

Assessment of contact tracing options for South Africa

By Dr David Johnson



409 The Studios
Old Castle Brewery
6 Beach Road
Woodstock, 7925
Cape Town, South Africa
Phone: +27 21 447 6332
Fax: +27 21 447 9529
www.researchictafrica.net

1. Executive Summary	1
2. Abbreviations	4
3. Acknowledgements	5
4. Introduction	6
5. Contact tracing approaches	9
5.1. Manual contact tracing	9
5.2. Direct proximity detection	10
5.3. Position-based tracking (GPS / cell tower triangulation)	12
5.4. Physical code scanning systems	13
6. Current device ecosystem and availability of smartphones	15
6.1. Contact tracing technology support	15
6.2. Contact tracing operating system aspects	17
6.3. Projected smartphone penetration	18
6.4. Potential effectiveness of smartphone-based contact tracing in South Africa	19
7. Current smartphone applications/platforms available	20
7.1. Safe Paths	21
7.2. Path check suite	21
7.3. BlueTrace (Known as TraceTogether in Singapore)	22
7.4. Covid Watch	22
7.5. Covid Alert South Africa	22
7.6. Covi-ID	23
8. Current challenges deploying Covid Alert in South Africa	23
9. Heat Maps	24
9.1. Active cases	24
9.2. Movement data	24
9.3. Crowdsourced hotspot mapping	26
10. Immunity passports	27
11. Data protection considerations	28
11.1. Weaknesses at point of detection	28
11.2. Weaknesses in stored identity data	29
12. Conclusion	29
13. References	33

1. Executive Summary

Current epidemiology research on COVID-19 shows that contact tracing is only able to curb the growth of the epidemic, if we identify 50% of the positive cases and trace 60% of their contacts with no delay (Ferretti et al., 2020). If we take more than three days to quarantine contacts, the growth of the epidemic cannot be controlled. This puts enormous strain and pressure on manual contact tracing regimes to meet these tight requirements and provides motivation for other more automated tools that use smartphones or some other means to help provide faster notification times.

In countries like South Africa that have a dual economy with high income inequality and unemployment, there is no one-size-fits-all solution to contact tracing. Most automated contact tracing hinges on owning a smartphone and having Internet access, but Smartphone ownership and Internet access is limited. Current estimates are that between 49 and 52% of the rural population and between 63 and 69% of the urban population own a smartphone. A national contact tracing system that depends on smartphone ownership alone would leave a large section of the population (mostly the low-income portion of the population) locked out of the contact tracing programme.

There is an argument to be made for smartphone-based contact tracing in urban areas due to its higher smartphone penetration. The effectiveness of a smartphone application in detecting person to person encounters follows a square law where the number of encounters is asymptotically proportional to the square of fraction of the population using the application. If a contact tracing application was installed on smartphones in urban areas and we achieved close to 100% uptake (approximately 60% of the population that have smartphones with the required contact tracing features); we would detect approximately 36% of the contacts made.

Epidemiology models show us that this level of contact detection would require 80%¹ of the cases to be detected with immediate notification and isolation to have an impact on reducing the spread of the virus. This is a tough target and provides motivation for a better approach that uses a combination of multiple contact tracing regimes (manual and automated) that all have an underpinning theme of being privacy-preserving.

The following approach is suggested:

- Continue with manual contact tracing augmented by the **COVID Connect application** and ensure that the notification interval does not exceed two days and ensure that checking the status of test outcomes can be carried out in privacy. An external security audit should be regularly carried out on the central database, to ensure it is POPI compliant and the sensitive data is only used for its original intended purpose and is anonymized for research or deleted once the pandemic is over.

- **Rapidly scale up the GAEN-based contact tracing system, COVID Alert**, for users who have smartphones by using a widespread marketing campaign on radio, television and the Internet and as part of a daily COVID-19 cases report. Specifically target the major city centres where exposure risk and smartphone penetration are highest.
- Ensure that **zero-rating of tracing key data** used by the app functions on all South Africa's networks as promised.
- **Translate the app** into all South Africa's official languages to ensure that there are no barriers to uptake.
- Explore mechanisms such as **data rebates**, once the app is installed, to overcome the current technical impossibility of zero-rating the app (3MB) and its library dependency (45MB) download. The data rebate could make use of a code generated by the app to claim a rebate. Providing users with a little more data than is consumed by the app – 100MB, for example - will also provide an added incentive to install it.
- Establish a **contact tracing technology lab** at a neutral organization such as the CSIR or a University to carry out tests on battery drain by the app as well as privacy checks and publish these on the Coronavirus website to put user's minds at ease and combat fake news about the app.
- For users without smartphones, users that don't want to install the GAEN-based application due to security concerns or users who want additional knowledge about potential contacts, deploy the **CoviID system**.
- Continue with **country wide hotspot mapping** (such as the one being run at the CSIR in partnership with the National Department of Health) using randomized locations of individuals who test positive and aggregate movement data from operators and platform providers such as Google. This system can be supplemented with a GAEN-based contact tracing system and the CoviID system to provide a more complete picture of where there are higher risks of infection.
- Use an **incentive scheme** to encourage users and businesses to make use of contact tracing applications. For example, medical aids schemes that have reward programs such as Discovery Vitality and Momentum Multiply that already have some tracking systems for fitness and safety purposes could provide rewards for 14-day self-isolation. For users that are not on these medical schemes, mobile operators could partner with the government to provide data rebates for users that install the app and when self-reporting their status. Tracking users not on private medical aids who haven't opted into their health and safety tracking systems is fraught with privacy concerns and should be avoided.
- Ensure that all deployed systems can **interoperate in a secure manner**. Data formats for contact and location data and security mechanisms for shared data should be agreed on. This will help, for example, provide notifications to individuals where detection of this exposure could have been through manual contact tracing, smartphone-based contact tracing or QR-code-based contact tracing.

- **Cross-border contact tracing** will become critical as South Africa opens up its borders. Similar to Europe (Lomas, 2020), South Africa should participate in discussions in various regions on how to exchange encrypted tracing keys of infected individuals to enable travellers who enter the country to be alerted if they were in contact with somebody who tested positive for COVID-19 while outside the country.

Time barriers to implementation are often more political than technological. It may take time to agree on a protocol for providing test verification codes that can securely provide confirmation of test status to multiple applications without revealing personal information. The Protection of Personal Information Act 4 of 2013 (POPIA), which finally came into force on 1 July 2020 can be used as the guiding principle for this purpose. Contact tracing creates another political challenge - it allows certain sectors of the economy to open up and others not. For example, more crowded businesses districts in the city may need to temporarily close whereas less dense suburban businesses may be able to stay open. This will need to be managed very sensitively.

It is also critical to have oversight to develop and enforce privacy guidelines for these technologies and continually review the impact in real-world situations. In South Africa, a judge has been appointed for this purpose, but civil society organisations, community groups and social movements should also continue to keep a close watch on how sensitive data collected from contact tracing systems is used and disseminated.

The challenges of zero-rating sites and health apps like COVID Alert and the lack of access for many low-income users who are required to stay home and continue to be economically active or continue their education provides strong motivation for a free basic data rate service in South Africa. This basic data rate service would provide always on, low-bandwidth access for all South Africans on any operator network and ensure that a basic level of access to critical digital services is always available.

Given that many of these recommendations will take time to put in place and implement, it would be prudent to implement these without delay to at least attempt to contain any further new waves of the COVID-19 pandemic and to contain new pandemics that will occur in the future. But, equally importantly, we also need to constantly guard against abuse of our civil liberties by an increasingly securitised state during the pandemic.

2. Abbreviations

BLE: Bluetooth Lower Energy

BR: Bluetooth Basic Rate

DDOS: Distributed Denial of Service Attack

EDR: Enhanced Data Rate

ENS: Exposure Notification framework

GAEN: Google Apple Exposure Notification

NDoH: National Department of Health

proxID: Proximity ID used in the Google Apple Exposure Notification system

TEE: trusted execution environment

WHO: World Health Organisation

3. Acknowledgements

This study was made possible by having many conversations with experts on the topic and I'm thankful for the inputs from Jabu Mtsweni, head of the Cyber and Information Research Centre at CSIR and Co-Pierre Georg, Associate Professor at the University of Cape Town School of Economics. I am also grateful for the editing contributions from Albert Lysko, Principal Researcher at CSIR's Next Generation Enterprises and Institutions cluster, Meena Lysko from Move Beyond Consulting and Alex Comninos and Fazila Farouk at Research ICT Africa. Much of the initial draft of this work was inspired by a Webinar titled: COVID-19, Technology, Privacy and Civil Liberties by Ed Felten at Princeton's Center for Information and Technology Policy.

4. Introduction

Containing the spread of COVID-19 (SARS-CoV-2) involves an interlocking set of activities and none of these alone are a silver bullet. Due to the high natural rate of infection for COVID-19 (an R_0 factor of 2.3), a very radical set of steps are required to control its spread. The prime challenge is that you are always one step behind controlling the spread of the virus if you only self-isolate when you know you're infected. This is due to the virus spreading while asymptomatic. Modelling data shows that if only those with symptoms are identified and isolated, you cannot stop the spread of the disease as you are highly likely to have already passed on the illness.

