CAN CONTACT TRACING APPS TURN THE TIDE? THE STORY SO FAR

The idea of track and trace and the use of contact tracing apps has become a key component in the fight against Coronavirus. This article looks at the story so far and some of the privacy challenges track and trace faces.

WHAT IS CONTACT TRACING?

individuals who have been exposed to a disease to prevent onward transmission" (WHO)

By determining and documenting the movements and interactions of an individual, contact tracing can help determine when (and possibly where) infected individuals have been in contact with others, therefore creating a traceable "map" of individuals who have been exposed.

Contact tracing methods (particularly automatic contact tracing on a large scale) can help individuals quickly identify whether they have been exposed to infection and need to self-isolate, before they start to display symptoms. This could slow the spread of the infection and allow governments to more quickly and safely ease general lockdown measures whilst still protecting overall public safety.

For further information on the privacy and employment considerations and practical steps for employers when implementing tech tools in response to COVID-19, please read our article Test, track and trace : The Coronavirus health and safety, human rights and data protection conundrum for employers.

WHY TECH COULD MAKE THE DIFFERENCE

Manual contact tracing requires a team of individuals (typically a combination of call handlers and health professionals) to contact individuals who have been infected and gather information about places they have been and individuals they have met, to establish a list of "at risk" individuals. These "at risk" individuals are then contacted.

Automatic contact tracing deploys technology to log when two people physically encounter one another, typically using Bluetooth Low Energy signals to exchange a code. When one user reports symptoms of infection (for example through an app), a cascade of alerts are made so that identified "at risk" encountered persons are automatically notified without the need for a human contacting them.

Automatic contact tracing should be more effective as it identifies a greater range of "at risk" individuals, particularly those who the infected individual

either: (a) forgets or chooses not to identify; or (b) cannot identify or provide appropriate contact details for. It can also reduce the risk of human error of the manual contact tracing team.

There are however a number of operational challenges if deploying this tech solution.

For example, if an app for a device is used, a significant number of the population will be required to use that app for it to be effective. App developers within the NHS have estimated that over 60 per cent of the UK population will need to use the same contact tracing app for it to be "successful" (however, such apps have been found to still have a "protective effect" when used "at much lower levels", according Oxford University researchers). There are certain societal groups which may not be able to access or use the technology.

There are further technical challenges. Bluetooth signal strength can vary substantially, based on several factors, including how deeply a handset is placed in a bag, whether two people are walking side-by-side or behind the other, and whether the handsets are indoors rather than outdoors. For example, developers using the Apple-Google technology have had difficulties using Bluetooth to estimate distance between two users, at times being unable to differentiate between a handset in a bag one metre away and a phone in a hand three metres away.

THE GLOBAL RESPONSE

A contact tracing app developed in Germany was downloaded 6.5 million times within 24 hours of its release. Contact tracing apps are seen as a key tool to combat and mitigate the effects of COVID-19; programmes are being rolled out globally. Versions of contact tracing apps have been deployed in several countries, including Australia, Canada, China, France, and Hong Kong and are further in the process of development in Spain and Singapore, amongst others. The World Health Organisation have also discussed the possibility of developing a Bluetooth-based contact tracing app that could be used for contact tracing in low- and middle-income countries.

Apple and Google entered into a joint venture to produce an Application Programming Interface (API) for public health agencies to incorporate into their own contact tracing apps, and a system-level contact tracing system compatible with iOS and Android devices. The tech giants entered into the joint venture to address concerns regarding the poor interoperability between contact tracing apps and several mobile devices. Interoperability between apps within different countries is another challenge; this can be mitigated through the use of a single underlying technology for different countries' apps.

CENTRALISED V DECENTRALISED MODEL

All mobile contact tracing apps have largely the same function – to notify asymptomatic individuals when they have been in contact with an infected individual. However, two different models have been proposed, broadly distinguished on the basis of where the data is held.

In a typical centralised system, the smartphone shares its own pseudonymised InstallationID plus codes gathered from other phones to a

centralised database (a remote computer server) then uses this database to do the contact matching and risk analysis.

In a typical de-centralised system (proposed by Apple and Google in the context of their contact tracing systems) the phone only provides the InstallationID to a remote database. Then, the smartphone downloads the database, does the contact matching and sends the alerts all "on phone".

A de-centralised system therefore collects and stores less user data, reducing data vulnerability and GDPR compliance risk; but reducing opportunities to perform analysis, testing and auditing.

WHAT IS THE UK SOLUTION?

In May 2020 the UK Government trialled a centralised system contact tracing app ("Version 1") designed by NHSX, the digital innovation branch of the NHS. The UK ran a six-week trial of Version 1 on the Isle of Wight which finished in June 2020.

