EMERGING ISSUES IN DIGITAL ID PART 2

MOBILE LOCATION DATA TO TRACE & MONITOR COVID-19 CASES

A Use Case and Issue Brief
Prepared by CIPIT

Strathmore University

Centre for Intellectual Property and Information Technology Law

01

BACKGROUND

Amid the COVID-19 pandemic, governments are increasingly seeking technological solutions to prevent the virus from spreading further. Geo-location-based technologies, that are able to track mobile phones, could ease the tracing of movements of COVID-19 positive patients and those they may have come into contact with.

Already, South Africa, Austria, Italy, Israel, Iran, South Korea, Singapore, Taiwan, the USA, and others have authorised the use of location data obtained from telecommunications providers and tech platforms for contact tracing.[1] The sourcing of the location data is reliant on cell tower signals, Bluetooth Low Energy (BLE) and Global Positioning System (GPS).

The location data may also be used for: monitoring compliance with quarantine and social distancing orders; analysing general patterns of the movements and behaviours of the public or; marking hot spots.[2] Some countries, like South Africa, are planning to cross-reference the location data against personal information such as names, ID numbers, addresses, phone numbers and test results registered in mobile apps or big data systems to track exposed persons.[3]

While this solution is arguably critical to combat COVID-19, the implementation of these digital contact tracing systems creates surveillance infrastructures that have the potential of being used in a manner that violates the rights and freedoms of natural persons, if not well monitored.

