monitor social media to ensure that people heeded quarantine regulations. In Italy, a research agency reportedly scraped more than 500 000 instagram profiles to see if people were adhering to lockdown rules. South African authorities have not utilised social media monitoring software to police adherence to Covid-19 restrictions.

HUMAN RIGHTS AND THE LAW

Social media monitoring software utilises sophisticated algorithms to collect an analyse personal data about individuals. The data is gathered from across various social networking platforms. This analysis provides authorities and private businesses with detailed insights into people's lives, including their relationships, emotions, beliefs, political leanings and future plans.

Advocacy groups warn that the invasive technology can be used to monitor protestors and target political leaders and influencers, as well as monitor people's movements in real-time. Since the technology primarily aims to predict unwanted behaviour, it necessarily monitors innocent people. Advocacy groups argue that the software threatens people's right to freedom of expression and association, and the right to privacy.

The same can be said of employers' use of social media monitoring to monitor workers' personal online conduct.

SOCIAL MEDIA MONITORING

HUMAN RIGHTS AND THE LAW

Social media monitoring software involves the collection and processing of personal data. Even if social media posts are made publicly available, those post still constitute the personal information of the user. That means that the processing of social media posts and conversations are still regulated by the Protection of Personal Information Act. Because the Act allows for data processing for security purposes, it is possible that police and intelligence services could utilise such software despite POPIA restrictions.

As is the case with geolocation data gathered by apps and sold to third parties, publicly available social media posts can potentially be sold legally to third parties. This is possible because anyone using a social media platform must consent to certain conditions before using the platform. These conditions include granting permission to have certain data and content from one's social media page shared with third parties. This information can again be sold on to police and intelligence agencies. In South Africa, there is little transparency as to the manner in which police and intelligence services utilise this type of commercially available software.

Proponents of social media monitoring maintain that they should be free to collect and analyse information posted on social media if those posts are made public. They say that once you choose to make your information public, you can no longer enjoy any sort of privacy protections. In South Africa, legal advisers are telling the public that their public social media posts are unlikely to be protected by the Protection of Personal Information Act, since they chose to disclose the information. This is a dangerous argument, because it fails to take into account the impact of Big Data analytics - including analytics used by police to monitor social media. Data privacy laws are also meant to protect us from Big Data analytics.

Big data refers to the phenomenon whereby information is produced in vast quantities, thanks largely to the Internet and the increased processing capacity of computers. Data comes in many different formats, including text, audio, images, video and the like. Analytics such as that used by social media monitoring software allow police or private companies to create a detailed picture of one's personal life very quickly, since the automated process can search for, aggregate, store, categorise and interpret data much faster than a human being. A collection of all publicly available data about someone provides a far more accurate picture of that person than any one piece of data on its own.

COVID-19 VACCINE PASSPORTS

WHAT IS IT?

A Covid-19 vaccine passport serves as proof that you have received your Covid-19 vaccine. It can be an an application on your smartphone with a unique code, or a hardcopy certificate, like a yellow-fever certificate. There is no globally accepted, standard format for a Covid-19 vaccine passport. The idea behind a vaccine passport, is to curb the spread of the coronavirus by restricting access to certain spaces on the basis of a person's vaccination status.

Air travel to certain countries have long required proof of vaccination against certain diseases. Similarly, proof of Covid-19 vaccination may become a requirement before one is allowed to enter certain countries. Another concept that has emerged, is the requirement of proof of vaccination to enter certain places within one's home country. These could include shops, restaurants, and workplaces.

GLOBAL USE

Although the World Health Organisation has said that Covid-19 vaccine passports should not be a requirement for international travel, some countries are making it a condition for entry. China already introduced such passports in March 2021. The European Union made Covid-19 vaccine passports available for all residents in July 2021. Known as the "Digital Green Certificate", it will be mandatory for persons travelling through EU countries. In June 2021 health ministers from the G7 countries agreed to support vaccine certificates that would be mutually acceptable to all nations, allowing for international travel to resume fully. In July 2021, Japan sought to have its Covid-19 vaccine passport accepted by 10 other countries.

Some parts of the world have voiced their opposition to vaccine passport requirements for international travel. At the 2021 G7 summit, India, attending as a guest country, said that vaccine passports will be detrimental to developing nations (where vaccination has been slower). In April 2021, the African Centre for Disease Control said such passports would only worsen existing global inequalities, and that they were not appropriate while poorer countries were lagging behind rich nations in vaccinating citizens.

