NORTON ROSE FULBRIGHT

Contact tracing apps in France

A new world for data privacy

As of December 2, 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, developed by INRIA (National Institute for Research in Digital Science and Technology) was made public on June 2, 2020.

A decree (*Decree No. 2020-650 of May 29, 2020 relating to data processing known as "StopCovid"*) was published on May 29, 2020, setting the definitive legal framework for the implementation of the app.

The Government presented a new version of the app named "TousAntiCovid" on October 22, 2020. The Health Ministry stated that TousAntiCovid is an update of the latest version of StopCovid. As part of the new features, TousAntiCovid provides easy access to other tools including *"DepistageCovid"*, which provides a map of nearby testing centres and waiting times, and *"MesConseilsCovid"*, which provides personalised advice on how to protect oneself and others.

Since its launch, the app has been downloaded by almost 9.5 million people and more than 13,000 people have been notified as having been in contact with an infected person.

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)?

Two weeks after the app launched, Gaëtan Leurent, a French researcher in cryptography, explained that the app collects more data than originally understood. His findings show that all cross-contacts are sent to the central server, contrary to the government guidance which states that only the app users who had been in contact for 15 minutes, closer than one meter away from a person who tested positive for COVID-19 would be stored, meaning that the app processes more data than necessary to trace the spread of the virus, and is not compliant with the data minimization principle. The French Government has not denied the comments.

The second version of StopCovid, launched at the end of June, remedied this problem, but the French Data Protection Authority (the "CNIL") noted that this second version still contained certain shortcomings concerning user information, the subcontracting contract granted to INRIA and certain data processing aimed at securing the app. Therefore, the CNIL gave the Health Ministry formal notice to remedy this on July 20, 2020. Following the formal notice, as the CNIL considered the processing implemented were now compliant with the EU and French legislative data protection requirements, it declared the closure of the formal notice on September 3, 2020.

The main concern relates to the use of a centralized server, which 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

Was the first version of the app.

TousAntiCovid

Is the new version of the app (since October 22, 2020).

2. Is the app voluntary?

Yes

If a user is clinically diagnosed or is tested positive for COVID-19, he or she can choose to report it to the app and to transmit his or her proximity history to the server. The app can be uninstalled at any time.

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 CNIL states in its opinion of April 24, 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 TousAntiCovid. The CNIL expressly refers to employers, who may not subordinate certain rights to the use of this app, as this would amount to discrimination. Besides, an employer cannot compel their employees to download the app.

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.

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), 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.

With the launch of TousAntiCovid, the Government once again considers that the centralised architecture offers more guarantees and security. It makes it possible to prevent a server from collecting the list of people who have tested positive (even anonymously) and to prevent this list from circulating, or being stored, on a server or on telephones.

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?

Yes

A privacy impact assessment has been carried out prior to the implementation of the scheme, pursuant to CNIL's recommendations.

The CNIL stated in its opinion released on May 25, 2020 that the app incorporates privacy by design.

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

Yes

The shared authentication key and the crypto-identifiers are retained until the user uninstalls TousAntiCovid and in any event no later than six months after the end of the state of health emergency in France (currently set to be February 16, 2021).

Proximity history data recorded by the app on the mobile phone are kept for 15 days from the time they are recorded. When this data is shared on the central server, it is also kept for 15 days from the time it is recorded.

The infected person's data (in particular the date of the onset of symptoms and the unique code provided by the doctor that he or she shares with the app to trigger the sharing of his or her history with the central server) are not kept.

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

Yes

Security modules will be used to protect the encryption keys allowing access to the identifiers of the persons concerned in the central server.

A committee will be set up, bringing together several entities to which fragments of the encryption keys would be entrusted, in order to ensure that no single player can misappropriate the data. The CNIL considers that such a measure is likely to limit the risks of misappropriation of the central database.

In addition, the CNIL considers that the use of the certificate pinning mechanism ("certificate pinning") will enable apps to securely authenticate the server with which they are communicating and thereby guarantee the strict confidentiality of the data exchanged with the server.

Security audits were carried out by the ANSSI throughout the development of the application.

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

The Decree of May 29, 2020 provides that StopCovid (now TousAntiCovid) may only be used for the following purposes:

1. to inform users of the app that there is a risk that they may have been infected with COVID-19;
2. to raise awareness among the users of the app, in particular those identified as contacts at risk of infection, about the symptoms of the virus and the measures to be adopted to prevent its spread;
3. to recommend that contacts at risk of infection be directed towards the competent health actors;
4. to adapt, if necessary, the definition of the parameters of the app allowing the identification of contacts at risk of infection through the use of anonymous statistical data at the national level.

The Privacy Policy of the new version of the application "TousAntiCovid" provides an additional purpose, namely to assist in the generation of a certificate of exemption for traveling.

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 issued an opinion on April 24, 2020 on the principle of implementing the StopCovid app. It then issued an opinion on May 25, 2020 on the draft Decree governing the app.

In these opinions, the CNIL noted that the app included guarantees and was generally in compliance with the French and EU legislation on the protection of personal data.

When the app was launched (on June 2, 2020), the CNIL had announced that it would control and monitor its functioning on the field. Following inspections carried out by the CNIL in June 2020, the CNIL issued a formal notice against the Health Ministry on July 20, 2020 which was closed on September 3, 2020 as the CNIL considered the processing implemented were compliant with the EU and French legislative data protection requirements.

On September 14, 2020, the CNIL published its quarterly opinion addressed to the French Parliament on the conditions of implementation of the SI-DEP (the screening information system), Contact Covid and StopCovid processing as part of the combat against COVID-19. The CNIL notes that the measures put in place in the context of the health crisis are, for the most part, respectful of personal data and that most of the recommendations made by the CNIL in its opinions have been taken into account. However, the CNIL requests that indicators be set up in order to evaluate more precisely the contribution of these systems to the management of COVID-19.

On October 23, 2020, the CNIL commented on the TousAntiCovid app.

The CNIL underlines that the structural elements of the system are not affected by the app's evolution. The deployment of the new app did not require a mandatory referral to the CNIL since no substantial changes affecting the processing of personal data has been implemented in relation to the app. However, the app provides new functionalities to the user: the application now includes updated information on the circulation of the virus and links to other digital tools already in use by the health authorities (for example, a map of places where people can be tested or the certificate of exemption).

This being said, the CNIL notes that, in order to ensure the respect of the privacy of users of the app, a new opinion will be published by the end of the year. Since the app will be regularly upgraded, the CNIL intends to remain particularly vigilant in reviewing these future developments. In particular, it may carry out new checks and, if necessary, rule again if the data processing is subject to substantial changes.

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 indicated that they would like to use private applications similar to StopCovid (now TousAntiCovid) 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

NORTON ROSE FULBRIGHT

Law around the world
nortonrosefulbright.com

EMEA 24297 – 12/20