There are only two paths to reduce the number of people encountering a contagious person; a shelter-at-home style policy or targeted quarantines. Shelter-at-home is a coarse tool that severely impacts the economy whereas targeted quarantines are a more fine-grain approach that allows some sectors of the economy to reopen. Contact tracing is a key component of targeted quarantines as potentially infected individuals need to be detected and then informed that they need to start self-isolation.

Some subset of the following six components are typically found in any country fighting against a pandemic.

- **Symptom screening:** Usually carried out by healthcare workers going door-to-door or in public spaces. This will involve a set of questions such as, "Have you had a fever and cough?" or "Have you travelled to a high-risk area?". Based on this screening, a test may or may not be carried out. Symptom screening is necessary due to the limited number of testing kits. Symptom screening can also be conducted virtually with an app or, in the case of South Africa, with the CovidConnect WhatsApp and SMS platform.
- **Testing:** This is normally carried out by public health officials or private health care providers. Swab samples are sent to test labs and reports are sent back to health officials who then inform the patient of the outcome. Testing is normally only carried out on high risk individuals who have symptoms that clearly show a high risk for COVID-19 or individuals who work in high risk environments where even mild symptoms may warrant a test.
- **Contact tracing:** This is the process to check who the infected patient has been exposed to. This can be a manual or digital process or a hybrid of both. In the manual process, the patient is asked who they have been in contact with. The digital process makes use of an automated approach where a location or proximity system on a user's phone or some other identifier provides information on who the infected individual has been in contact with.
- **Exposure notification:** This is the process to notify users who might have been exposed to someone with COVID-19. When contact tracing is done manually, notification is carried out by a health official who contacts the list of people listed as living in the individual's household or who they normally come into regular contact with. When contact tracing is automated, an infected individual's device running contact tracing software can report their positive status to

a central datastore using de-identified information and this can be broadcast to other user's smartphones to inform them that they have been exposed.

- **Hotspot detection:** This is a helpful tool to issue warnings about hotspots that could trigger super-spreader events. This can help direct focussed efforts for sanitizing areas or carrying out testing. This can be created manually or digitally or using a hybrid of both. For the manual case, patients who test positive and possibly their contacts can be plotted on a map with randomization of their position. For the digital case, software can use de-identified geolocation data from a GPS to plot movements on a hotspot map. Additional general population movement data from sources such as the Google community mobility report can be used to check movement patterns in the hotspot and estimate the risk of spread of the disease in that area.
- **Immunity passports:** Some work environments have higher risk for infections, such as public transport, the health sector and schools. Immunity passports would, in theory, enable employees, customers and contractors to set individual limits for persons who have shown symptoms of COVID-19. An immunity certificate could be issued when somebody has recovered or been vaccinated. The World Health Organisation (WHO) has argued against certificates as the jury is still out on whether recovery provides complete immunity. There are also many other risks such as score settling by employees, company sabotage and trying to encourage spread of the disease, where individuals try to get infected with COVID-19 in order to get immunity and obtain an immunity passport.

This study will focus on contact tracing specifically. However, information from contact tracing plays a key role in providing information for hotspot detection, screening and immunity passports as well as allowing smarter testing policy that directs testing resources to where they can create the most public good. Once contact tracing systems notify individuals that they have been exposed to a COVID-19 positive individual, they should be incentivized to self-isolate for 14 days (Wamslet & Selena, 2020) to help contain the spread of the virus.

Efficient containment requires almost immediate notification of contacts. Ferretti et al. created an epidemic model that shows a zone of control of spread of the virus for different combinations of (i) fraction of cases isolated, (ii) fraction of contacts quarantined and (iii) number of days until a COVID-19 positive person is isolated, and their contacts notified (Ferretti et al., 2020). This study shows that even a three-day delay in identification of contacts makes containing the virus impossible. Some examples are:

- 60% of contacts of half of all positive cases would need to be quarantined immediately.
- if we can only identify 20% of cases, we would need to quarantine 70% of contacts immediately
- If it takes two days to isolate patients and notify their contacts and we can only identify 20% of cases, we would need to quarantine 80% of their contacts.

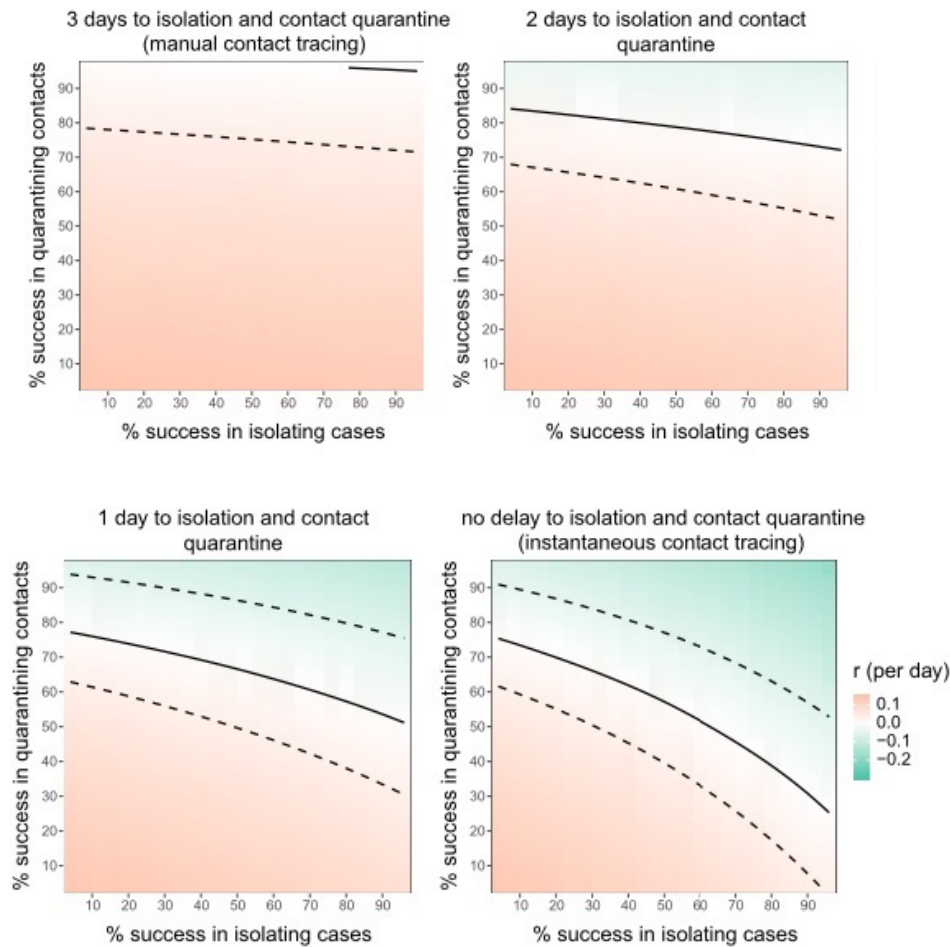


Figure 1: Quantifying intervention success (Ferretti et al., 2020)

Current estimates (See Section 4), based on projections, reveal that between 55 and 60% of South African adults own smartphones. However, urban areas may have reached between 62 and 69% smartphone penetration amongst adults (see Section 4).

The effectiveness of a smartphone application in detecting person to person encounters is as follows: the number of encounters is asymptotically proportional to the square of fraction of the population using the application. If a contact tracing application was installed on smartphones in urban areas and we achieved close to 100% uptake (60% of the population have the contact tracing application); we would still only detect approximately 36% of the contacts made.

Looking at Ferretti's model, we can see that

- Only immediate notification and isolation of more than 80% of cases with detection of 36% of contacts made will have an impact on reducing the spread of the virus.

- If app penetration only reached 50%, then we would only be able to detect 9% of contacts made, which would render the contact tracing application essentially ineffective.

This provides a somewhat weak argument for widespread use of an automated contact tracing. There may, however, be certain regions in urban areas or specific work environments where a much larger fraction of the population have smartphones and will be willing to use a contact tracing application. The reality is that every technique to curb the spread of the virus can help save lives, but no one single solution is likely to fully contain the virus. For example, Iceland reached 40% user uptake of their contact tracing in May 2020 - the highest in the world - but the system has had very little impact as yet (Johnson, 2020).

It's also critical that civil liberties are protected and using systems like contact tracing apps remain voluntary. Some countries, such as India, are forcing some of their citizens to install a contact tracing app or risk losing their jobs or reprisals (Howell O'Neill, 2020a). This approach will completely erode public trust in the government and likely lead to a backlash in the use of a contact tracing programme.

5. Contact tracing approaches

Contact tracing is the process used to check who a COVID-19 positive person has been in contact with during the contagious period of the disease and contacting and quarantining exposed people. Often these contacts will be made during the pre-symptomatic period of the disease following exposure to the virus and can be between five and 14 days.

