Contact tracing apps in the UK

A new world for data privacy

As of June 29, 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), in particular the technology arm of the NHS (NHSX), has been developing a contact tracing app. A trial was commenced on the Isle of Wight on 5 May. Due to limitations with the NHS app operating on Android and Apple devices, the UK government announced on 18 June 2020 that it will be switching to a model developed in conjunction with Apple and Google (which will work on a decentralised basis). Details regarding the roll-out of this app remain undetermined, although it is not expected to be ready until autumn 2020 at the earliest.

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

   NHS COVID-19, however rebranding of the app may occur.

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 envisaged to be used in this way and there is no suggestion this will change for the new redesigned app. According to NHSX the data will "only ever be used for NHS care, management, evaluation and research."

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

   It is not yet clear what information would be required to register.
   There are reports that a user will need to enter the first 3 characters of their post code (which resolves on average to about 8000 addresses) to allow the NHS to understand where infected persons reside. However, given plans to re-design the app, this may change.

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

   Bluetooth

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

   No
   The model of contact tracing app envisaged by Apple and Google does not involve information transfer to a centralised database.

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

   No
   Full details yet to be disclosed, but it is thought not.

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

   No
   It appears that it will be the individual's decision as to whether to disclose their infection status to the public health authorities. Further disclosure by the public health authorities of the identity of the infected user is not envisaged.

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

   N/A
   It is likely the new app will not involve collection of data in a centralised system so this would not be an issue.

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: Reportedly yes
    Risk assessment: Not known
    NHSX states that it has "prioritised security and privacy in all stages of the app's development, starting with the initial design, and user testing". The NHSX's results thus far will be used to contribute to further development of the app. It may be that further risk assessments will be undertaken if the app is drastically redesigned, however the same adherence to prioritising privacy should apply.

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

    Not known as yet

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, starting with the initial design, and user testing. The key security and privacy designs alongside the source code will be published so privacy experts can review this. The National Cyber Security Centre has been involved and published a paper on the privacy and security design on 3 May.
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>14. Are there clear limitations regarding who may have access to the data?</strong></td>
<td>No</td>
</tr>
<tr>
<td>The purposes for which the data may be used are set out under the following question. It is unclear as yet which third parties will support these activities.</td>
<td></td>
</tr>
<tr>
<td><strong>15. Are there clear limitations on the purposes for which the government may use the data?</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>NHSX states that data will only ever be used for NHS care, management, evaluation and research. Subsequent updates about the new app design will clarify the extent of government involvement in the data.</td>
<td></td>
</tr>
<tr>
<td><strong>16. Is the government of your country bound by privacy laws in respect of the contact tracing data?</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>17. Has the regulator commented/ provided guidance on the technology?</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>The final app has not yet been reviewed by the UK Information Commissioner’s Office (ICO). However, ICO has stated that it has “been working with NHSX to help them ensure a high level of transparency and governance”. ICO published an opinion on the underlying Apple/Google technology which was generally supportive of that model.</td>
<td></td>
</tr>
<tr>
<td><strong>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)?</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>SaferMe advertises a business contact tracing app in the UK.</td>
<td></td>
</tr>
</tbody>
</table>