NORTON ROSE FULBRIGHT

Contact tracing apps in Russia

A new world for data privacy

As of May 15, 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)?

There is no single technology that has been introduced consistently throughout Russia.

However, monitoring of the spread of COVID-19 is done at the local level and some technologies have been introduced in certain regions of Russia. Moscow, where the number of cases is highest (about 50% of the total cases), is the only region of Russia that has introduced a technology for monitoring the location of citizens (as well as their close contacts) with confirmed COVID-19 via an app called Social Monitoring.

The Social Monitoring App was developed by the Department of Information Technologies for the city of Moscow. The app is intended for monitoring violations of a self-isolation regime and quarantine established for those who are being treated at home and/or are limited in leaving their places of residence.

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 are significant privacy concerns regarding the implementation of a Social Monitoring App. In addition to those mentioned above they include the following:

- The use of unprotected sources of transmission of personal data which may increase possible exposures, cyber-attacks, leakage of information and its further disclosure to unintended users in the market;
- Launching the process of personal registration and institution of online surveillance over the population for some state aims which cannot be clearly identified at this time (e.g., taxation or other).
- Since the app allows easy monitoring of a change of geolocation and any movements from the place of personal residence, it allows identification of violators of the regime and for significant penalties to be imposed.
- The scope of information collected and transmitted with the use of the app raises issues. In particular, this concerns photos/selfies transmitted with the use of the app. Given that only limited information regarding how the app works is available, there are questions as to whether information transmitted with the use of the app is properly protected.

App details

1. What is the name of app

Social Monitoring

2. Is the app voluntary?

Yes

The use of the Social Monitoring App is compulsory for infected persons who are being treated at home and who are recorded in the unified database of confirmed COVID-19 cases. The installation of the Social Monitoring App is subject to required written consent of the person for the disclosure of personal data. Those who fail to provide written consent cannot be treated at home and are to be taken to a medical institution. In addition, significant penalties can be imposed for the refusal to install the Social Monitoring App is installed and for the failure to the reply to push messages received by the user.

The Social Monitoring App can be downloaded for free on a smartphone or is provided along with the smartphone (if absent) for temporary use.

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?

N/A

There is no officially available instruction on information required to register for the Social Monitoring App as registration for the app is available for infected persons only and not to the general public. According to public sources, the following information is required to be registered in the app: name, passport details, photo/selfie, contact phone and geolocation data. All personal details that are provided in connection with the use of the app are set forth in more detail in the consent for the disclosure of personal data to be signed by the COVID-19 infected person.

5. Is GPS or Bluetooth used?

N/A

The technology underlying the Social Monitoring App is not publicly available, but it is based on the records of the individuals' location. According to publicly available information, once installed, the Social Monitoring App requests access to GPS, Bluetooth, camera and all settings on the personal smartphone.

Monitoring of the location of an infected person is also done through the push messages sent via the Social Monitoring App which require an immediate response and provision of a selfie.

6. Is data stored on a centralised server?

Unknown

No official information is available.

According to officially available information on mos.ru (official site of the Mayor of Moscow), registration for the Social Monitoring App is available only for persons who are recorded in the unified data base as infected with COVID-19. Accordingly, it seems that the data is to be stored on a centralised server and should match the said data base.

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

Unknown

The identity and basic information of infected persons is reported by medical institutions and doctors visiting infected persons at home to the unified data base managed by the Ministry of Health of Russia.

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

No

Generally information is not disclosed to anyone other than the public health care authorities (and also recorded to the unified data base managed by the Ministry of Health of Russia) and contacts who may have been exposed to a risk of contracting COVID-19, the latter are only provided limited information in order to identify the risk of exposure.

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

Yes

Generally, each time personal data is shared with other users the consent is required. It seems that the Social Monitoring App does not allow for sharing any information. It is intended for control and monitoring purposes only.

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

No

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

Unknown

The Social Monitoring App as used in Moscow is subject to obtaining written consent of the user for the disclosure of personal information for the purposes of obtaining medical treatment at home. This generally indicates that data collection is compliant with the laws on personal data, without incorporating “privacy by design” or indicating if a privacy risk assessment has been completed.

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

Yes

The account generated for the user of the app is to be deactivated within 10 days upon his or her recovery as confirmed by a medical certificate or upon the hospitalization of the user to a medical institution if the self-isolation regime is violated. Information about his or her location will be stored by the Department of Information Technologies for no more than one year from the date on which the control of the self-isolation regime ends.

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

Yes

The project is being challenged by security experts on the grounds that the information is not encrypted and data protection is not properly ensured. At the same time, under the law, the operator of the personal data is responsible for the security of information and must take measures to avoid leaks. The Department of Information Technologies that administers Social Monitoring App is determined as an operator of personal data collected in connection with the use of the app. As such, it is to comply with the federal regulation on personal data, including data processing and safety requirements. In its turn this authority has approved a Policy on confidentiality in relation to processing and safety of personal data circulated in connection with the use of the app.

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

Yes

General legal regulation of personal data establishes basic principles and limitations as concerns the access to personal data. It should be the case that the consent signed by the infected person prior to installation of the app contains required information on who may have access to the information assumed to be medical institutions and the Ministry of Health and possibly police authorities.

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

Yes

The consent for the disclosure of personal data should contain information on the purposes for which such data is used and disclosed. The use of the Social Monitoring App is limited to monitoring the observation of the established self-isolation regime by infected persons.

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

Yes

Federal Law “On personal data” and Federal Law “On information, information technologies and the protection of information” contain the respective regulation.

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

Yes

Only basic information in the form of questions and answers relating to the work of the Social Monitoring App is placed on the official site of the Mayor of Moscow (mos.ru).

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

Alyona Kozyreva
Senior Associate
Moscow
Tel +7 499 924 5138
alyona.kozyreva@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 – 05/20