Commercial & Tech Law Blog

Privacy and data protection issues in COVID-19 contact tracing apps

Posted on June 22, 2020June 23, 2020 by eyadmin

Alex Razak (https://web.archive.org/web/20200721015855/http://www.linkedin.com/in/zxr) | Manager | Law | +447341079034 | alex.razak@uk.ey.com (https://web.archive.org/web/20200721015855/mailto:alex.razak@uk.ey.com)

Background

As countries move towards lifting the dramatic restrictions that were imposed to contain the rapid spread of COVID-19, more reliance is likely to be placed on contact tracing, especially contact tracing apps, to detect and control a further outbreak of COVID-19.

In this note, we highlight key privacy and data protection issues in relation to the development and use of COVID-19 contact tracing apps as well as the guidance from the UK's Information Commissioner's Office (ICO) on this matter.

This note is not intended to provide an exhaustive list of issues. Nor should it be relied upon as legal advice. Please do contact us if you require legal advice on any specific issues.

What is contact tracing?

Contact tracing is the process of tracing, assessing, and managing people who have been exposed to a probable or confirmed case of COVID-19 and who may be at risk of developing the disease and potentially infecting others. When systematically applied, it has the potential to break the chains of transmission and spread of COVID-19 as well as assist epidemiologists with monitoring the disease. It is regarded as an essential public health tool for controlling infectious disease outbreaks.

Contact tracing can be carried out manually – it has been carried out manually in response to other epidemics and also in the early stages of the current epidemic in some jurisdictions.

What is a contact tracing app?

A contact tracing app is a smartphone app that automates the process of contact tracing. Smartphones are used as a proxy for monitoring individuals by determining which smartphones have been close to each other for relevant periods. The data that is collected is then analysed to assess which persons may have been close enough and for long enough to

infect each other. The apps enable in-app alerts and notifications to be communicated to users if they have been in close proximity with an individual who has a positive COVID-19 result. In some cases, individuals may be asked to self-isolate.

The use of smartphone apps is intended to facilitate the implementation of contact tracing on a larger scale than may otherwise be practical through manual contact tracing. Manual tracing requires a workforce and also relies on a person's ability to recall their movements and does not easily allow contacts who are strangers to be identified. Mobile phone apps use automated data collection and analysis, potentially allowing for quicker and more precise contact tracing.

In the UK, the NHS launched the NHS COVID-19 App (https://web.archive.org/web/20200721015855/https://covid19.nhs.uk/). Separately, Apple and Google have partnered to develop an exposure notification system (https://web.archive.org/web/20200721015855/https://www.apple.com/uk/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/) for COVID-19. Whilst the NHS's contact tracing app is based on a different model to Apple and Google's exposure notification system, both models utilise Bluetooth technology in smartphones. Broadly, users of the app will exchange anonymous tokens with other app users in their proximity (akin to a virtual handshake). This exchange takes place through Bluetooth signals on the mobile phones. A data trail gets created as exchanges continue to take place. Should an infected person upload their diagnosis on their app, a notification will be sent in-app to all users who had recently exchanged tokens with the infected user and are deemed an infection risk themselves. Exposed persons may then be given instructions on next steps.

Following testing of the NHS COVID-19 App on the Isle of Wight, the UK government has announced (https://web.archive.org/web/20200721015855/https://www.gov.uk/government/news/next-phase-of-nhs-coronavirus-covid-19-app-announced) that it will be taking forward a solution that brings together the work on the NHS COVID-19 App and the Google/Apple solution. Separately, the NHS has announced (https://web.archive.org/web/20200721015855/https://faq.covid19.nhs.uk/article/KA-01097/en-us) that the government is shifting its focus to developing a solution based on Apple and Google technology and that users who downloaded the NHS COVID-19 App should uninstall it.

What personal data, if any, gets processed?

Compliance with the General Data Protection Regulation and the Data Protection Act 2018 will need to be considered where the contact tracing technology processes personal data. Additional protections are given to the processing of data concerning health.

The term "personal data" is defined broadly to include any information from which a person can be identified, directly or indirectly including by reference to an identifier. Common forms of personal data include a name and location data. An identifier can include location data as well as online identifiers provided by devices such as internet protocol addresses. A Bluetooth token may be personal data where it enables an individual to be identified directly or indirectly from it.

