

Contact tracing apps in Indonesia

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 Ministry of Information and Communication (MOCI) launched a mobile application called PeduliLindungi. The app enables users to compile data related to the spread of COVID-19 in their communities to help bolster the Indonesian Government's efforts to trace and track confirmed cases. Users are expected to register as participants and share their locations when travelling and also trace whether they have had contact with persons exposed to COVID-19. The app will also alert users entering crowds or COVID-19 red zones, namely locations where there are confirmed COVID-19 cases.

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)?

That said, the Government has not been very transparent on what measures or methods it is using to ensure protection of data privacy. For instance, the app mentions that it will have periodic updates to improve security and privacy. Whilst the private sector has conveyed privacy concerns, there has not been any major privacy incidents reported thus far.

App details

1. What is the name of app

PeduliLindungi

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

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

Yes

To register, a user's full name and mobile number is required.

5. Is GPS or Bluetooth used?

Bluetooth and Geolocation

6. Is data stored on a centralised server?

Unclear

The Indonesian Government does not specify where data is stored. However, normally central government (such as MOCI) launched applications use data centralised servers. Given the data involved here is considered as national strategic data, the data will need to be stored in Indonesia.

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

Unclear

However, given that the app is run by MOCI, it would be safe to assume that the identity will be captured centrally.

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

Yes

The app will record data proximity of one mobile phone to another in an encrypted format. Mobile numbers registered will be related to random IDs in a secured server and the user's data will not be disclosed to any third parties except when a user is identified to be in a risk of being infected. In such a case, the data will be disclosed to public health authorities who will contact potentially infected users.

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

Unclear

The app does not clearly specify whether consent is needed to share or upload data. However, in Indonesia, any transfer of personal data must be consented to by the data owner. The form of consent could also be obtained when users agree to register to the application.

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

Yes

As discussed above, the disclosure will be limited only if there are apparent risk of infection.

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

Unclear

There is no public information as to the degree of privacy risk assessment carried out.

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

Unclear

This is also not specified.

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

Yes

When launching the app, the Indonesian Government has expressly dealt with issues concerning data privacy and security through the use of encryption (for PeduliLindungi).

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

No

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

No

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

Yes

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

Yes

Yes, a number of public announcements have been made by MOCI on the use of PeduliLindungi.

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)?

No

Contacts



Shamim Razavi

Partner

Sydney

Tel +61 2 9330 8806

shamim.razavi@nortonrosefulbright.com



Ffion Flockhart

**Global Co-Head of Data Protection,
Privacy and Cybersecurity**

London

Tel +44 20 7444 2545

ffion.flockhart@nortonrosefulbright.com



Chris Cwalina

**Global Co-Head of Data Protection,
Privacy and Cybersecurity**

Washington DC

Tel +1 202 662 4691

chris.cwalina@nortonrosefulbright.com



Anna Gamvros

Partner

Hong Kong SAR

Tel +852 3405 2428

anna.gamvros@nortonrosefulbright.com



Marcus Evans

**Head of Data Protection, Privacy and
Cybersecurity, Europe**

London

Tel +44 20 7444 3959

marcus.evans@nortonrosefulbright.com