There are four broad contact tracing approaches and each of these will be discussed in turn

- Manual contact tracing:
- Direct proximity detection
- GPS tracking
- Physical code scanning systems

The key argument for non-manual contact tracing is that user location data or proximity detection is better than human memory and can also identify strangers you come into contact with. A hybrid of any of these four approaches can also be used by contact tracing applications or public health contact tracing programs.

5.1. Manual contact tracing

This is usually carried out by a public health official when a test is carried out. Typically you are asked to fill in a form where you list people in your household that you were exposed to as well as other people who you have been in contact with, in the past 14 days.

If the test is positive, the health official will then contact the exposed individuals and advise them to undergo a quarantine period of 14 days. The personal data from the individual carrying out the test and on the exposed individuals is confidential and kept at the department of health.

The main challenges with manual contact tracing are:

- It relies on human memory and most people won't be able to identify those they've been in contact with beyond their close contacts in their household or workplace.
- It takes time and a large number of human resources to carry out interviews and do follow ups on contacts.
- Modelling data shows that manual contact tracing alone is not enough to contain the spread of COVID-19.

Manual contact tracing can be enhanced with the use of a mobile phone application. For example, South Africa has launched the COVIDConnect platform built by the Praekelt Foundation that works on WhatsApp, SMS and USSD to provide patients with test results and steps through a set of questions to assess the severity of their symptoms (Labuschagne, 2020). Patients can also upload information on people they have been in contact within the days before they tested positive. COVIDConnect is not a contact tracing application in the true sense, it simply augments the manual contact tracing process and may free up some human resources and allow them to focus on more severe cases and focus their energy on follow ups in more serious areas.

5.2. Direct proximity detection

The core principle of direct proximity detection is to use short range technology on a smartphone to detect when two devices were near each other and keep a record of this interaction. Currently, the only technology on smartphones appropriate for this type of communication is Bluetooth, specifically Bluetooth Lower Energy (BLE). BLE was originally marketed by the Bluetooth Special Interest Group (Bluetooth SIG) at applications in the healthcare, fitness, security, and home entertainment industries. BLE is available on 90% of smartphones made since 2014.

It runs as an independent communication channel to Bluetooth Basic Rate (BR) and Enhanced Data Rate (EDR) used for links such as audio connections to headsets and data synchronization to PCs and is not compatible with these protocols but BLE can coexist with the BR and EDR and uses. The standard was integrated into Bluetooth 4.0 in December 2009. BLE has very little impact on the battery life of a phone, as it only uses between 0.25 and 0.01 Watts when actively communicating for short bursts of time.

The advantage of Bluetooth based systems over GPS:

- Only detects real close-contact encounters within a limited 3D radius, whereas GPS could record false positives on a multi-story building at the same 2D location

- Has a privacy advantage over GPS as no position information is stored and is less vulnerable to de-anonymization, although it is not full proof against these kinds of attacks (see Section 7)

For users without smartphones, there is also the option of producing dedicated devices with BLE built in. These could be produced for as little as \$10 (Hart et al., 2020).

There are two approaches currently used by Bluetooth based systems:

- Centralized warning system with a rotating hashed centralized ID
 - Users are provided with a random ID only known to central authority
 - All users broadcast a beacon with a hashed version of their ID, which changes often (e.g. every 15 mins)
 - All devices within range of the beacon record IDs they detect
 - When diagnosed as positive, a user sends the central authority the IDs they recorded
 - The central authority then identifies who was exposed by checking if the hashes of centrally known IDS match and then contacting individuals exposed
 - Risks:
 - ◆ Susceptible to government abuse
 - ◆ One central database of medical information
 - Current deployments:
 - ◆ TraceTogether, Singapore
- Central Server, Decentralized rotating pseudorandom tokens
 - Everyone creates their own random token-generator and uses this to broadcast rotating randomized tokens at a recurring frequency
 - Nearby devices record tokens they detect
 - When diagnosed, a user sends their token generator to a central server
 - The token generator of the positive user is broadcast across the network to all devices
 - All users check if the token generator generates tokens that match tokens they have been exposed to
 - Advantages:
 - ◆ Mitigates the centralization risk as the central server stores and forwards tracing keys that look random and have no value
 - ◆ Low bandwidth requirements as users are not sending all received tokens to central server
 - ◆ Allows a variety of key retention lifetime options
 - Current deployments:
 - ◆ Google Apple Exposure Notification (GAEN)

The best example of a central server, decentralized rotating pseudorandom token system is the Exposure Notification framework (ENF), also known as the Privacy-Preserving Contact Tracing Project, developed by Apple and Google. Most of the literature calls this system the GAEN (Google Apple Exposure Notification) system. The system was announced on 10 April and is used to facilitate digital contact tracing on Android-based phones and iPhones. The framework is only available to governments and health agencies who develop an application for their country/state/province and agree to strict privacy and security guidelines.

The GAEN system works as follows:

- Broadcasts a rolling proximity ID; also known as a proxilD (changes every 15 mins)
- Device records every proxilD it hears
- Every user has a tracing key that only the user knows. This is used to derive a daily tracing key, which in turn is used to derive proxilDs that change every 15 mins (using publicly known methods)
- When diagnosed, a user consents to upload their daily tracing key to some public server (these look random and have no value should this server get compromised)
- All users download tracing keys (e.g. every day) and recalculate the COVID-19 positive list proxilDs (they've received) based on tracing keys
- A user checks to see if they saw any of these positive proxilDs

As of 1 September, 2020, the GAEN system has been released in 27 countries and is in active development in 10 more countries (Rahman, 2020) (See Appendix A for full list). On 2 September 2020, the Department of Health, South Africa deployed a GAEN-based system called Covid Alert.¹ The app makes use of all the features of GAEN to detect when somebody has been in contact with somebody for more than 15 minutes, but also makes use of a unique secret SMS code that is sent when a person is tested positive. This code is entered into the Covid Alert app and then notifies all users with the App that have been in contact with the positive user within a 15-day window period. The SMS code is used to ensure that users don't report false positive cases in the system.

5.3. Position-based tracking (GPS / cell tower triangulation)

Position-based tracking, that uses GPS or cell tower triangulation can be used to build a location history of an individual, which in turn can be compared to other individual location histories to look for interactions.

Cell phone tower triangulation data is generally too coarse grain to identify potential exposure events. Most cell phone towers can only identify users to within a 400m accuracy level. In densely populated

¹ <https://play.google.com/store/apps/details?id=za.gov.health.covidconnect&hl=en>

townships, for example, this could contain over 1000 people. Generally, cell phone data has been used for:

- Generating heat maps showing movement data
- Checking compliance with national lockdown measures
- Checking individual compliance in more authoritarian governments

We will therefore only continue to discuss GPS-based tracking for determining location for contact tracing purposes.

A significant advantage of this approach is that it can track surface transmission. i.e. a tracked infected user may have touched a surface, which a potentially exposed tracked user intersects with. Another advantage is that phones often already store GPS information; for example, the Google Maps application constantly stores location information. A contact tracing app could extract pre-existing tracking information and identify potential exposure events even before the application was installed.

A disadvantage of position-based tracking systems is that they are less accurate at detecting a real exposure event. For example, in a multi-story building, a GPS may locate two people at the same 2D point when they may be on different floors of the building. Another disadvantage of location-based tracking is that it is harder to anonymize correctly and a central authority tracking location data could be open to abuse or a target for hackers or bad actors.

Originally, the widely used PathCheck application was only making use of GPS data, but following the development of GAEN. The PathCheck² application advertises its mobile app as either a GPS or GAEN system. In the GPS system, GPS data is only stored on a user's phone. When an individual is notified of a positive test result, they voluntarily send encrypted identifiable data to a specialized server, which a contact tracer verifies. This is then de-identified by the system and de-identified data is published on the server. Healthy users of the system download these de-identified points of interest to see potential exposure events.

Storing your own GPS data can also help augment manual contact tracing by helping you remember where you were in the manual contact tracing interview.

5.4. Physical code scanning systems

The de-facto standard for storing a rich set of information in a physical printed code is the QR code system. QR code-based scanning for check in systems (e.g. for airplane tickets) or for payments have been around since the 1990s. Most of these systems embed information about the user or the product

² <https://pathcheck.org>

inside the QR code in a similar way that barcodes work but can store much more information; QR codes store up to 4296 characters.

In China, QR code-based systems on phones are used to control the movement of people and identify those who have been diagnosed with the virus or visited areas with high infection rates. QR code-based access in China is now at restaurants, shops, malls and banks and they are even used for entry to neighbourhoods. Data is centrally stored and once the system builds up a profile of areas you have visited, a green status means you can enter any area, a yellow status means you need to be quarantined and a red status indicates infection or travel to a high risk area; a user moving around with a red status may even warrant the police being called.

Many companies are developing less privacy-invasive systems using QR codes. Co-Pierre Georg in the School of Economics at University of Cape Town has developed a privacy-preserving application called CoviID built on blockchain technology that also allows an identifier, linked with geolocation information, to be scanned even when users don't have a mobile phone.

