NORTON ROSE FULBRIGHT

Contact tracing apps in The Netherlands

A new world for data privacy

As of December 18, 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 Government launched a contact tracing app, CoronaMelder, on October 10, 2020. The accompanying Act, the Temporary Act Notification-application Covid-19 (*Tijdelijke wet notificatieapplicatie covid-19*) (the **Temporary Act**) was passed by the Dutch Parliament on October 6, 2020. The Dutch Data Protection Authority (the DDPA) advised the Dutch Government on CoronaMelder on August 6, 2020.

Furthermore, the Government had published a draft bill which amends the Dutch Telecommunication Act (*Telecommunicatiewet*) and allows the National Institute for Health and Environment (*Rijksinstituut voor Volksgezondheid en Milieu*) (**RIVM**) to access telecommunication data (the aggregated location and traffic data of citizens) through the Dutch Central Bureau of Statistics (*Centraal Bureau voor de Statistiek*) for the purpose of controlling the spread of COVID-19, the Temporary Act Information Provision RIVM regarding Cocid-19 (*Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19*). The DDPA had reviewed the initial version of the draft bill and identified a number of areas that required improvement: (i) given that the bill was drafted with great urgency, its scope should be limited to the COVID-19 crisis alone (it allowed RIVM to access data for future epidemics as well); (ii) the purpose and necessity of the extended powers of the RIVM needed to be stated clearly; and (iii) no maximum retention period for the telecommunication data was included. The Government had considered the comments from the DDPA and published the draft bill on May 29, 2020, as well as a revised draft bill on June 24, 2020. The DDPA had subsequently commented in the media that it does not agree with the draft bill. According to the DDPA, the data is not unconditionally anonymised, the purpose and necessity of the bill need to be stated more clearly and the safeguards proposed by the DDPA need to be implemented into the new draft bill more sufficiently. On October 2, 2020, another revised draft bill was published by the Government. The State Secretary of the Ministry of Economic Affairs and Climate Policy (*Staatssecretaris van Economische Zaken en Klimaat*) also published an accompanying letter. In the letter, the State Secretary confirms that, due to the anonymization of the data, no personal data will be processed as a result of the draft bill. Furthermore, according to the State Secretary, the safeguards proposed by the DDPA in respect of the initial draft bill have been implemented, where feasible. Finally, the State Secretary reiterates the purpose and necessity of the draft bill. The DDPA has not yet responded to the letter or the revised draft bill.

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)?

According to the legislative history of the Temporary Act, one of the major concerns from the Parliament, the DDPA, the Netherlands Institute for Human Rights (College voor de rechten van de mens) and others was that the use of the app would be made compulsory by third parties. The Temporary Act therefore contains a so-called "anti-abuse" clause, which prohibits anyone from requiring the others to use CoronaMelder, or any other similar digital resource.

On August 6, 2020 the DDPA provided advice in respect of CoronaMelder. Although the DDPA was overall satisfied with the development of the app, it also identified a number of issues:

- The biggest privacy concern of the DDPA related to the *Google Apple Exposure Notification Framework*, the underlying software in the mobile operating systems of Google (Android) and Apple (iOS) that enables the use of CoronaMelder. The DDPA stipulated that it is

unclear whether Google and Apple are able to access the data of the users of CoronaMelder. The DDPA stated that the relevant data controller (i.e. the Minister of Health, Welfare and Sport and the Regional Public Health Authorities (the local GGD)) should enter into an agreement with Google and Apple that ensures the privacy of the users of the app. It is emphasized in the legislative history of the Temporary Act that Apple and Google do not process any personal data through the app.

- Since CoronaMelder has major privacy impacts, the use of the app should have a legal basis (through an accompanying act) that contains sufficient safeguards. The Temporary Act provides such a legal basis.
- Furthermore, the DDPA commented that the security of the backend server of the app should comply with the requirements under the General Data Protection Regulation (GDPR). At the time of the advice, there was no host for the backend server, as the Dutch Tax Authority withdrew itself as a host. After the advice of the DDPA, it has been determined that CIBG (an implementing body of the Ministry of Health, Welfare and Sport) and KPN (a Dutch telecommunications company) will manage the backend server. It is unclear whether the DDPA deems the security provided by these hosts sufficient.

In addition, it was previously indicated by stakeholders that it is important to make clear which (governmental) organisations will use the app and who the data controller is in respect of the personal data. This is important as the data controller is responsible for complying with the GDPR and is the point of contact for data subjects in order to receive information on the data processing and to enforce their data subject rights under the GDPR. According to the Temporary Act, the Minister of Health, Welfare and Sport is the joint controller, together with the Regional Public Health Authorities (the local GGD).

Since CoronaMelder was launched, critics have expressed that, although the app makes use of anonymized codes, in certain cases the identity of an infected user can still be unravelled. To illustrate this, a website has been launched on which visitors can see who uses CoronaMelder and can subsequently attribute a name to such users on the website. The Ministry of Economic Affairs and Climate Policy acknowledges that the risk of identification exists, but it has also stressed that the privacy risks seem to be limited, as identification would require significant efforts.