Following this trial, on 18 June 2020 it was announced that the UK would stop developing Version 1 in its current form instead moving forward with a new model utilising technology produced in the Apple-Google joint venture (the decentralised model) system produced by the two companies as well as the learnings from Version 1 ("Version 2").

Version 1 had faced a significant amount of criticism in particular from a privacy/user rights perspective; the Parliamentary Joint Committee on Human Rights described the law regulating Version 1 as an "unsatisfactory mismatch across the GDPR, the Data Protection Act 2018, Article 8 European Convention on Human Rights and caselaw on the right to privacy" and drafted a bespoke Digital Contact Tracing (Data Protection) Bill in response. At the time the Health Secretary rejected the need to introduce new legislation.

GDPR CHALLENGES OF CONTACT TRACING APPS

True anonymisation?

The GDPR only applies to personal data, i.e. information from which an individual is, or can be, identified. Truly anonymised data is not within the scope of the GDPR.

Anonymised data, from a GDPR perspective, means data which no longer identifies the person, and which cannot reasonably be processed in such a way as to re-identify the relevant person. If the data is only temporarily anonymised, it is only considered pseudonymised under the GDPR.

The InstallationID proposed to be provided in Version 1 and in other similar centralised apps is likely only to be pseudonymised as it would be possible to re-identify the underlying individual by using other information which is collected from the user or by combining it with other publicly available sources of information. Generally, a centralised model provides greater opportunities to re-identify individuals, as more data is shared and stored on a central database, thereby significantly increasing the scope of personal data which will be governed by the GDPR

Data Subject Rights

The GDPR gives rights to individuals over their personal data which is being processed. This includes rights in certain circumstances to access the data and rights to have the data deleted. In order to fulfil this obligation, the back end technology must be appropriately designed to have this functionality.

This is particularly relevant in the context of a centralised app, such as Version 1, where more data of the individual is stored on a central database. Government responses with respect to Version 1 had suggested that giving full effect to these rights in practice may not have been achievable – in particular once data is uploaded to the central database it is aggregated with the other data and loses its identifiable qualities. This could have meant that Version 1, in this sense, would not have been compliant with the GDPR.

Data Security

The GDPR requires that appropriate technical and organisational security measures are taken to ensure deployment of a level of security appropriate to the risk. The centralised approach presents a heightened level of risk (versus a decentralised system) as significant volumes of data (including the more sensitive health data) are stored on a central server, presenting a single target for a malicious actor and a single source of vulnerability for an unintended disclosure.

Given the heightened risk of the centralised system, regulators will expect a greater level of technical and organisational security measures which will require additional cost, resource and time. The ICO, the UK's privacy regulator, has particularly stressed that appropriate cryptographic/security techniques should be deployed to secure the data, both at rest (in servers and apps) and in transit (between apps and the server).

Data Minimisation

A fundamental principle of the GDPR is that the personal data collected should be limited to what is necessary for the purposes for which they are processed ("data minimisation"). An ICO statement seems to supports the use of the decentralised model: they have specifically stated that first consideration should be made to whether matches can be made on-device and that where this approach is "available, feasible and enables you to achieve your purposes, then you should use it". In practice, the use of a centralised model creates significantly more privacy risk and therefore, greater GDPR compliance risk.

Analytical Use

The GDPR requires that personal data is processed lawfully, fairly and in a transparent manner and that it is collected for specified, explicit and legitimate purposes. In the context of contact tracing apps the ICO specifically flagged that "gathering, augmenting or correlating user data" without express permission should be avoided.

The government had initially proposed that Version 1 had a clear advantage with a greater ability to conduct research or to link other datasets at some point in the future, which whilst useful from an practical perspective, would have presented clear privacy challenges to do so in a manner compliant with the GDPR and regulator expectations.

THE FUTURE

Contact tracing apps, if deployed correctly, could form an important part of the global COVID-19 response. It presents a clear use case for the deployment of technology, particularly with respect to automation and scalability. Given the nature of the data collected, the actors at play and the intended size of the user base, getting privacy right is key both from a legal perspective and from a strategic perspective. Without user trust and user buy-in, such apps will not achieve user participation at the levels required to deliver meaningful results. Given the clear time pressure, it remains to be seen if and when a UK contact tracing app will be effectively delivered.

CONTACTS

Jonathan Kewley
Partner

T +44 20 7006 3629
E jonathan.kewley
@cliffordchance.com

Jamie Andrew
Senior Associate

T +44 20 7006 1367
E jamie.andrew
@cliffordchance.com

Uche Eseonu
Trainee Solicitor

T +44 20 7006 6188
E uche.eseonu
@cliffordchance.com