CoviID works using the following steps:

- A User generates a unique QR-code identifier, which can be on a phone or printed on a card.
- Verifiers can be restaurants, security guards, etc. who scan the code on a printout or phone.
- When a user reports positive, the manual contact tracer queries CoviID API for geolocation receipts.
- The user must consent to the query to access their data.
- Verifiers can provide more context on the location / e.g. indoor / outdoor and what protections are in place.

CoviID can also use Bluetooth and geolocation to track and trace the movements of an individual covering the two weeks prior to their testing positive for the virus. The difference between typical QR-systems like the one used in China and CoviID, is that users maintain full control over their data. Data generated by contact transactions (e.g. scanning somebody's QR code at a restaurant) is stored centrally but in a trusted execution environment. In this system whenever a user, such as a government agent, needs access to the data, permission must be obtained from the data owner to expose portions of the data that the user has given permission to. This limits the extent to which information about them is shared with others, a key aspect of a system being privacy preserving.

With the system being able to operate in environments where users don't own a smartphone, CoviID or similar systems are very well suited to the current South African context and other contexts with low smartphone penetration.

6. Current device ecosystem and availability of smartphones

The most recent studies on smartphones in South Africa are the ICASA State of the ICT Sector Report (ICASA, 2020) published March 2020, the Pew Research Centre study published October 2018 (using data collected in Q4 2017) (Silver & Johnson, 2020) and the 2018 After Access study (Gillwald & Mothobi, 2019) published July 2018 (using data collected during 2017).

The ICASA study used supply side data and counted the total number of data SIM cards from mobile operators as of September 2019 to estimate the smartphone penetration. Their study showed that 91.2% of the population have smart phone subscriptions (up from 81.7% in 2018 and 74.2% in 2017), but this also accounts for users who have multiple phones or Sim cards. A study by GeoPoll on smartphone usage and data costs in South Africa in February 2020 among 400 respondents, found that 60% of respondents own more than one phone (GeoPoll, 2020).

The Pew research study made use of survey data collected in Q4 2017 of users 18 and older to collect information on the types of phones people own and the type of applications they use as well as demographic information. They report percentages based on the total sample in their survey. Their study found that nine-in-ten adults own a mobile phone, i.e. 40% own a basic feature phone and 51% own a smartphone.

The After Access study made use of survey data collected in 2017 covering a total of 1814 respondents randomly sampled from adults 15 years and older living in households. The study found that 54% of the urban population owned a smartphone and 33% of the rural population owned a smartphone. The average smartphone ownership was 47%.

These mixed statistics from different time periods and users owning multiple SIM cards make the real smartphone penetration number hard to predict accurately. Using the trend in smartphone subscriptions from ICASA that has shown a 23% increase from 2017 to 2019; the potential true smartphone penetration can be estimated using the 2017 After Access study as a baseline and extrapolating this estimate to September 2019. This method results in a smartphone penetration level of 57.34% in 2019. This may have grown to near 60% in 2020; but some level of market saturation may have occurred with the ICASA smartphone subscription level increase also including additional acquisition of multiple subscriptions. For the purpose of this study, we will assume a potential national smartphone penetration in 2020 for adults has now reached levels between 55 and 60%.

6.1. Contact tracing technology support

Contact tracing driven by mobile operators using cell phone tower data can work on any mobile phone, but fundamentally violates personal privacy and other human rights. Contact tracing making use of

Bluetooth and GPS technology can be designed using privacy protecting principles but only works on smartphones.

The following table looks at the current device ecosystem for all phones that support Bluetooth Low Energy (used by most contact tracing applications) and GPS since 2014 (phone up to 6.5 years old). According to the consumer electronics association, the average smartphone life expectancy is 4.7 years but there is an active 2nd hand market for smartphones in Africa and changing the battery can give a phone a few more years of life.

	Total	Percentage
All phones (since Jan 2014)	3837	
Smart phones (since Jan 2014)	3693	
All phones with BLE	3327	86.71%
Smartphones with BLE	3313	89.71%
All phones with GPS	3621	94.37%
Smartphones with GPS	3608	97.70%

Table 1. BLE and GPS support on all smartphones since 2014

The following table looks at low end market phones (phone less than 100 GBP / 115 USD) that support Bluetooth Low Energy and GPS.

	Total	Percentage
All phones (since Jan 2014)	518	
Smart phones (since Jan 2014)	455	
All phones with BLE	404	77.99%
Smartphones with BLE	396	87.03%
All phones with GPS	446	86.10%
Smartphones with GPS	441	96.92%

Table 2. BLE and GPS support on low-end smartphones since 2014 (price less than \$115)

Currently contact tracing applications usually require a smartphone to operate. At this stage, the author does not know of any contact tracing applications that can use Bluetooth or GPS on a feature phone. This means that the only relevant statistics are smartphones with BLE and GPS. Smartphones supporting BLE technology is in the 87% to 89% range but with most users in South Africa owning low-end smartphones, the real number is likely to be close to 87%. Smartphones supporting GPS technology is 97% to 98% range and the actual penetration of GPS smartphones is likely to be around 97%. BLE has

very little impact on the battery life of a phone whereas GPS can have a more significant impact on a phones battery life if left on indefinitely; users are therefore more likely to opt for a BLE solution to avoid battery drainage.

Given the current smartphone penetration, the number of potential devices as a percentage of the population that can use the different technologies is as follows:

	Minimum (%)	Maximum (%)
Smartphone penetration	55	60
Contact tracing smartphones with BLE	47.9	52.2
Contact tracing smartphones with GPS	53.4	58.2

Table 3. Availability of BLE and GPS smartphones in South Africa

6.2. Contact tracing operating system aspects

Another important aspect of support for contact tracing on smartphones, is the current operating system distribution in South Africa. All the contact tracing software solutions that have been released (described in Section 4.) run on Android on Apple iOS. Statcounter³ has been monitoring operating system market share since January 2009. The current global market share for mobile operating systems as of August 2020 is as follows:

- Android: 74.25%
- iOS: 25.15%
- Samsung: 0.23%
- Other: 0.13%
- KaiOS: 0.08%
- Windows: 0.03%

Android and iOS make up 99.4% market share making other operating systems, essentially insignificant.

In Africa the market share as of August 2020 is as follows:

- Android: 86.89%
- iOS: 10.57%
- Other: 1.76%

³ <https://gs.statcounter.com/os-market-share/mobile>

- Series 40: 0.18%
- Linux: 0.15%
- Nokia: 0.1%

Android and iOS make up 97.46% market share, the remaining operating systems are mostly used in lower end feature phones and are therefore already assimilated in the statistics capturing the fraction of smartphones in South Africa. The only other potential contender operating system in the smartphone market is Huawei's HarmonyOS, but phones with this operating system have yet to become available on phones in the African market.

The Android app makes use of a library called Google Play Services to implement GAEN, which is regularly updated on users phones. GAEN on Google Play Services requires at least Android 5.0 (lollipop) and up - released November 2014 - should be on all android smartphones made since 2015. However, Google does advise using Android 6.0 (Marshmallow) and up - released October 2015 and cannot vouch for the stability of GAEN on Android 5.0.

The iPhone app requires iOS 13.5 or later - released May 2020 and only runs on iPhone7 and upwards (released October 2016), which is generally available on apple iPhones from 2017 onwards.

The latest iOS, version 13.7, and the latest Android Google Play Services will have built in GAEN that can exchange proxIDs with other phones without a contact tracing app being installed. This could be a crucial aspect of increasing the number of phones that are exchanging Bluetooth beacons even before an app is installed to check if you've had an exposure event or want to self-report a positive test for Covid-19.

Currently there does not appear to be any risk that current smartphones in South Africa won't be able to run the contact tracing applications, such as COVI Alert SA, due to a lack of Android or iOS-based smartphones. Technology-related limited uptake will likely only be linked to not owning a smartphone with BLE or a small fraction of very old phones that cannot install an operating system from Android 5.0 or iOS 13.5 onwards.

6.3. Projected smartphone penetration

The penetration threshold of devices with BLE technology (the technology used for contact tracing in the COVI Alert App in South Africa) is too low to reach any level of meaningful contact tracing across the whole country. However, this technology can be used in specific contexts such as large office spaces, amongst health workers or even in urban areas where smartphone penetration is much higher. There hasn't been a demand-side smartphone survey since 2017 but extrapolating data from the 2017 After

Access survey, we project the following estimate for smartphone penetration in 2020 for urban and rural areas, shown in Table 4.

	Total	Rural	Urban	Urban (GPS)		Urban (BLE)	
				All	Low end	All	Low end
Population size 2020 (million)	59.31	19.76	39.55				
Population 2020 (percent)		33.31%	66.69%				
Smartphone penetration lower limit 2020 (percent)	55%	38.61%	63.18%	61.73%	61.24%	56.68%	54.99%
Smartphones penetration upper limit 2020 (percent)	60%	42.12%	68.93%	67.34%	66.81%	61.84%	59.99%

Table 4. Projected Availability of BLE and GPS smartphones in urban South Africa

This projection shows that there is potential to use smartphone contact tracing in urban centres, with potential smartphone penetration between 63 and 69% of the adult population. Technology support shows projected urban smartphones supporting GPS between 62% and 67% of the adult population and projected urban smartphones supporting BLE between 57% and 62% of the adult population. The numbers are marginally lower for low end phones.