The world over, countries have seen mixed reactions to the use of Covid-19 vaccine passports for movements within domestic borders. The United States provides a prime example of such varying responses. President Joseph Biden has ruled out the introduction of a national vaccine passport, thus making it a state-level decision. By July 2021, four states had made such passports available, but 20 states had banned them.

In March 2021, New York state introduced a digital vaccine passport which citizens must present if they want to attend an event for which admission numbers were limited due to Covid-19 restrictions. The app-based passport has to be shown in conjunction with the person's identity document before they can enter sport stadiums, wedding venues or the movie theatre, for instance. At the other extreme, the Governor of Oklahoma state banned government bodies from making vaccination a requirement to enter government buildings. Schools are also not permitted to deny a child entry if they have not been vaccinated.

COVID-19 VACCINE PASSPORTS

USE IN SOUTH AFRICA

The South African government has not yet announced plans to introduce Covid-19 vaccine passports for international travel or domestic use. The country is still in the early phases of its vaccination roll-out, and the process has been slowed by supply chain issues. As of July 2021, only 0.8% of the population (nearly half a million people) had been fully vaccinated. With the slow rate of vaccine administration, it is unclear when exactly vaccine passports will become feasible.

As elsewhere, privacy is a concern in South Africa. The Protection of Personal Information Act extends to people's private medical data. A Covid-19 vaccine passport commonly reveals one's name, address, identity number, your vaccination status, and if you weren't vaccinated, it could contain information about your recovery from a positive diagnosis. Digitised vaccine passports relying on smartphone apps may result in social exclusion for some. The Pew Research Center in the US estimated 8% of South Africans share a smartphone with another person, while 5% have no access to one. In rural South Africa, people are dependent on 2G and 3G mobile connections. That means that digitised app-based vaccine passports in rural areas could be impractical.

HUMAN RIGHTS AND THE LAW

Covid-19 vaccine passports are accompanied by a host of human rights concerns. Those against its use warn that it will exacerbate existing inequalities and perhaps lead to a two-tier society where those who are not vaccinated are excluded from certain social sectors and activities. There are a number of reasons why people may choose not to vaccinate. These may include lack of access to vaccines, underlying health conditions, mistrust of the medical community, and religious or ethical beliefs.

There are also major privacy concerns about vaccine passports. If they are digitised passports linked to a government database with information about citizens' vaccination status, a number of issues arise, including how long that data should be stored, how it will be secured from cyberattacks, and who can have legitimate access. Digital vaccine passports may, in some cases, also keep track of which venues were frequented by the passport holder, creating location data that also constitutes personal information.

CONCLUSIONS AND WAY FORWARD

Limitations of POPIA: Although the Protection of Personal Information Act (POPIA) came into effect on 1 July 2021, it remains to be seen to what extent this will impact the use of facial recognition technology, licence plate recognition technologyand social media monitoring by either the police or the private security sector. One of the conditions under which parties are exempt from restrictions in processing personal data, is if it is required for safety and security purposes. It is thus unclear if POPIA will have any impact on the use of these technologies by police and intelligence services. This is a particular concern in light of the argument levelled by the security sector that one cannot reasonably expect privacy when walking or driving in public areas, or when making a public social media post.

Big Data: The public must be made aware that in the era of Big Data and its accompanying analytics, thousands of data points about one individual can be collected, stored, analysed and distilled into an accurate profile of a person's life, beliefs, habits, health, activities, work and so forth. This is true even if those data points were scattered throughout the public domain. Privacy legislation must be used to protect people from the mass aggregation, storing processing and analysis of personal data that could reveal intimate details about their private lives. Civil society groups need to make the public aware that as technology changes, so should the definition of what can be viewed as a reasonable expectation of privacy.

Covid-19 regulations: There are nospecific regulations governing the use of surveillance cameras and facial recognition software, licence plate recognition technology, and social media monitoring to impose COVID-19 protocols. By December 2020, at least 17 000 individuals nationally have been arrested for not adhering to mask protocols in public and contravening social gathering regulations. People thus arrested have permanent criminal records. If police were to be equipped with FTR, LPR or social media monitoring software, this could aid them in implementing these regulations on a far wider scale. Advocates have warned that such surveillance can remain even after the Covid-19 pandemic is under control. Civil society will have to monitor the use of such surveillance methods and make the public aware of the potential dangers of the country slipping into permanent state of surveillance.

