NORTON ROSE FULBRIGHT

Contact tracing apps in South Africa

A new world for data privacy

As of May 11, 2020

The COVID-19 pandemic has seen governments across the world restricting civil liberties and movement to new levels. To aid the safe lifting of current public health restrictions, new technologies are being developed – contact tracing apps – and rolled out to automate labour intensive tasks critical to containing the spread of the virus. Our contact tracing survey summarises the principal regulatory and policy issues applicable to contact tracing across a range of key jurisdictions in real time.

Is technology being used by the government to monitor and control the spread of COVID-19 (e.g. contact tracing app, CCTV, cell phone location data, credit-card history)?

The South African government has partnered with the University of Cape Town to develop a smartphone app to assist government with tracking people who may be unaware that they have COVID-19 and to track people who have come into contact with others who are COVID-19 positive. The App is called Covi-ID.

The South African Government acknowledged that it is critical that the Government works collaboratively with South African technology companies and individuals to leverage technology capabilities in the fight against COVID-19 and its effects.

We are aware that the Government has approached technology companies to identify suitable projects that may assist the Government with its response to the crisis, in particular, its plan to develop a national COVID-19 Tracing Database. The database seeks to track people who are known or suspected to have come into contact with persons known or suspected to have COVID-19.

On 2 May 2020, the Department of Health also launched a Whatsapp based symptom reporting process. The details of the back end and privacy controls are unknown at this stage.

What are considered to be the major privacy concerns in relation to the app in your jurisdiction (in relation to its use (a) by the government; and (b) by private sector organisations)?

Given that South African privacy laws are not yet in force, there is a concern that personal information may not be properly protected during the pandemic and may be used for further processing not anticipated on collection of the data. On the WhatsApp symptom tracker it is unclear who is processing the information submitted and where else it may be disclosed. There are no terms and conditions available regarding the use of this functionality.

Even though South African privacy laws are not in place, there is a constitutional right of privacy; however this may be infringed where there are larger public interest considerations that outweigh the impact on privacy.

The Covi-ID App has a GDPR-based privacy policy and also voluntarily submits to the South African data privacy laws not yet in place.

App details

1. **What is the name of app**

   Covi-ID

2. **Is the app voluntary?**

   Yes

   It is voluntary at this stage. However it may be used by employers or healthcare practitioners in future.

   The WhatsApp-based platform is entirely voluntary.

3. **Is there any suggestion that use of the app and a clean result may be necessary to enter workplaces or any commercial or public buildings (or is this explicitly or implicitly prohibited)?**

   Unknown

   It appears that organisations can sign up to the App for employee testing. However this is voluntary. The App appears to be designed specifically to protect the privacy of individuals in that it generates an infection status by a QR code which can then be scanned and read by a healthcare practitioner or employer.

4. **What information is required to register for the app? Is the information collected considered excessive?**

   Unknown

   Yes personal information is required. Covi-ID app will collect a user's personal location and infection status, and store it on their phone using a technology called self-sovereign identity – not on a centralised government or private-sector database. This provides the user with full authority and control over who gets access to the data, for what purpose and for how long.

5. **Is GPS or Bluetooth used?**

   Bluetooth and Geolocation

6. **Is data stored on a centralised server?**

   No

   The Covi-ID app will collect users' personal locations and their infection statuses, and store the data on individual's phones using a technology called self-sovereign identity– not on a centralised government or private-sector database.

7. **Does the identity of the infected user get captured centrally?**

   No

8. **Is the identity of the infected user disclosed to proximate users or public health authorities? Is it disclosed to anyone else?**

   No

   The user has authority and control over who has access to the data, the purpose for which it is used and for how long the authority has access to it.

   From the above, it is our understanding that the user is in control of whether or not their data is shared with public health authorities.

9. **Is consent needed to share data with other users/ upload the data to a centralised system?**

   Yes

   The user has authority and control over who has access to the data, the purpose for which it is used and for how long the authority has access.

10. **Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?**

    Uxnknown

11. **Does the app incorporate "privacy by design" and was a privacy risk assessment completed?**

    Privacy by design: Yes
    Risk Assessment: Unknown

    The app uses blockchain technology, which helps to ensure protection of privacy. There are reportedly measures in place to reveal only the most necessary information.

12. **How long will the data be kept for, are there clear lines around timing?**

    Unknown

13. **Has data security been addressed expressly (e.g. encryption)?**

    Unknown

14. Are there clear limitations regarding who may have access to the data?

Yes

The Covi-ID app user has authority and control over who has access to the data.

The information contained on the COVID-19 Tracing Database is to be kept confidential. No person may disclose any information contained in the COVID-19 Tracing Database or any information obtained through regulation 8 of the amended Disaster Management regulations, unless authorised to do so and unless the disclosure is necessary for the purpose of addressing, preventing or combatting the spread of the virus.

15. Are there clear limitations on the purposes for which the government may use the data?

Yes

A responsible party may further process personal information of a data subject, notwithstanding the fact that such processing is not compatible with the original purpose for which it was collected, if it is necessary to prevent a serious and imminent threat to public safety or public health, the life or health of a data subject or another individual. This exception also applies if the information is used for historical, statistical or research purposes.

16. Is the government of your country bound by privacy laws in respect of the contact tracing data?

No

The Protection of Personal Information Act is not yet in force. However the Information Regulator has published a guidance note as previously mentioned.

Regulation 8 of the amended Disaster Management regulations, gazetted on 2 April 2020, further indicates how the information collected and contained on the COVID-19 Tracing Database is to be processed.

17. Has the regulator commented/ provided guidance on the technology?

Yes

The Information Regulator has published a guidance note to public and private bodies and their operators on the limitation of the right to privacy when processing personal information of data subjects for the purpose of containing the spread and reducing the impact of COVID-19 and this would regulate the sharing process.

18. Are there any private sector initiatives you are aware of to use/ integrate the app or the information from the app (e.g. to reflect the results back to workforces)?

N/A

Contacts

Rosalind Lake
Director
Durban
Tel +27 31 582 5816
rosalind.lake@nortonrosefulbright.com

Chris Cwalina
Global Co-Head of Data Protection, Privacy and Cybersecurity
Washington DC
Tel +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Marcus Evans
Head of Data Protection, Privacy and Cybersecurity, Europe
London
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Ffion Flockhart
Global Co-Head of Data Protection, Privacy and Cybersecurity
London
Tel +44 20 7444 2545
ffion.flockhart@nortonrosefulbright.com

Anna Gamvros
Head of Data Protection, Privacy and Cybersecurity, Asia
Hong Kong SAR
Tel +852 3405 2428
anna.gamvros@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Law around the world
nortonrosefulbright.com