6.4. Potential effectiveness of smartphone-based contact tracing in South Africa

The effectiveness of a smartphone application in detecting person-to-person encounters follows Metcalfe's law where the number of encounters is asymptotically proportional to the square of fraction of the population using the application. If a contact tracing application was installed on smartphones in urban areas and we achieved close to 100% uptake (application installed on approximately 60% of the population's smartphones in urban areas); we would detect approximately 36% of the contacts made.

Looking at Ferretti's model, we can see that only immediate notification and isolation of more than 80% of cases with detection of 36% of contacts made, will have an impact on reducing the spread of the virus (keeping the $R_0 < 1$). Having 60% of the population using the app to achieve disease control is also reported by a study done at Oxford in April 2020 (Oxford, 2020).

This is a tough target to achieve. For a city-wide smartphone-based contact tracing programme to be effective, additional contact tracing techniques beyond smartphones would be needed to supplement automated app-based contact tracing. Supplemental data from systems such as CoviID and manual contact with a notification period of under two days could be used. Singapore has followed this

approach and deployed a QR code-based system to augment their TraceTogether application. Even if the 60% target for population uptake is not achieved, any amount of user uptake can still reduce the number of daily new cases, albeit without full disease control (See Figure 2).

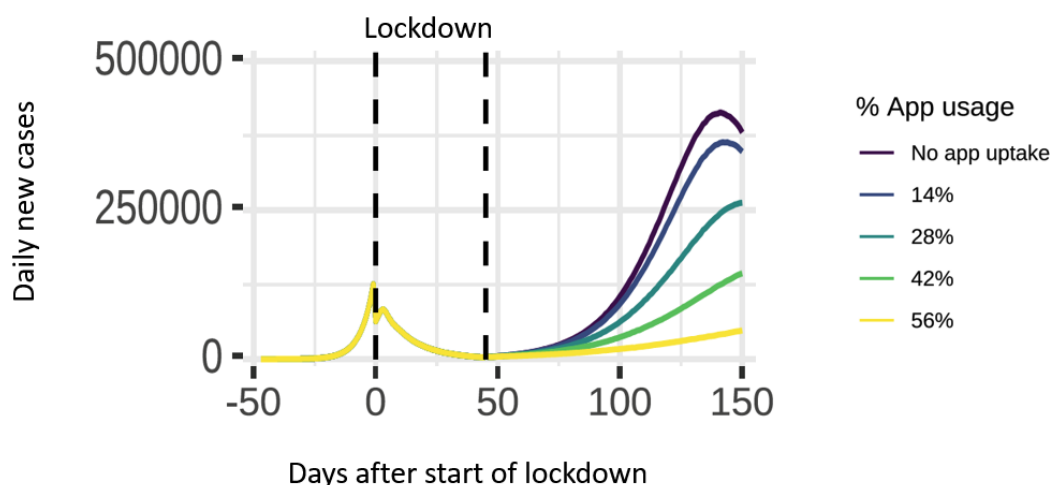


Figure 2: Number of daily new cases vs percent of population using App (Howell O'Neill, 2020b)

The deployment of an automated contact tracing system would require quick user uptake, and this could only be achieved if there was a high degree of public trust in the technology; especially the government's ability to ethically manage user data and with tamper-proof incentive mechanisms that reward users for compliance.

One additional caution is that the smartphone survey data only studied penetration amongst the adult population. When the entire population is taken into account - an important consideration given that young people are also carriers of the disease - the real penetration numbers will be lower, making it more difficult to use the contact tracing technology effectively.

7. Current smartphone applications/platforms available

All contact tracing applications⁴ essentially have two functions as shown in Figure 3: (1) Determine the contacts of between an individual and all other individuals using the application and (2) Notify contacts when an individual tests positive for the Virus

⁴ https://en.wikipedia.org/wiki/COVID-19_apps

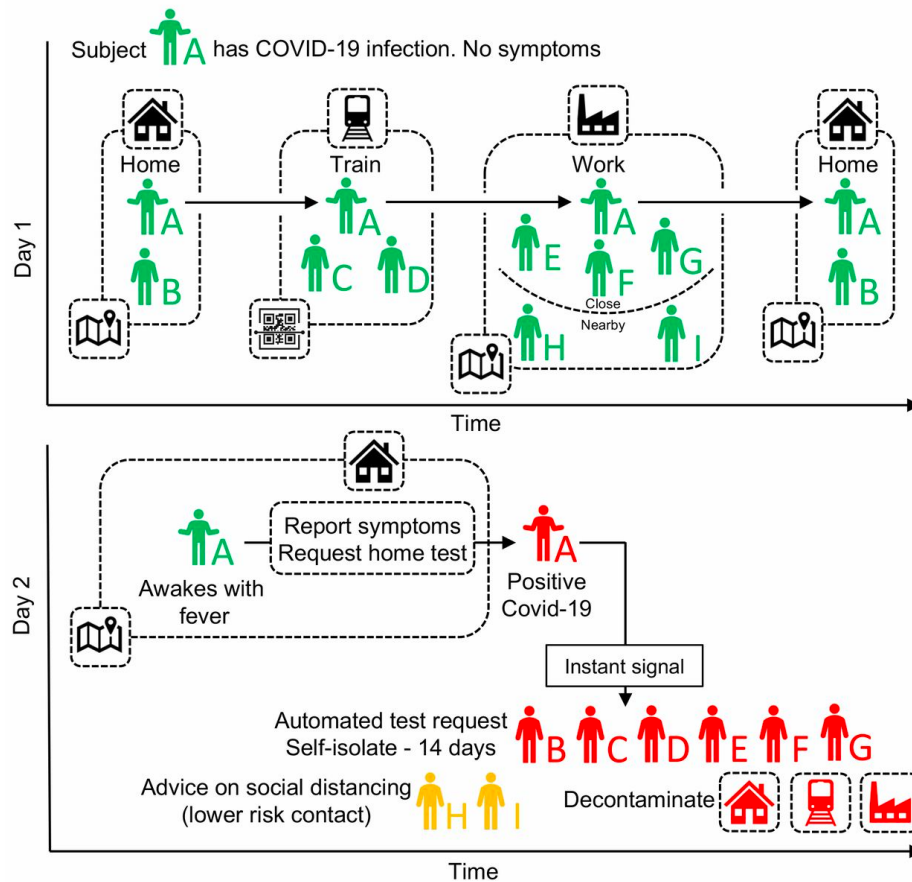


Figure 3: Contact tracing application timeline (Ferretti, Luca, et al., 2020)

7.1. Safe Paths

COVID Safe Paths⁵ is a mobile app for digital contract tracing (DCT) sponsored by Path Check, a non-profit and developed by a growing global community of engineers, designers, and contributors. Safe Paths is based on research originally conducted at the MIT Media Lab. Safe Paths mainly uses GPS for location tracking and maintains privacy by only storing GPS data on the users device in five minute intervals. The logged data only leaves the device if the user chooses to send the information to an authorized public health authority (PHA) as part of the contact tracing process.

7.2. Path check suite

The Path Check⁶ suite of open source software gives public and private sector organizations solutions for digital contact tracing and exposure notification using the GAEN protocol. It's a fully open source

⁵ <https://safepaths.mit.edu/>

⁶ <https://pathcheck.org/>

solution and includes a customizable mobile app and has a production-ready exposure notification server based on the Google open source project.

7.3. BlueTrace (Known as TraceTogether in Singapore)

BlueTrace⁷ is an open-source application protocol developed by the Singaporean Government. BlueTrace is the underlying system for the TraceTogether app. Australia has already adopted the protocol and many other countries such as New Zealand are considering BlueTrace for adoption. The protocol has strict preservation of privacy and requires health authority co-operation. For contact tracing (device to device communication) it uses the BLE protocol. It communicates a timeline of contacts to a centralized server owned by a health authority if a user tests positive. The health authority uses the logs it receives to notify users who came into contact with the infected patient.

7.4. Covid Watch

Covid Watch⁸ is an open source non-profit founded in February 2020 by Standard University. Their core mission is building mobile technology to fight the spread of COVID-19 pandemic while still defending digital privacy and preserving civil liberties during the pandemic. It started as an independent research collaboration between Stanford University and the University of Waterloo, and was the first team in the world to publish a white paper on contact tracing and develop a fully anonymous Bluetooth exposure alert protocol - the CEN Protocol, later renamed the TCN Protocol - in collaboration with CoEpi in early March 2020. This was a precursor to similar decentralized protocols such as the Google/Apple Exposure Notification system.