According to the NHS website (https://web.archive.org/web/20200721015855/https://covid19.nhs.uk/privacy-and-data.html), the NHS COVID-19 App would not collect personal information from users and users would remain anonymous. As per the FAQ's[1] published on Apple's website (https://web.archive.org/web/20200721015855/https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf), those using Apple and Google's exposure notification system will not be able to identify other users and user identity will not be shared with Apple and Google. Both contact tracing frameworks involve the processing of health information (for example, where a user reports a positive diagnosis of COVID-19 through the app).

Whilst the systems are designed to avoid identification of individual users. It is worth noting that the publicly available data protection impact assessment (DPIA) of the NHS's contact tracing app states that information obtained from a user and their smartphone undergoes a process of pseudonymisation. It is therefore not *entirely* anonymous. Furthermore, the published DPIA of a contact tracing software known as the Decentralised Privacy-Preserving Proximity Tracing or in short, DP^3T, acknowledges that re-identification of individual users cannot be entirely excluded. Taking the system as a whole, the information that is shared between users through their use of the app, at some points, is characterised as personal data.

What is the guidance from the ICO and the EU?

The ICO has released an opinion (https://web.archive.org/web/20200721015855/https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf) in response to the joint effort announced by Apple and Google. The ICO's opinion also considers the DP^3T contact tracing system. The ICO has released a further statement (https://web.archive.org/web/20200721015855/https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf) on its expectations on how contact tracing solutions may be developed in line with the principles of data protection by design and default. The guidance includes a series of best practice recommendations. Separately, the European Data Protection Board (EDPB) has also issued guidelines (https://web.archive.org/web/20200721015855/https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf) on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.

Guidance from the ICO and the EDPB is aligned in the view that data protection legislation should not be viewed as an inconvenience in the fight against the current pandemic. Data protection legislation should therefore be viewed as integral to the construction and maintenance of contact tracing technology. Key points from the ICO's statement are summarised below.

- **Data Protection Impact Assessments.** A DPIA is required for contact tracing solutions prior to implementation, given that the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA may also need to iterate over time.
- **Transparency.** Transparency is one of the fundamental principles of data protection legislation and this is made clear in the ICO's statement. Developers of the app or service should be transparent about the purpose of the app or service and explain whether the purpose is only proximity notification or whether it is broader. Further processing for

purposes unrelated to the primary aim should be excluded. Users must be provided with clear and comprehensive information about the data the app processes before the processing takes place.

- **Data minimisation.** Collection of personal data should be kept to a minimum and to that which is necessary. Contact tracing apps should only collect or otherwise process information that is required for the core purpose of contact tracing. Location data and other device identifiers beyond any that are strictly necessary for the core purpose should not be collected.
- **Privacy by design and data security.** Data protection must be integrated into the processing activities that are conducted throughout the lifecycle of the app. Appropriate cryptographic/security techniques should be employed to secure the data.
- **User control.** Ensure that users can exercise their rights via the app where these rights apply.
- **App use should be voluntary.** Use of the contact tracing app, from installation to sharing of information, should be voluntary. There should be no negative consequences for individuals if they do not take action.
- **Lawful basis for processing personal data and data concerning health.** Processing of personal data should be based on a lawful basis. Processing of personal data concerning health requires additional conditions to be met.

Can organisations oblige employees, customers or visitors to use the contact tracing app?

Businesses may wish to make use of contact tracing apps to help provide an additional assurance that those entering its premises (whether employees or visitors) have not been infected. One way of doing this would be to ask individuals wishing to enter business premises whether they have the contact tracing app installed on their smartphone and if so, whether they have received a possible infection alert within a certain time frame. In our earlier blog entitled Privacy and data security issues amidst the Coronavirus (COVID-19) pandemic (https://web.archive.org/web/20200721015855/https://commercialandtechlawblog.ey.com/2020/03/19/privacy-and-data-security-issues-amidst-the-coronavirus-covid-19-pandemic/), we discussed the key privacy and information security issues that businesses should consider as part of their business continuity measures, and the issues considered in that blog continue to be relevant. It is worth noting however that use of the contact tracing app is not legally mandatory for members of the public and organisations should consider seeking independent legal advice if they wish to oblige their employees or visitors to use the app.

How we can help

This note sets out some of the key privacy and data protection issues in relation to the use of COVID-19 contact tracing app in England and Wales. The use of contact tracing (manual and app-based) is expected to increase as the UK moves towards moving out of the current lockdown. These issues are also likely be arising in other jurisdictions. If you have any questions in relation to this note, please do get in touch with us.

Alex Razak

22.06.2020

[1] May 2020 v.1.1