A&L Goodbody

Focus on
COVID-19
Coronavirus

Contact Tracing Apps – *A Privacy Primer*

As part of their lockdown exit strategy, governments around the world are launching Apps with contact tracing functions.

Introduction

The idea behind contact tracing Apps is that users will be alerted when another App user has tested positive to COVID-19, thereby enabling them to take appropriate action, such as self-isolating or undergoing testing.

It remains to be seen how effective contact tracing Apps will be in the fight against COVID-19, but it is clear that in order for the Apps to work, they need to be widely downloaded and used. The European Commission has highlighted that evidence from Singapore, and a study by Oxford University, show that 60-75% of a population need to use the App for it to be efficient. The popularity, acceptance, and use of the Apps will undoubtedly depend on the extent to which the Apps enable individuals to control the collection and use of their personal data.

The European Commission and European Data Protection Board (**EDPB**) have published guidance for EU Member States and App developers, to help ensure the Apps comply with EU data protection laws, in particular the GDPR and ePrivacy Directive 2002/58/EC. Contact tracing guidance recognises that there is no one-size-fits-all solution, and that the envisaged technical solutions need to be examined in detail, on a case-by-case basis.

In developing contact tracing Apps, governments will also need to balance an individual's right to protection of their personal data under Article 8 of the Charter of Fundamental Rights of the EU, against other rights, such as freedom of movement and the right to engage in work which are suffering unprecedented restrictions due to the lockdown.

It is hoped that the development of contact tracing Apps in compliance with this guidance, will help reassure users that their fundamental right to protection of their personal data will be respected, and that data collected by the Apps will not be used for any other purposes, such as enforcement of lockdown or quarantine restrictions.

Why are governments turning to contact tracing apps?

Traditionally, the contact tracing tools employed by national health authorities has involved manually contacting and tracking down people who have been exposed to an infected person. However, this can be a resource-intensive and onerous process, and relies on information provided by infected persons regarding their movements and interactions, during the time they may have been infectious. It is hoped that contact tracing Apps will improve the speed and effectiveness of contact tracing, and help people return to normal life as the lockdown restrictions ease. Manual contact tracing will continue to play an important role, in particular for those such as the elderly, who could be more vulnerable to infection but less likely to have a mobile phone or have the digital skills to use such Apps. Many EU Member States have yet to launch contact tracing Apps, but it is likely there will be more activity in this area over the coming weeks due to the easing

of lock-down restrictions, and the recent launch by Apple and Google of their contact tracing API.

Are governments taking a privacy-friendly approach in their contact tracing apps?

Google & Apple joint initiative

Many governments around the world are developing contact tracing apps which meet the privacy standard advocated by Google and Apple, in order to ensure their apps will function effectively on Android and IOS devices. Google and Apple, the world's leading makers of smartphone operating systems, recently released their contact tracing API (known as the "*exposure notification*" API) to help prevent the spread of COVID-19. Some 22 countries (including Ireland) across 5 continents and a number of US states have already requested access to the software. Notable omissions are the UK and France.

The API is not itself a contact tracing App, rather it enables governments and public health authorities to incorporate the software into their own apps that people install. The API will enable Bluetooth technology to run in the background of the phone, including on a locked phone. Without this ability for background use of Bluetooth technology, the utility of Apps would be greatly decreased. Users would need to have their phones unlocked and turned on, for the Apps to be able to use Bluetooth and log encounters. Apple and Google are limiting use of their API technology to government contact-tracing Apps. Privacy activists have praised the protections offered by Apple and Google's API, as being in line with the principles of data protection by design and by default.

Google and Apple have explicitly barred use of the API in any apps that seek GPS location data from users, which means some apps being developed by public health authorities for contact tracing will not be able to use the API. In addition, the API can will only work on Apps using a decentralised system that uses randomly generated temporary keys created on a user's device (but not tied to their specific identify or information). The API allows public health authorities to define what constitutes potential exposure in terms of exposed time and distance, and they can tweak transmission risk and other factors according to their own standards.

Centralised Vs decentralised approach

One key issue of contention amongst governments is whether data collected by the App should be stored on a centralised basis (i.e. on a centralised system which public health authorities have access to) or decentralised basis (i.e. on a user's mobile device). The centralised approach enables national health authorities to make use of the data, by providing advice to users and their contacts as and when necessary. Whilst the decentralised basis, puts users in more control of their data, and alerts them automatically if they have been exposed to individuals infected with COVID-19. The EDPB accepts both the centralised or decentralised approaches as valid options, although the decentralised approach better aligns with the GDPR's data minimisation principle. Apple and Google have said that only decentralised Apps will be able to run continuously using Bluetooth on their IOS and Android devices. For centralised Apps to be able to run continuously, a phone would need to be left unlocked at all times.