7.5. Covid Alert South Africa

On 2 September 2020, the Department of Health, South Africa deployed a GAEN-based system called Covid Alert.⁹ The app makes use of all the features of GAEN to detect when somebody has been in contact with somebody for more than 15 minutes but also makes use of a unique secret SMS code that is sent when a person is tested positive. This code is entered into the Covid Alert app and then notifies all users with the App that have been in contact with the positive user within a 15 day window period. The SMS code is used to ensure that users don't report false positive cases in the system.

- The app is 3 MB in size on android and 5MB in size on Apple OS and therefore has a negligible data cost
- The Google Play Services update to provide GAEN support is approximately 45 MB in size; not a negligible data cost

⁷ <https://bluetrace.io/>

⁸ <https://www.covid-watch.org/>

⁹ <https://play.google.com/store/apps/details?id=za.gov.health.covidconnect&hl=en>

- You will not have to pay for mobile data when you use the app – the data to use the app has been zero-rated by all of South Africa’s mobile network providers

7.6. Covi-ID

Covi-ID¹⁰ is a privacy-preserving contact tracing application built on blockchain technology that allows an identifier, linked with geolocation information, to be scanned even when users don’t have a mobile phone. It was developed at University of Cape Town by Associate Professor Co-Pierre Georg, convenor of UCT’s master’s in financial technology. A User generates a unique QR-code identifier which can be scanned at geo-referenced locations such as restaurants or security checkpoints. When a user reports positive, the manual contact tracer queries the Covi-ID API for geolocation receipts and after the user provides consent to access their data, notifications can be sent out of contacts made. Covi-ID can also use Bluetooth and geolocation to track and trace the movements of an individual covering the two weeks prior to their testing positive for the virus.

8. Current challenges deploying Covid Alert in South Africa

In September 2020, President Cyril Ramaphosa announced that zero-rating of the app would allow users to overcome cost of data as an obstacle to using the app. Testing carried out by Research ICT Africa has failed to identify an instance in which the app is zero-rated. Zero-rating one app alone on the Google Play Store or Apple App Store, is also technically infeasible as almost all websites and web services today are encrypted. ISPs have to zero rate entire sites as the URL to the specific parts of the site that needs to be zero-rated is encrypted. This can be observed in the current list of zero-rated sites during COVID-19¹¹. The encrypted connection to the app store (essential to the security and privacy of users) means that only the whole store, not a single app can be zero rated.

To solve this problem, the government could explore mechanisms such as data rebates once the app is installed to ensure that the data required to download the app itself does not preclude use of the app for low-income users. The data rebate could make use of a code generated by the app that is sent to the operator to get, for example, 100MB of data back on your data package.

While zero-rating of COVID-19 related content, communications channels, and applications should be encouraged, the difficulty of zero-rating in general points towards the need for a deeper approach for bringing down the cost of data or providing free data to support the fight against COVID-19. While the download of the Android app is only 3MB (with a possible required upgrade of the Google Play services app of approximately 45MB), and the data it transmits is even smaller (a couple of kilobytes), the use

¹⁰ <https://www.coviid.me/>

¹¹ <https://mybroadband.co.za/news/internet/356371-here-is-the-full-list-of-zero-rated-websites-in-south-africa.html>

of the app is only a small component of the data needed for contact tracing (including contacting contacts through WhatsApp for example). Contact screening, consuming information about COVID-19, working from home, and quarantining/isolating while still enjoying and exercising one's freedoms to communicate and associate are critical to creating a fair and just socio-economic environment during a pandemic.

9. Heat Maps

Heat maps are used to provide information about the level of risk of infection in specific areas of the country. The level of risk is typically generated using a combination of active cases combined with the level of movement in that area. This provides an indication of the probability of encountering an infected person in that area.

9.1. Active cases

Active cases can be collected from manual contact tracing. When a person tests positive, their location can be randomized (e.g. to a 200m radius) and plotted as a region on a map. When more cases with randomized positions are placed on the map and there are more overlapping regions, the risk 'temperature' in those overlapping regions increases. Active cases and regions that an infected person has visited can also be collected from automated contact tracing software that collects position information. Differential privacy can be used to improve the privacy of the data, but this is not completely safe. For example if there is only one active case in the area, it may be fairly trivial to establish who this is based on the rough movement patterns matching some observed behaviour.

9.2. Movement data

Movement data to carry out mobility modelling can be obtained from a number of sources. Generally public reports only present aggregate data but users usually have access to a historic record of their own personal movements.

- **Mobile networks:** Countries such as South Africa have legislation in place that allows the government to monitor people's movement using data from mobile operators for the purposes of restricting the spread of the pandemic. This information would need to be kept confidential and under the POPI act, cannot be used beyond the scope of the original intention. Data from the operators can be supplied in de-identified form to organisations that can, for example, produce heat maps.

- Location data collected by platform providers such as Google and Apple. These providers collect movement data for services such as navigation, tracking the location of a lost device. Historic movement data is often stored from the point where the user account was created.
- Location aware applications such as Facebook. Many web and phone applications capture location information to provide a location-aware service to users such as targeted advertisements, and social networking functions such as ‘users nearby’

The best example of publicly available movement data is the Google community mobility report shown in Figure 4.

Western Cape

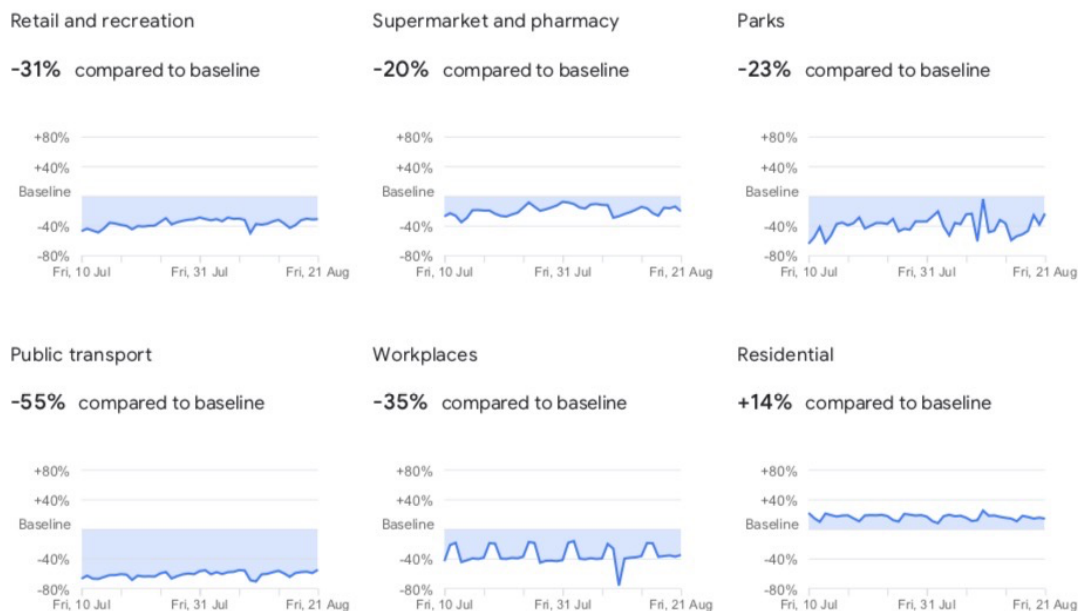


Figure 4. Google community mobility report for the Western Cape

- This helps you know how much mobility there is for different types of areas (grocery stores, parks, workplaces) compared to a baseline before any lockdown was put in place.
- Location data is collected by Google’s location tracking built into the Android operating system.
- They report aggregate data only using differential privacy. Differential privacy adds enough noise so that the noise is greater than the individual contribution to the dataset but not enough to wash out the value of the information in the aggregate data. The result that you see is statistically nearly identical to what it would be if your own data was deleted.

Currently the CSIR’s Information & Cyber Security Centre is carrying out hotspot mapping in partnership with NDoH using randomized aggregate movement data NDoH receives from operators and platform providers. NDoH also receives location data of the position of COVID-19 positive individuals. These

positions are scrubbed before sending to the mapping system by randomizing the position to an area within a 300 m radius (this radius is increased in lower density areas). The CSIR provides the mapping system that uses randomized location data and movement data to produce hot spot maps like the one seen in Figure 1.

