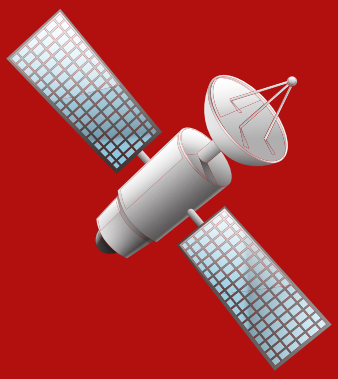
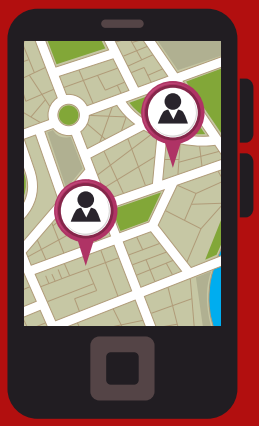
MOBILE PHONES AND LOCATION DATA

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. Europe also has a GPS, known as Galileo. Russia and China have similar navigations systems, known as GLOSNASS and BeiDou respectively.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 wireless router), 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.

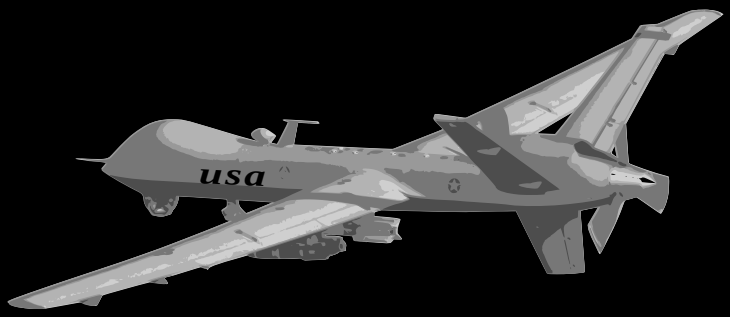
GLOBAL USE

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

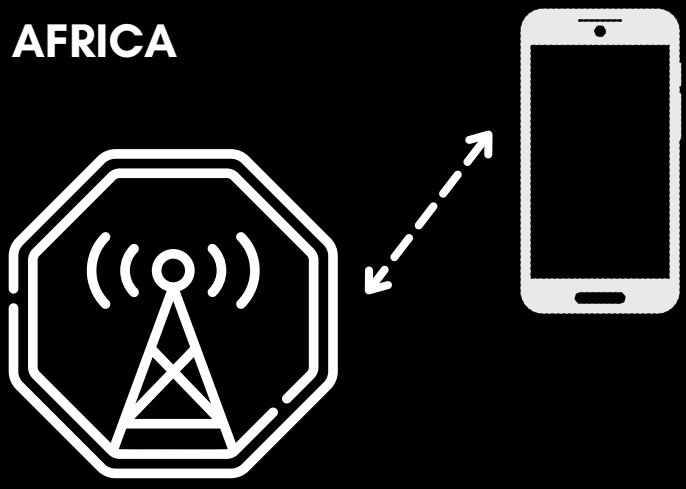
Although the use of the geolocation tracking is largely commercial, reports have surfaced of governments using location data generated by smartphone apps to track citizens. In November 2020 Vice news reported that the United States military was purchasing location data generated by a Muslim prayer app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



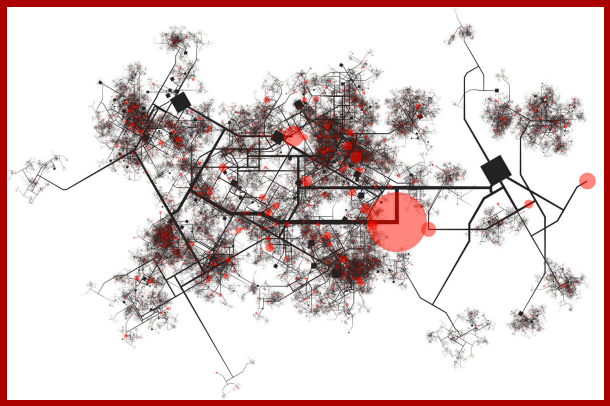
Police commonly use section 205 of the Criminal Procedures Act to compel cellular service providers to provide them with the location data generated when mobile phones connect to cell towers. This is known as tower data, and is typically contained in the billing records of a cell phone company's customer. 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 a 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.

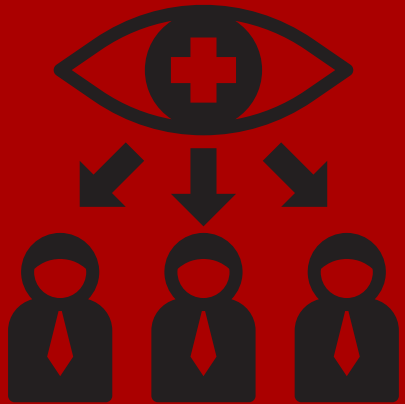
MOBILE PHONES AND LOCATION DATA

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 data 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.

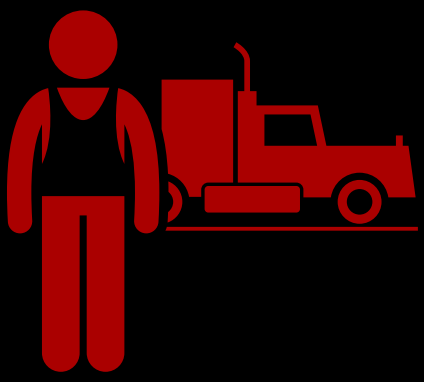
In countries where governments have employed invasive Covid-19 tracking apps using mobile phone location data, privacy advocates and researchers have been critical of the implications for individual privacy, warning that the surveillance may remain long after the pandemic has been brought under control.



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.



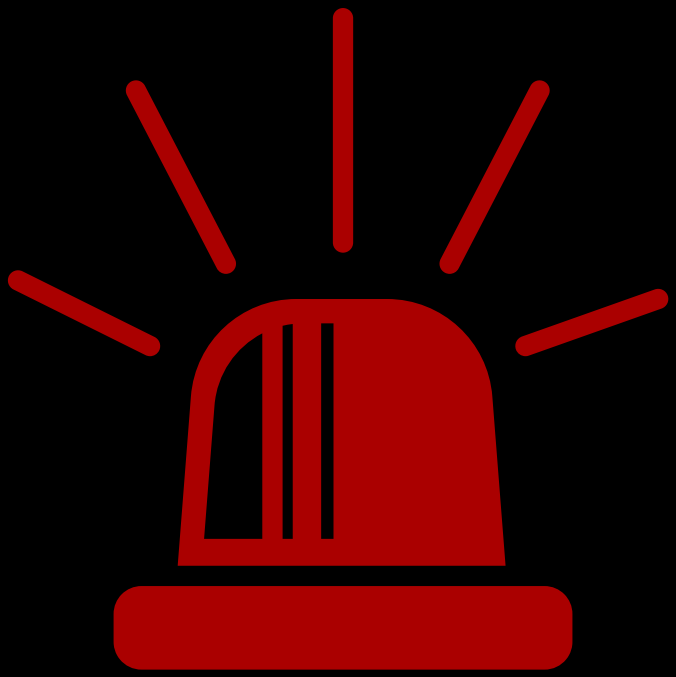
In terms of law enforcement, South African police appear to make minimal use of legal avenues that allow them to request location data from overseas companies who usually store application data. Although they can make use of a mutual legal assistance treaty to obtain such data from large organisations 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 connected, 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.