App details

1. What is the name of app

CoronaMelder

2. Is the app voluntary?

Yes

The Temporary Act contains a so-called "anti-abuse" clause, which prohibits anyone from requiring the others to use CoronaMelder, or any other similar digital resource. This prohibition includes making the use of the application (or another similar digital resources), the sharing of any information from it, or announcing whether or not any notifications have been received conditional for: (i) accessing buildings or other facilities, (ii) employment, (iii) the use of a service, (iv) participating in any form of interpersonal contact, or (v) receiving any benefit. This prohibition therefore applies to all third parties. It also applies to all contact tracing apps, including but not limited to CoronaMelder.

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

As stated above, pursuant to the "anti-abuse" clause it is prohibited to require the others to use CoronaMelder, or any other similar digital resource, or share any information from it (including announcing whether or not any notification have been received).

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

The Government indicates on its website that no personal data will need to be submitted in order to use the app.

5. Is GPS or Bluetooth used?

CoronaMelder uses Bluetooth Low Energy.

6. Is data stored on a centralised server?

Yes

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

No

CoronaMelder uses the exposure notification framework supplied by Apple and Google pursuant to which the identity of infected users is not captured. Under this framework, the app exchanges variable codes, the so-called Rolling Proximity Indicators (RPI) that are created every 10-20 minutes, with other users of the app that are in close proximity. The RPI's are derived from "Temporary Exposure Keys" (TEK) that are created on a daily basis. The RPI from other users, and the TEK of the user itself will be stored in the app for 14 days. Both the TEK and the RPI cannot be traced back to an individual. Only if a user of CoronaMelder receives a positive test result, the user may choose to send its TEK, together with a validation code provided by the Regional Public Health Authority (the GGD) and the date on which the individual experiences the first symptoms, to the backend server. This backend server facilitates the review and exchange of codes between users and the GGD. The codes of the backend server are regularly collected by the smartphones of other users. The Google Apple Exposure Notification Framework checks if there is a risk for other users. If a risk is identified, the other user(s) will be notified, whereby they will also be informed on which date the contact with the infected user took place, without disclosing the identity of the infected user.

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

According to the Temporary Act, the identity of the infected user will not be disclosed to the proximate users (they will only receive a notification that they were in close proximity of an infected user, indicating the date on which the contact took place). Given that the identity of users will not be captured, the identity will also not be disclosed to others (such as public health authorities) through the app.

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

Yes

When downloading and using CoronaMelder, separate consent will need to be provided for (i) saving CoronaMelder, (i) saving the user's own TEK's, (iii) sending RPI's to other users in close proximity, (iv) saving RPI's of other users in close proximity, and (v), if the user receives a positive test result, sending the TEK's, RPI's and the day the first symptoms were experienced to the backend server.

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

No, in the legislative history of the Temporary Act it is stipulated the identity of the notified users will not be disclosed to the Minister of Health, Welfare and Sport and the Regional Public Health Authorities (the GGD).

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

This is required under the GDPR. The Government conducted a protection impact assessment (PIA) and discussed it with the DDPA before the app was launched on October 10, 2020.

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

The data (i.e. anonymised codes of the user and the proximate users) will be stored in the app for 14 days. If the data is uploaded to the backend server, it will be stored for 14 days as well, except for the IP addresses of the smartphone of the user, which will be stored in the backend server for security purposes for 7 days.

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

Yes

The app has been developed with experts in various areas to ensure that the app complies with applicable security and privacy standards. According to the legislative history of the Temporary Act, while developing the application, the Government has followed the recommendations of the European Commission and the European Data Protection Board. One of the most important security measures is that the app only makes use of anonymised codes to determine whether contact between users took place.

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

It seems that only the data controllers (i.e. the Minister of Health, Welfare and Sport and the Regional Public Health Authorities (the local GGD)) and the processors of the backend server (i.e. CIBG and KPN) have access to the data included in the backend server. In order to upload data to the backend server, the Regional Public Health Authorities (the local GGD) will also process the validation code and the date the individual experienced the first symptoms in the GGD portal of the app, which can only be accessed by authorised GGD employees. The data controllers and data processors do not have access to the personal data stored locally on the smartphones of the users.

Under the Temporary Act, data may be shared with other member states of the European Union that use similar notification applications.

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

The legislative history of the Temporary Act stipulates that the app and the data included in it may only be used to support the Regional Public Health Authorities (the local GGD) with their contact tracing investigations in the context of combating Covid-19.

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 DDPA was closely involved in the development of CoronaMelder and the DDPA published its advice in respect of CoronaMelder on August 6, 2020.

As stated above, the DDP identified a number of issues, which have been addressed in the legislative history of the Temporary Act. The DDPA has not responded to the final version of the Temporary Act.

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

Jurriaan Jansen
Partner
Amsterdam
Tel +31 20 462 9381
jurriaan.jansen@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