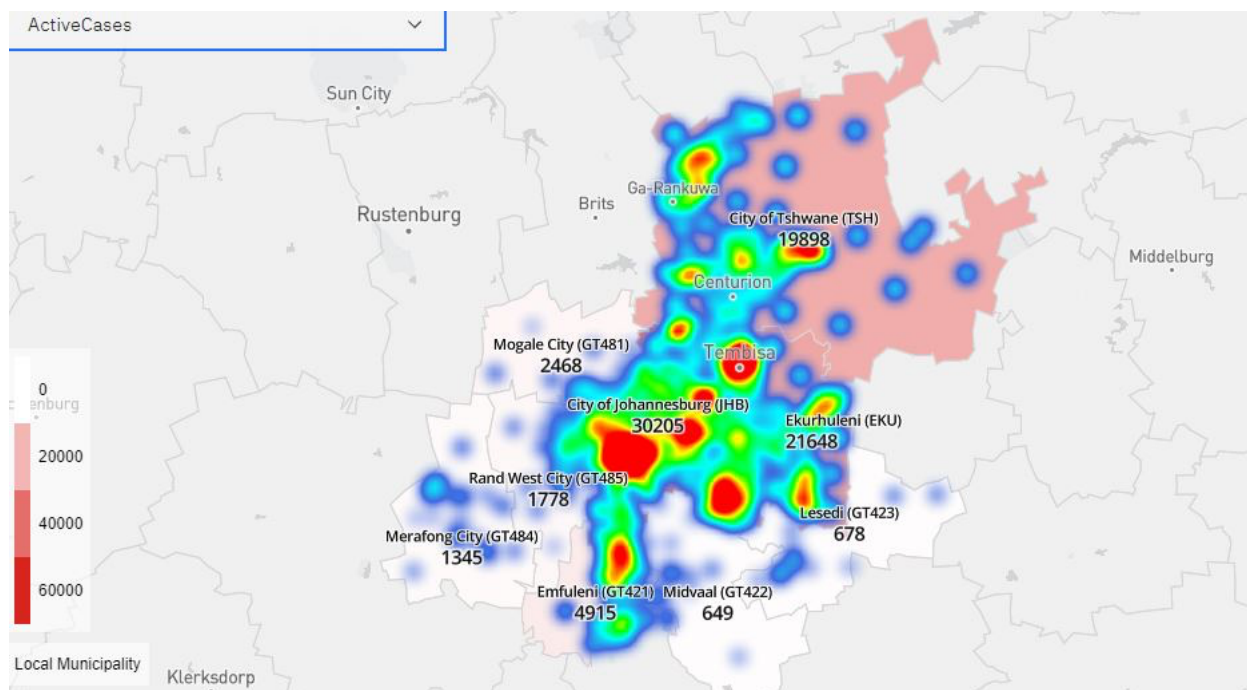


Figure 5. CSIR hotspot mapping system built in partnership with NDoH

9.3. Crowdsourced hotspot mapping

The current Hotspot mapping process uses data which is gathered through a labour intensive process. A free tool conceptualised and developed by Move Beyond Consulting (MBC) uses a crowdsourced online tool to screen millions at any time and any place.¹² The tool also provides a map interface so users and health authorities can look up the spatial distribution of Covid-19 positive screens and thereby remain informed of hotspots in real-time.

Users report their symptoms through a set of self-assessment questions, in line with screening guidelines for covid-19. Users could be individuals reporting their own or a friend's or a family member's symptoms, and any medical practitioner or on-foot screening staff. The tool is readily available for add-on to existing tracing and mapping tools.

¹² <http://www.datavisuals.co.za/miweather/selfassessment.php>

10. Immunity passports

The argument for immunity passports is that certain jobs create higher risk for exposure than normal due to the proximity and length of contact time of these individuals with each other. Having an immunity passport that certifies that you are immune could provide peace of mind and allow the business to operate even when the pandemic continues to have high infection rates. Work environments such as hospitals and hotels individuals such as taxi drivers would be potential candidates.

An immunity passport would be issued to certify that somebody is immune which could be obtained by having the disease and recovering (verified by an antibody test) or receiving a vaccination. The key argument is that it helps an area or country return to economic activity sooner.

There are, however, a number of serious challenges with immunity passports:

- The worldwide average lower bound on the number of those who are immune will be approximately twenty times the number of people who die (estimate established from current world data on number of individuals who have recovered vs number of individuals who have died). For example, if the fraction of the population that die is 0.5%, the immunity will only be 10%.
- It creates an incentive to get the disease as it could allow you to get a job or return to work sooner.
- It provides an incentive to cheat and could create a market for forged immunity passports.
- A major concern is the base rate problem due to the error rates in COVID-19 tests (currently around 5%). The base rate problem occurs when the prevalence, the proportion of those who have a given condition, is lower than the test's false positive rate. Even tests that have a very low chance of giving a false positive in an individual case will give more false than true positives overall.

To illustrate the case for South Africa with a population of approximately 60 million. Let's assume that we reach a 2% immunity level (approximately 1.2 million people who recover and are immune; current recoveries as of 10 September 2020 are 567,000).

	Immunity test positive	Immunity test negative
Actual immunity (1.2M)	1.14M	0.06M
Not immune (58.8M)	2.94M (72% chance not	55.86M

	immune)	
Total	4.08M	55.92M

Table 5. Demonstration of base rate problem for positive and negative immunity tests

The result in Table 5. shows that more of the population are receiving false positive immunity results (2.94M) than those that have true positive immunity results (1.14M). Hence, an immunity passport won't work as the only option is more immunity, which would mean more deaths, or much more accurate tests that are not available in the short term.

11. Data protection considerations

The data protection aspects of contact tracing fall in two categories, weaknesses at point of detection and weaknesses where identity data is stored.

11.1. Weaknesses at point of detection

De-identification fallacy: This is a weakness in any system that is using random identifiers and supposedly conveys no information and therefore has no privacy risk. Simple observation can often easily help identify the person connected to the random identifier. For example, Alice and Bob have lunch at a specific time and day and record each other's random IDs. Later that day Bob's random ID reports as positive. Alice now knows Bob was infected

Paparazzi attack: If you wanted to target a famous or prominent person. You could dedicate a device that obtains their random ID at regular intervals by placing it near them. Eventually you'll be able to check if they are positive, as your dedicated paparazzi device will be notified that it has been in contact with a COVID-19 positive person.

Cloned devices: In this attack, you arrange for many cloned devices to send the same random ID. This could create widespread panic if it was possible to get this cloned ID to report as positive

Bomb threat attack: In this attack, you target one specific area or business by transmitting random IDs in a place, and then reporting as positive to effectively sabotage the business and shut it down.

Bluetooth distance hacking: In order to amplify the impact of any of the above attacks, you can add a high gain antenna to Bluetooth device to extend range and hear many more random IDs or broadcast more random IDs.

The current COVID Alert system used by South Africa makes use of a secret SMS code sent to the individual that tests positive for COVID-19. This secret SMS code has to be entered into the Contact tracing app in order to flag yourself as positive. This system should prevent the bomb threat and cloned device type attacks.

11.2. Weaknesses in stored identity data

Central database of COVID-19 positive patients: This database contains names and addresses of covid-19 positive individuals and their contacts. This data is stored at the DoH, is accessed by health officials and is susceptible to hacks that use social engineering or network attacks.

Data on contacts made by automated contact tracing services:

- GAEN system: This system only stores daily tracing keys of those that self-report as positive. The central server acts as a relay of these tracing keys. The keys look random and have no value should this server get compromised.
- The Cov-ID system stores data using a trusted execution environment (TEE) that is encrypted with the TEE's public key. Data can only be viewed by a third party with the user's consent

Government policy and attitudes towards these potential privacy concerns are diverse. A good summary of potential threats to personal freedoms by Government contact tracing programs is available from Privacy International.¹³

12. Conclusion

In countries, like South Africa, that have a dual economy with high income inequality and unemployment, there is no one-size-fits-all solution to contact tracing. Most automated contact tracing hinges on owning a smartphone and having Internet access but Smartphone ownership and Internet access is limited. Current estimates are that between 49 and 52% of the rural population and between 63 and 69% of the urban population own a smartphone. A national contact tracing system that depends on smartphone ownership alone would leave a large section of population (mostly the low-income portion of the population) locked out of a contact tracing programme.

The ultimate approach will use a combination of multiple contact tracing regimes (manual and automated) that all have an underpinning theme of being privacy-preserving.

The following approach is suggested:

¹³ <https://privacyinternational.org/examples/location-data-and-covid-19>

- Continue with manual contact tracing augmented by the **COVID Connect application** and ensure that the **notification interval does not exceed 2 days** and ensure that checking the status of test outcomes can be carried out in privacy. An external security audit should be regularly carried out on the central database, to ensure it is POPI compliant and the sensitive data is only used for its original intended purpose and is anonymized for research or deleted once the pandemic is over.
- **Rapidly scale up the GAEN-based contact tracing system, COVID Alert**, for users who have smartphones by using a widespread marketing campaign on radio, television and the Internet and as part of a daily COVID-19 cases report. Specifically target the major city centres where exposure risk and smartphone penetration are highest.
- Ensure that **zero-rating of tracing key data** used by the app functions on all South Africa's networks as promised.
- **Translate the app** into all South Africa's official languages to ensure that there are no barriers to uptake.
- Explore mechanisms such as **data rebates**, once the app is installed, to overcome the current technical impossibility of zero-rating the app (3MB) and its library dependency (45MB) download. The data rebate could make use of a code generated by the app to claim a rebate. Providing users with a little more data than is consumed by the app – 100MB, for example - will also provide an added incentive to install it.
- Establish a **contact tracing technology lab** at a neutral organization such as the CSIR or a University to carry out tests on battery drain by the app as well as privacy checks and publish these on the Coronavirus website to put user's minds at ease and combat fake news about the app.
- For users without smartphones, users that don't want to install the GAEN-based application due to security concerns or users who want additional knowledge about potential contacts, deploy the **CoviID system**.
- Continue with **country wide hotspot mapping** (such as the one being run at the CSIR in partnership with NDoH) using randomized locations of individuals who test positive and aggregate movement data from operators and platform providers such as Google. This system can be supplemented with a GAEN-based contact tracing system and the CoviID system to provide a more complete picture of where there are higher risks of infection.
- Use an **incentive scheme** to encourage users and businesses to make use of contact tracing applications. For example, medical aids schemes that have reward programs such as Discovery Vitality and Momentum Multiply that already have some tracking systems for fitness and safety purposes could provide rewards for 14 day self-isolation. For users that are not on these medical schemes, mobile operators could partner with the government to provide data rebates for users that install the app and when self-reporting their status. Tracking users not on private medical aids who haven't opted into their health and safety tracking systems is fraught with privacy concerns and should be avoided.

