Contact tracing apps in France

A new world for data privacy

As of May 22, 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 app, StopCovid, has been developed by INRIA (National Institute for Research in Digital Science and Technology). Tests are still in progress and the French Government is hoping to launch the app in early June.

Parliamentary debates will be held on 27 May.

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)?

The CNIL has stressed that the collection and storage of data should be limited to that which is strictly necessary for the use of the app (for example, the app cannot collect geolocation data), and for a limited period of time. The data must be deleted when the app is no longer in use. However, it is impossible to estimate such a duration.

The other main risks raised include:

- The use of a centralized server increases the risk of possible cyber-attacks and the temptation to exploit this data for purposes other than those provided for by law.
- Discrimination – people who do not use the app might not be able to work or access certain public places freely, meaning their consent was not freely given and therefore is void.
- Surveillance – in the event that the app is adopted by part of the population, it is feared that the French Government may more easily impose it on the rest of the population against their will. Moreover, the app is not based on pure anonymization – it is at best pseudonymous, which does not protect against any kind of individual surveillance.
- Security acclimatization – once the app is deployed, it will be easier for the French Government to add coercive functions to it (individual control of lockdown). Moreover, the app provides an incentive to subject one’s body to constant surveillance, which will reinforce the social acceptability of other technologies, such as facial recognition or automated video surveillance, which are currently widely rejected.
App details

1. What is the name of app

StopCovid

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

The French data protection authority (“the CNIL”) states in its opinion of 24 April, 2020, that the “voluntary” mode of the app implies that no negative consequences can be associated with a person’s refusal to use the app. Thus, screening tests, care, the ability to travel, access to certain services (e.g. public transport) cannot be made conditional on the use of StopCovid. The CNIL expressly refers to employers, who may not subordinate certain rights to the use of this app, as this would amount to discrimination.

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

No

No information will be needed to register the app. However, according to the CNIL, this could result in an increased risk of cyber-attack. It therefore calls for appropriate security measures to be implemented.

The app will generate ephemeral crypto-identifiers (e.g. every 15 minutes) associated to the terminal (and not the person).

5. Is GPS or Bluetooth used?

Bluetooth

6. Is data stored on a centralised server?

Yes

The app will record the crypto-identifiers of smartphones encountered during a trip. When a user indicates to the app that he/she is contaminated, the app sends the history of encountered crypto-identifiers to a central server (the one of a health authority – which one is yet to be confirmed), without disclosing its own crypto-identifiers.

Each smartphone that has downloaded the app regularly checks with this central server to see if its crypto-identifiers are among those at risk. If they are, the app will generate an alert sent to the user, to indicate that he/she might have been exposed to the virus, and the measures to be taken.

However, this decision has been the subject of much criticism. It has been abandoned in Germany, which opted for a decentralized system.

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

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

Yes

If a person is tested positive by a health authority and if this person wishes to inform the app with this updated status, the history of crypto-identifiers of smartphones which have had contact will be automatically shared with the central server. The smartphones (and their owners) will receive an alert without knowing the identity of the person infected.

No data is shared with other users.
10. Is the identity of the proximate users disclosed to public health authorities? Is it disclosed to anyone else?

No

Only crypto identifiers of the proximate users would be disclosed on the central server – and no one else. However the CNIL considers that in order to be able to inform a user of a possible exposure to the virus, the central server must check if there is a match between the pseudonyms attributed, at the time of its installation, to the application of this user and those that have been transmitted to the central server by the app of another person recognized as positive. The result is that there remains a link between the pseudonyms and the downloaded applications, each application being itself installed on a terminal, which generally corresponds to a specific natural person.

As a result of this link, the Commission considers that the device will process personal data within the meaning of the GDPR.

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

Recommended

The CNIL recommended that a PIA is carried out prior to the implementation of the scheme as the processing is likely to present high risks (health data, large-scale use, systematic monitoring, and use of a new technological solution).

According to INRIA and the French Government, the app incorporates privacy by design (notably in terms of security, consent, data minimization, transparency and data retention period).

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

Yes

Crypto-identifiers that are no longer relevant from an epidemiological point of view will be deleted every 15 days. At any time, the user can delete their data which will permanently erase all information uploaded to the server. When deleting the application from the smartphone, the user’s data in the application will also be deleted.

The app itself is not intended to last beyond the health crisis.

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

Yes

The StopCovid application project is based on the construction of a history of pseudonymized contacts, using Bluetooth signals. The application protocol has defined technical specifications for communication via Bluetooth, limiting the size of the information transmitted between smartphones.

The project has been challenged by security experts, notably ANSSI, and is still being tested.

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

Yes

The crypto-identifiers are only accessed by the designated health authority, on the central server.

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

Yes/No

The app will only be used to alert persons that might have been exposed to the virus (the CNIL considers this as a fair and proportionate purpose). Should the app be used for other purposes in the future (monitoring compliance with lockdown measures, tracking the number of infected persons, contacting an infected person, etc.), a new assessment of the balance between such purposes and user privacy will have to be made.

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

The CNIL provided an opinion on the current version of the project on 24 April 2020 and has required to be consulted again before the final version is launched.

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)?

Yes

Certain companies have already indicated that they would like to use private applications similar to StopCovid to monitor their employees’ state of health. However, in France, this will only be possible within a very strict legislative and regulatory framework.
Contacts

Nadège Martin  
Partner  
Paris  
Tel +33 1 56 59 5374  
nadege.martin@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