NORTON ROSE FULBRIGHT

Contact tracing apps in the UK

A new world for data privacy

As of October 05, 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)?

Yes. The National Health Service (NHS), has rolled-out a contact-tracing smartphone app for people living in England and Wales, aged 16 or over. It is based on decentralised "exposure notification" and "exposure logging" technology developed by Apple and Google. The app can instruct users to self-isolate if it detects that they were nearby an individual with the virus; it can alert to the level of coronavirus risk in users' postcode districts; it includes a check-in scanner to alert users if a venue visited has been categorised as an outbreak hotspot; and it allows users to order a coronavirus test. Different apps are in use in Scotland and Northern Ireland.

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)?

Concerns centre on privacy principles of security, data minimisation, transparency and accountability and these apply both to private and Government use of tracing apps.

In particular in relation to Government use:

- Government surveillance – government harvesting superfluous data and being able to centralise the data and use it for unrelated purposes.
- Lack of trust in Government to store and handle data appropriately if the data is centralised.
- Centralised data being held indefinitely given the ongoing nature of the pandemic.
- A lack of Government accountability.
- Privacy being trumped by community health concerns.

In particular in relation to private sector use:

- Employee surveillance beyond what is necessary for the purposes of maintaining a safe work environment – e.g. using data for keeping tighter controls on employee movements/engagements.
- Unnecessary dissemination of data within a business beyond strict confines of relevant HR manager.

App details

1. **What is the name of app?**

   NHS COVID-19

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 NHS developed app is not currently used in this way and there is no suggestion this will change.

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

   Users will need to enter the first 3 characters of their post code (a 'postcode district' which resolves on average to about 8000 addresses) to allow the NHS to understand where concentrations of infections are occurring without being able to identify individual users/ devices.

5. **Is GPS or Bluetooth used?**

   Bluetooth 4.0 or higher

6. **Is data stored on a centralised server?**

   Data that could identify a user is not stored centrally. Non-identifying data may be stored on a centralised server with the user's consent.

   All the data that could directly identify a user is held on their mobile device, is not stored centrally and is not shared anywhere else.

   The app generates a code identifying the device which changes every day. Another code based on the device code is generated every 15 minutes. This code is shared with other users of the app to register proximity.

   If the user has a positive test result, the app will ask for the user's consent to share their daily codes with other app users. These codes cannot be associated with the user or their mobile device.

   If the user who has tested positive agrees, his or her daily codes will be uploaded to the central system (hosted on Amazon Web Services UK and Microsoft Azure Cloud Services UK). The central system will then send the codes to every other app user's mobile device and each user's app will check for any matches. Where there are matches, the user will get an alert that they have been in contact with someone who tested positive. The central system will not know who the users have been in contact with and it does not record matches.

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

   It will be the individual's decision as to whether to disclose their infection status to the public health authorities. The public health authorities will not disclose the identity of the infected user.

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

   Yes

   The basic processing is not undertaken using consent. However, the user's 15 minute codes are not released to other users to be matched unless the user consents to his or her positive test result being shared in this way (as there is a remote risk that other users would be able to infer who had infected them if they had had very little contact with other people).

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?**

    Privacy by design: Yes
    Risk assessment: Yes

    NHSX (the technology arm of the NHS) states that it has "prioritised security and privacy in all stages of the app's development, starting with the initial design, and user testing".

    A Data Protection Impact Assessment has been conducted and is publicly available at https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/the-nhs-test-and-trace-app-early-adopter-trial-august-2020-data-protection-impact-assessment.

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

Diagnosis keys are retained on the user's mobile device for 14 days. Submitted diagnosis keys are retained on the UK Department of Health and Social Care secure computing infrastructure for 14 days. QR codes that are scanned by the user when visiting venues are deleted after 21 days. The retention period for analytics data is subject to confirmation.

Data submitted by app users will not contain direct, indirect or consistent identifiers, accordingly retention is not relevant in the GDPR context (as they do not include personal data). For completeness, of these records, those which are used to hold organisations to account is held for 8 years, and thosewhich are used to monitor communicable diseases are held for 20 years.

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

Yes

According to NHSX, security has been "prioritised" at all stages of the app's development. The key security and privacy designs alongside the source code are published so privacy experts can review this. By way of example, all data is stored in encrypted storage, and data in transit is encrypted with TLS1.2+ using modern cipher suites. The National Cyber Security Centre and other cyber security experts continue to advise on how to protect the privacy of app users, including the controls used to anonymise and aggregate data.

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

No

The purposes for which the data may be used are set out under the following questions.

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

Yes

NHSX states that data will only ever be used for NHS care, management, evaluation and research.

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

Yes

However, the UK Parliament's Human Rights Committee proposed legislation to limit the use that Government could make of data collected through the NHS COVID-19 app but the Government rejected its proposals. The Government's position is that the existing data protection framework is sufficient.

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

Yes

The UK Information Commissioner's Office (ICO) has "been working with NHSX to help them ensure a high level of transparency and governance". The ICO published an opinion on the underlying Apple/Google technology which was generally supportive of that model. It also published an update on 18 September 2020 in respect of the regulatory work undertaken for the app which makes it clear that the developer has shared and consulted with the ICO on data protection impact assessments for the app. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/09/blog-data-protection-considerations-and-the-nhs-covid-19-app/

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

SaferMe advertises a business contact tracing app in the UK.

Contacts

Lara White
Partner
London
Tel +44 20 7444 5158
lara.white@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