- Ensure that all deployed systems can **interoperate in a secure manner**. Data formats for contact and location data and security mechanisms for shared data should be agreed on. This will help, for example, provide notifications to individuals where detection of this exposure could have been through manual contact tracing, smartphone-based contact tracing or QR-code-based contact tracing.
- **Cross-border contact tracing** will become critical as South Africa opens up its borders. South Africa should participate in discussions in various regions on how to exchange encrypted tracing keys (Lomas, 2020) of infected individuals to enable travellers who enter the country to be alerted if they were in contact with somebody who tested positive for COVID-19 while outside the country.

Time barriers to implementation are often more political than technological. It may take time to agree on a protocol for providing test verification codes that can securely provide confirmation of test status to multiple applications without revealing personal information. The Protection of Personal Information Act 4 of 2013 (POPIA), which finally came into force on 1 July 2020 can be used as the guiding principle for this purpose. Contact tracing creates another political challenge - it allows certain sectors of the economy to open up and others not. For example, more crowded businesses districts in the city may need to temporarily close whereas less dense suburban businesses may be able to stay open. This will need to be managed very sensitively.

It is also critical to have oversight to develop and enforce privacy guidelines for these technologies and continually review the impact in real-world situations. In South Africa, a judge has been appointed for this purpose, but civil society organisations, community groups and social movements should also continue to keep a close watch on how sensitive data collected from contact tracing systems is used and disseminated.

The challenges of zero-rating sites and health apps like COVID Alert and the lack of access for many low-income users who are required to stay home and continue to be economically active or continue their education provides strong motivation for a free basic data rate service in South Africa. This basic data rate service would provide always on, low-bandwidth access for all South Africans on any operator network and ensure that a basic level of access to critical digital services is always available.

Given that many of these recommendations will take time to put in place and implement, it would be prudent to implement these without delay to at least attempt to contain any further new waves of the COVID-19 pandemic and to contain new pandemics that will occur in the future. But, equally importantly, we also need to constantly guard against abuse of our civil liberties by an increasingly securitized state during the pandemic.

Author contact details

Name:	Dr David Johnson
Tel:	+27 21 782 3420
e-mail:	djohnson@cs.uct.ac.za
Mobile:	+27 72 522 1740

13. References

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Bonsall, D. G., & Fraser, C. (2020). Quantifying dynamics of SARS-CoV-2 transmission suggests that epidemic control and avoidance is feasible through instantaneous digital contact tracing. MedRxiv preprint, March 12, 2020. doi: 10.1101/2020.03.08.20032946.

GeoPoll. (2020, February). Smartphone Usage And Data Costs In South Africa. <https://www.geopoll.com/resources/south-africa-smartphone-internet-usage/#result>

Gillwald, A., & Mothobi, O. (2019). A Demand-Side View Of Mobile Internet From 10 African Countries (Policy Paper No. 7; Series 5: After Access – Assessing Digital Inequality in Africa). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

Hart, V., Siddarth, D., Cantrell, B., Tretikov, L., Eckersley, P., Langford, J., Leibrand, S., Kakade, S., Latta, S., Lewis, D., & others. (2020). Outpacing the virus: Digital response to containing the spread of covid-19 while mitigating privacy risks. COVID-19 Rapid Response Impact Initiative, White Paper, 5.

Howell O'Neill, P. (2020, May 7). India is forcing people to use its covid app, unlike any other democracy. MIT Technology Review. <https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/>

ICASA. (2020). The State of the ICT Sector Report in South Africa. Independent Communications Authority of South Africa. <https://www.icasa.org.za/uploads/files/State-of-the-ICT-Sector-Report-March-2020.pdf>

Johnson, B. (2020, May 11). Nearly 40% of Icelanders are using a covid app—And it hasn't helped much. MIT Technology Review. <https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing/>

Labuschagne, H. (2020, August 1). Major concerns over South Africa's COVID-19 contact tracing. My Broadband. <https://mybroadband.co.za/news/software/361219-major-concerns-over-south-africas-covid-19-contact-tracing.html>

Lomas, N. (2020, September 14). Europe starts testing app interoperability service to power cross-border COVID-19 exposure alerts. TechCrunch. <https://techcrunch.com/2020/09/14/europe-starts-testing-app-interoperability-service-to-power-cross-border-covid-19-exposure-alerts/>

Oxford. (2020, April 16). Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. University of Oxford. <https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown>

Rahman, M. (2020, October 7). Here are the countries using Google and Apple's COVID-19 Contact Tracing API. XDA. <https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/>

Silver, L., & Johnson, C. (2020, October 9). Majorities in sub-Saharan Africa own mobile phones, but smartphone adoption is modest [Pew Research Centre]. Global Attitude and Trends. <https://www.pewresearch.org/global/2018/10/09/majorities-in-sub-saharan-africa-own-mobile-phones-but-smartphone-adoption-is-modest/>

Wamslet, L., & Selena, S.-D. (2020, April 1). The Science Behind A 14-Day Quarantine After Possible COVID-19 Exposure. NPR. <https://www.npr.org/sections/health-shots/2020/04/01/824903684/the-science-behind-a-14-day-quarantine-after-possible-covid-19-exposure>

Appendix A: List of countries using GAEN

Obtained from XDA Developers (<https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/>) on 31 August 2020.

Region	App Name	Android Package Name	Status
Australia	COVIDTrace	au.gov.dta.covidtrace	In-Development
Austria	Stopp Corona	at.rotekreuz.stopcorona	Released
Belgium	–	be.sciensano.coronalert	In-Development
Brazil	Coronavirus – SUS	br.gov.datasus.guardioes	Released
Brunei	BruHealth	egnc.moh.bruhealthtrace	Testing ENS
Canada	COVID Alert	ca.gc.hcsc.canada.stopcovid	Released
Croatia	Stop COVID-19	hr.miz.evidencijakontakata	Released
Czech Republic	eRouška	cz.covid19cz.erouska.dev	In-Development
Denmark	Smittestop	com.netcompany.smittestop_exposure_notification	Released
Ecuador	ASI	ec.gob.asi.android	Released
Estonia	Hoia	ee.tehik.hoia	Released
Finland	Koronavilkku	fi.thl.koronahaavi	Released
Germany	Corona-Warn-App	de.rki.coronawarnapp	Released
Gibraltar	Beat Covid Gibraltar	com.gha.covid.tracker	Released
Guam	Guam Covid Alert	org.pathcheck.guam.bt	Released
Ireland	Covid Tracker	com.covidtracker.hse	Released
Italy	Immuni	it.ministerodellasalute.immuni	Released
Japan	COCOA – COVID-19 Contact App	jp.go.mhlw.covid19radar	Released
Kazakhstan	eGov bizbirgemiz	kz.nitec.bizbirgemiz	In-Development
Kenya	–	ke.go.health_togethertrace	In-Development
Latvia	Apturi Covid Latvia	lv.spkc.gov.apuricovid	Released
Malta?	–	mt.gov.dp3t	In-Development

Mexico	COVID-19MX	mx.gob.www	Testing ENS
Netherlands	CoronaMelder	nl.rijksoverheid.en	Released
Northern Ireland	StopCOVID NI	net.hscni.covidtracker	Released
Philippines	StaySafe PH	ph.staysafe.mobileapp	Testing ENS
Poland	ProteGO Safe	pl.gov.mc.protegosafe	Released
Portugal	STAYAWAY COVID	fct.inesctec.stayaway	Released
Saudi Arabia	Tabaud	sa.gov.nic.tabaud	Released
Scotland	–	gov.scot.covidtracker	In-Development
Slovenia	OstaniZdrav	si.gov.ostanizdrav	Released
South Africa	COVIDConnect	za.gov.health.covidconnect	Released
Spain	Radar COVID	es.gob.radarcovid	Released
Switzerland	SwissCovid	ch.admin.bag.dp3t	Released
United Kingdom	NHS COVID-19	uk.nhs.covid19.production	Released
Uruguay	Coronavirus UY	uy.gub.salud.plancovid19uy	Released
USA – Alabama	GuideSafe	gov.adph.exposurenotifications	Released