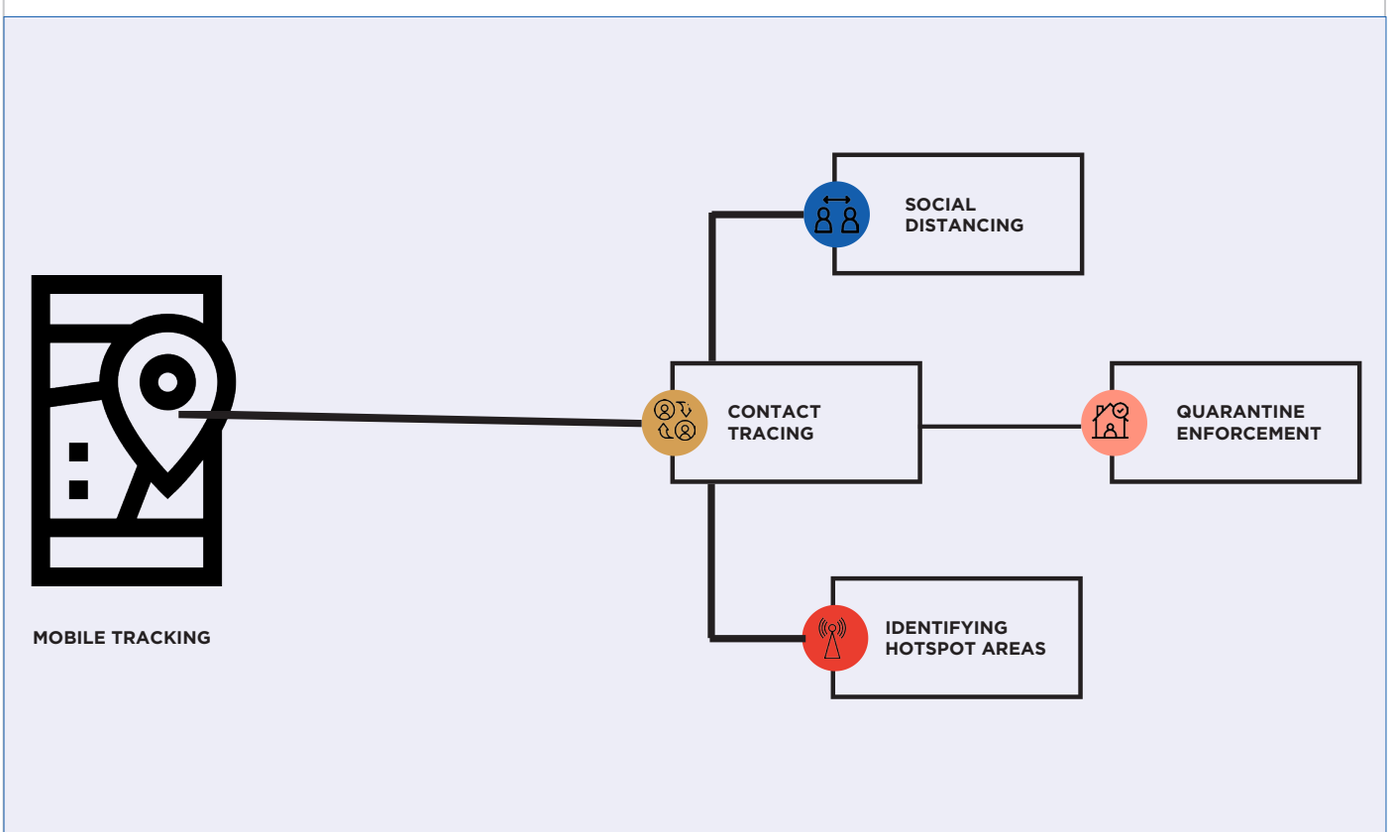


Fig1. Mobile Tracking Visual

JUSTIFICATIONS FOR THE USE CASE

In the use case of mobile tracking to monitor COVID-19 cases, the issues raised for which Digital ID has been proposed as a solution are:

1. Contact tracing.
2. Aid the monitoring and enforcement of social distancing.
3. Quarantine enforcement.
4. Use of data by health officials to identify COVID-19 hotspot areas.

DATA INVOLVED IN THE USE CASE

The data collected for Digital ID in the use case of mobile tracking to monitor COVID-19 cases may include:

1. Location, including physical proximity to other people and any known infected individuals.
2. Individual's contact lists.
3. Individual's identification information e.g. names, addresses, etc.
4. Health records e.g. COVID -19 test results.

RISKS INVOLVED IN THE USE CASE

The risks associated with the use of mobile tracking to monitor COVID-19 cases may include

1. Violation of the fundamental right to privacy.
2. Indiscriminate use of subjects' location for purposes not specified and/or intended.
3. Use of the data by the government for purposes that are not consistent with human rights norms.

[1] CIPESA, (2020) 'Covid-19 in Africa: When is Surveillance Necessary and Proportionate?'
<https://cipesa.org/2020/03/covid-19-in-africa-when-is-surveillance-necessary-and-proportionate/>

[2] Human Rights Watch(2020) ,'Mobile Location Data and Covid-19: Q&A
<https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa> .

[3] Dyer L,(2020)'COVID-19: TRACING CONTACTS' Bowmans Blog.
<https://www.bowmanslaw.com/insights/technology-media-and-telecommunications/covid-19-tracing-contacts/>

02

ANALYSIS

Unlike the United States, most countries in Africa do not allow anonymous operation of mobile devices. It is a legal requirement to supply an official ID in order to register a SIM. Thus, the location of any given mobile device can be connected, in theory, to the individual that owns the SIM. While this ought to increase the feasibility of mobile contact tracing in much of Africa, other factors are influential. GPS-enabled smart phones are relatively less common in many parts of Africa, and triangulation of cell signals for feature phones is significantly less effective. Behavioural factors are also important: it is known that individuals are not always physically located with their registered SIM – loaning of phones or owning multiple SIMs are common practices in many parts of Africa, and such behaviours would reduce the accuracy of mobile tracking.

Given the above factors, mobile tracing is likely to be more effective for containing isolated cases of a viral infection, but is unlikely to be as effective if the virus enters the general population. Where mobile tracing is used, important questions are raised particularly around data protection.

Data protection rules across the world generally allow for the release of personal information to government authorities even without the knowledge or consent of data subjects in the interest of safeguarding public health. Preventing the spread of COVID-19 is, no doubt, a public interest that may outweigh privacy concerns arising from the use of contact tracing systems. All the same, governments' technological responses for tracing COVID-19 need not to be abused at the expense of data subjects' rights. Key questions that arise from the use of the contact tracing systems include: What data is collected? Who is collecting data? How is data used? With whom can the data be shared? and; How long should the data be stored?

