Contact tracing apps in United Arab Emirates

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 UAE’s Department of Health has launched a new COVID-19 tracing app called TraceCovid to “test, treat and track” as an effective measure to prevent the spread of infectious diseases. The app identifies people who have been in close contact with infected individuals, allowing authorities to immediately reach out to possibly infected individuals and provide them with the necessary healthcare treatments. The Department of Health Abu Dhabi invited members of the public to download the app to help authorities track potential infections.

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)?

There is no Federal data privacy regulator or regulations/laws in the UAE so no comments from any such authority exists. The Government has not provided too much information on what measures and actions it is using to ensure data privacy. The Department of Health Abu Dhabi only said that privacy of personal information will be protected - there is therefore a concern that personal data collected may not be properly protected during the pandemic and may be used for further processing that was not anticipated.

App details

1. What is the name of app
   TraceCovid

2. Is the app voluntary?
   Yes

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)?
   No
   So far no but things are changing every day in the UAE and unilateral decisions such as these can be taken and imposed overnight by way of ministerial decision.

4. What information is required to register for the app? Is the information collected considered excessive?
   Yes
   User’s mobile number needs to be provided.

5. Is GPS or Bluetooth used?
   Bluetooth and Geolocation
   Bluetooth and location service access (GPS) need to be activated for the app to function effectively.
6. Is data stored on a centralised server?
Unclear

7. Does the identity of the infected user get captured centrally?
Unclear
Authorities say that “the app works by exchanging a Secure Tracing Identifier (STI) to track people's movements anonymously” but no details or more information has been provided so far.

8. Is the identity of the infected user disclosed to proximate users or public health authorities? Is it disclosed to anyone else?
No
TraceCovid is a mobile app that uses Bluetooth to pick up signals from nearby mobile phones that also have the app installed, through a process called contact tracing. The app on both the devices will exchange an encrypted Secure Tracing Identifier (STI) and store it on the devices. The STI in each device will, therefore, be a list of all persons in close contact with the user. When one of the users is infected with the virus, the authorities will request the infected user to upload the list of STI stored on his or her device. Also, a user who has tested positive can contact the authorities to share details of STI.

9. Is consent needed to share data with other users/up upload the data to a centralised system?
Unclear
According to the description provided by the authorities no consent is required but there is an understanding that by downloading the app the relevant person understands that her/his data may be disclosed to the authorities as explained in response to Question 8 above.

10. Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?
No
The app on both the devices will exchange an encrypted Secure Tracing Identifier (STI) and store it on the devices. The STI in each device will, therefore, be a list of all persons in close contact with the user.

11. Does the app incorporate “privacy by design” and was a privacy risk assessment completed?
Unclear

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

13. Has data security been addressed expressly (e.g. encryption)?
Unclear
The relevant authorities have only stated that the privacy of personal data will be protected.

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

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

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

17. Has the regulator commented/ provided guidance on the technology?
There has been a press release and there is a dedicated website: https://tracecovid.ae/.

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)?
Not that we are aware of.
Contacts

Adjou Ait Ben Idir  
Partner  
Dubai  
Tel +971 4 369 6393  
adjou.aitbenidir@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