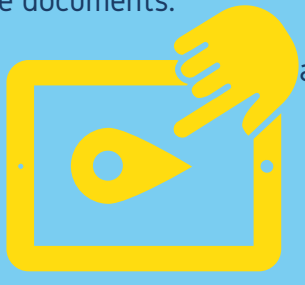
The Department of Home Affairs: The DHA's draft identity management policy allows for the use of facial recognition and other biometric searches without a warrant. The draft policy already makes some provision for this various forms of independent oversight bodies to manage the Automated Biometric Identification System and police searches of the system. However, it may be necessary for civil groups to pressure the DHA into establishing a truly independent oversight committee for ABIS. This is especially important since it is not known to what extent the Information Regulator (appointed in terms of the Protection of Personal Information Act) will regulate police use of ABIS, since this is a public safety function and could be exempt from the provisions of POPIA.

CONCLUSIONS AND WAY FORWARD

Advocating for stricter, targeted legislation to regulate licence plate recognition usage should be a focal point for privacy advocates in South Africa. This is necessary to prevent abuse of the system by private and public entities, and to create an independent entity where citizens can complain about suspected misuses by the police or private security services. At this stage, it is unclear if POPIA will provide an adequate framework for such regulation, since vehicle registration numbers are not mentioned explicitly as personal information in the Protection of Personal Information Act. Advocacy groups also need to investigate whether the blanket collection and storage of vehicle registration details of all South African citizens (irrespective of criminal status) are truly required and justified – be it for law enforcement or commercial purposes. It may be useful to advocate for shorter retention periods of registration details.

Section 205 of the Criminal Procedures Act: Civil society need to request more regular releases of statistics for police requests for call-related information and location data from mobile service providers. The first and last release of such statistics occurred in 2016 after substantive efforts from the R2K campaign. Police use this legislation extensively to gather extremely this data which can then be analysed with computer software to reveal even greater detail about a person's life. This is a process overseen by the lower courts and within police ranks. Other than this, there is no public accountability of what arguably constitutes the greatest part of the South African Police Service's surveillance efforts. Civil society needs to call for transparency in the process, as well as accountability reports showing how, if at all, callers' personal information actually assisted in criminal investigations.

Mobile phone location data and social media monitoring software: Further investigation is required into whether South African intelligence and law enforcement agencies use such technologies (either in-house, or via outsourcing). The public was only made aware of the planned purchase of the RIPJAR social media monitoring software because it emerged during a court case. Such purchases should be made public in the planning documents, financial statements, and annual reports of law enforcement agencies as well as the State Security Agency. If these bodies outsource these services, it should be noted in the same documents.



There should also be publicly available reports accounting for the degree to and manner in which these surveillance tools actually assisted law enforcement and intelligence services in carrying out their duties. Much of the information that is used in these two forms of surveillance can simply be purchased from private data brokers, meaning there is nothing protecting the public from police surveillance in the virtual landscape. Unless civil society intervenes, this will not change.

CONCLUSIONS AND WAY FORWARD

Location tracking and social media monitoring of employees: It is necessary for both employers and employees to become aware of the implications of the Protection of Personal Information Act on these practices. Employers will have to justify the collection and storage of such information, ensure that it is secure, and make sure that the employee is aware of the monitoring. Research is needed into how widely social media monitoring is used by employers in South Africa to profile potential employees, and the implications of POPIA for this practice.

Commercial location tracking: The public in general needs to become aware of the extent to which their smartphone applications generate data about their online activity, mobile phone usage, day-to-day activity, as well as location data. They also need to be made aware of what happens to this data once it is collected and sold to third parties and data brokers. If people are not aware of how invasive smartphone applications truly are, they will not support advocacy movements for greater user privacy.

Covid-19 vaccine passports: While it may be an unavoidable requirement for international travel, advocacy groups must guard against the introduction fo vaccine passports for access to everyday services and amenities (such as shops, schools, government buildings, restaurants, etc.). People may choose not to be vaccinated for an array of reasons, including health, religious and personal convictions. This could place them before an impossible choice: vaccinate, or be marginalised.