The collection and analysis of the collected data could reveal a people's attributes in a manner that is invasive to their privacy. Location data, for instance, could reveal a person's identity, location, behaviour, associations, and activities.[4] This information can be abused if it falls into the wrong hands. This data, if stored in a centralised system, also may not be secure as it may be hacked.

Similarly, the collection and processing of health data and particularly the publication of information online, poses risks to the safety of affected persons. Persons that test positive for COVID-19 may experience harassment or social stigma depending on how much information is revealed to the public.[5]

While the digital contact tracing systems are currently intended to prevent COVID-19 from spreading further, a lack of clarity on the specific purposes for which personal data may be used, by whom it may be used and for what period it may be stored, could be taken advantage of by governments who may extend the use of the collected data for other unnecessary purposes, post the pandemic.

As will be discussed later in the case study, some of these safeguards to ensure that the personal data is properly handled are incorporated in South Africa's regulations.

[4] Human Rights Watch (2020) ,'Mobile Location Data and Covid-19: Q&A <https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa> .

[5] Human Rights Watch(2020) ,'Mobile Location Data and Covid-19: Q&A <https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa>

GOOD ID PRINCIPLES IN THE USE CASE

1. Transparency and oversight in the data collection and data sharing.
2. Clarity on purpose limitation.
3. Checks on the implementation of any policies and the protection of the right to privacy and other fundamental freedoms and rights.
4. Mitigate any risk of enabling discrimination or other rights abuses against marginalized populations.
5. Protection and safeguards against indiscriminate surveillance.
6. Controlled and authorised access of the database system.
7. Anonymized personal information before sharing.
8. Clear data storage directives.
9. Technical and operational safeguards put in place to ascertain the security of the database system and confidentiality of personal information collected and shared.
10. Use of a decentralized database as opposed to a centralized one that is far more exposed to higher risk of cyber-attacks.

Fig2. Good ID Principles

03

CONCLUSION

While digital COVID-19 contact tracing may be useful for the rapid tracing of persons exposed to the virus, governments' use of digital identity systems that centralize sensitive personal information are a big trade-off on the privacy of persons and have the potential of being misused. For these reasons, it is important for governments to commit to ensuring that their digital contact tracing systems adhere to legal standards and that those processing the data are accountable.

ACKNOWLEDGEMENTS

This work is part of #GoodID, a Global South project funded by Omidyar Network.
For more information please visit www.cipit.strathmore.edu and www.good-id.org

04

ADDENDUM: SOUTH AFRICA AS A CASE STUDY

On 25th March 2020 in a bid to control the rise of COVID-19 cases in South Africa, the Minister of Telecommunication and Postal services Stella Ndabeni-Abrahams, announced the use of cell-phone tracking to retrieve data that would be used to curb the fast spreading virus. The announcement was followed by the gazettement of the Disaster Management Regulations that would allow mobile phone tracking.

The announcement and consequent regulations were met with unrest and uncertainty with many South Africans raising concerns about the government's interference with their right to privacy by accessing their cell phone data which would include their locations and contact lists. The regulations directed:

> *"The Electronic Communication Network Service (ECNS) and Electronic Communication Service (ECS) Licensees, internet and the digital sector in general, must provide location-based services in collaboration with the relevant authorities identified to support designated departments to assist and combat the spread of Covid-19."*

South African legal experts and civil society organizations raised concerns as to the implementation of the regulations as a reading of the regulation suggested the forceful handing over of location based data from the various telecommunication agencies in South Africa. Digital rights activist Murray Hunter while addressing the implications of the regulations described the regulations as being vague and lacking in transparency and oversight. These concerns were widely shared as the regulations at best failed to address key data protection principles and the implications of mobile phone tracking particularly in respect to the protection of the right to privacy and the likelihood of interference with other human rights.[6]

The vagueness and uncertainty, particularly the indiscriminate surveillance of South African citizens by their government led to an amendment to the regulations through a gazette published on 2nd April 2020. The regulations provided for a clear understanding of contact tracing through cell-phones as well the data that would be collected, how it would be used and the storage.

The regulations provided for the establishment of a COVID-19 tracing database to be established by the National Department of Health enabling the tracing of persons who are known or reasonably suspected of to have come in contact with a person known or suspected to have contracted COVID-19. The tracing data base would have all information deemed necessary for the contact tracing and would include:

- The first name and surname;
- Identity or passport numbers;
- Residential address and other address where such person could be located;
- Cellular phone numbers of all persons who have been tested for COVID-19;
- The COVID-19 test results of all such persons; and
- The details of the known or suspected contacts of any person who tested positive for COVID-19.

The regulations further address checks to ensure that all information stored in the database is confidential and only accessible to persons authorized and where the disclosure is necessary for the purpose of addressing, preventing or combatting the spread of COVID-19. In specifically addressing cell phone tracking, the regulations were amended to read:

The Director-General: Health may, in writing and without prior notice to the person concerned, direct an electronic communications service provider licensed under the Electronic Communications Act, 2005 (Act No. 36 of 2005) to provide him or her, for inclusion in the COVID-19 Tracing Database, with such information as that electronic communications service provider has available to it regarding: -

(a) The location or movements of any person known or reasonably suspected to have contracted COVID-19; and

(b) The location or movements of any person known or reasonably suspected to have come into contact, during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated, with a person contemplated in subparagraph (a), and the electronic communications service provider must promptly comply with the directive concerned.

The amendment addressed a body of accountability being the Director General health and equally addressed transparency through specifying the period for which the data collected through tracing of cell phones would be used. Further to this the information held in the COVID-19 tracing database can only be held by the Director General –health for a period of six weeks and thereafter destroyed.

Although the amendment to the regulations are a welcome step in the right direction where the government is intent on relying on cell phone tracking to curb the spread of COVID-19, a few challenges are still noted particularly on implementation, the assured confidentiality of the database, technical and organizational measures and the potential risk of breach as the database holds wide personal information in a centralized database system.

Oversight of the entire system to ensure the right to privacy and other human rights are protected was secured through the appointment of retired Judge of the Constitutional Court Kate O'Reagan. The judge is tasked with making recommendations on the amendments to contact tracing and the enforcement of the regulation while ensuring the Department of Health is able to engage in urgent and effective contact tracing to curb the spread of COVID-19.[7]

South Africa fast embraced the concept of mobile tracking to aid contact tracing borrowing from countries like South Korea and Germany who have been applauded for managing the spread of the virus effectively. Globally, there are 47 contact tracing apps in use with 53% of the apps using GPS data, 15% using Bluetooth and 28% using both GPS and Bluetooth. 11 apps (23%) have no privacy policy. 25 apps (53%) do not disclose how long they will store users' data for and 28 apps (60%) have no publicly stated anonymity measures.[8]

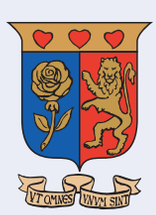
Whereas we understand the need for governments to try and get ahead of the pandemic and the use of all resources that are likely to restrict human rights for health reasons it is important to ensure that human rights are taken into consideration and the measures taken to limit these freedoms and rights are law full, necessary and proportionate. These same rules ought to apply in all measures being taken especially in the tracking and consequent management of COVID-19 cases using mobile location data.[9]

---

[6] Elri Voight (2020), 'Covid-19: Progress on Cell Phone Tracking.' City Press
<https://www.news24.com/citypress/News/covid-19-progress-on-cell-phone-tracking-but-concerns-remain-20200406>

[7] Top10VPN. 'Covid-19 Digital Rights Tracker.'
< https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/>

[8] Human Rights Watch, 'Mobile Location Data & Covid 19.' < https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa>



Ole Sangale Rd, Madaraka Estate.
PO Box 59857 00200, Nairobi, Kenya | Tel +254 (0)703 034 612
Email: cipit@strathmore.edu | Website: https://cipit.strathmore.edu