Asia

The Chinese and South Korean governments are taking a more privacy intrusive approach to contact tracing, and effectively putting their citizens under mass surveillance.

China - The Chinese government has deployed an App called Alipay Health Code, which is mandatory, and uses location tracking. The authorities provide users with a QR (quick response) colour code in green, amber or red, based on their health status and travel history. These codes are scanned before allowing users entry to public transport or establishments.

South Korea - The South Korean government uses a contact tracing system known as the 'COVID-19 Smart Management System' (**SMS**), rather than a contact tracing app. SMS uses data from 28 organisations, such as National Police Agency, the Credit Finance Association, three smartphone companies, and 22 credit card companies, to trace the movement of individuals with infected with COVID-19. GPS location tracking, smartphone data, credit card data and

CCTV are all compiled to trace an individual's movements. The use of this surveillance method, and the excessive amount of data collected, creates fundamental privacy issues for citizens.

Singapore - In contrast, the Singaporean government has been widely praised for the privacy-friendly features of its TraceTogether App. The App is voluntary, and uses Bluetooth technology rather than GPS location tracking. Users receive a push notification to their phone when the Bluetooth field of their phone has overlapped with the field of an individual who has tested positive for COVID-19. It identifies users within 2m (6.6ft) of another person for more than 30 minutes. The App stores records of a user's Bluetooth encounters, and their duration, for 21 days on the user's phone. It generates encrypted data logs on the person's phone, which can be decrypted and analysed by the government where necessary. Unfortunately, it has emerged that only 20-25% of Singapore's population is using the App. The lower than expected uptake of the App may, in part, be due to the fact that it does not work properly when in the background on iphones, because of the way Apple restricts use of Bluetooth technology. However, this problem will be resolved through use of Apple and Google's API.

Europe

European countries are seeking to achieve similar success to China and South Korea in flattening the curve of COVID-19 infections, through deployment of contact tracing Apps, but without turning into totalitarian regimes. Most contact tracing Apps being developed by European governments are voluntary, and avoid GPS location tracking and a centralised database. These features are essential in order for the apps to work on Apple and Google's API.

Ireland - The Irish Government recently issued a statement and briefing for Minister Simon Harris on its proposed HSE COVID-19 contact tracing App. Use of the proposed App will be voluntary; use Bluetooth technology, and store data on a decentralised basis on the user's device, as required in order to use Apple and Google's API. Italy, Germany, Switzerland and Austria, amongst others, are also adopting these features in their contact tracing Apps. The proposed HSE App may also contain symptom tracker functionalities, in addition to contact tracing. While the App will not record or collect exact GPS location, infected users may be given the option of volunteering their "*general locality*". Whilst the HSE accepts location information is not necessary for contact tracing purposes, it said that such information would help public health experts to map, monitor and manage the spread of COVID-19. A group of civil societies, scientists and academics has reportedly written an open letter asking the HSE to follow the EDBP's recommendations by publishing the App's draft specification and user requirements, Data Protection Impact Assessment (**DPIA**) and source code, to enable public scrutiny of the App. The HSE is engaging with the Data Protection Commission (**DPC**) on privacy aspects of the App, to ensure it complies with data protection laws.

UK - The UK government is developing an App called NHSX. It is currently proposed that NHSX will be voluntary; use Bluetooth technology, and store data on a centralised database operated by the National Health Service (**NHS**). As previously discussed, if the latter feature is adopted, NHSX will not be able to benefit from Apple and Google's API. The UK Information Commissioner's Office (**ICO**) is having ongoing conversations with NHSX regarding its planned contact tracing App, and has published a discussion document setting out best practice recommendations. In particular, the ICO recommends that "*data should remain on the user's device as far as is reasonably practicable. Backend infrastructure should only collect that which is strictly necessary in the context of the functions it provides*". Like the UK, France and Norway are opting for a centralised system. The UK government has also published a DPIA in relation to the trial of NHSX in the Isle of Wight.

The different technical approaches being adopted by European governments to developing contact tracing Apps raises questions about the cross-border inoperability of the Apps. As most of these Apps are currently a work-in-progress, and details of their specifications are sketchy, it remains to be seen to what extent they will comply with EU privacy and data protection laws.

EU Guidance

European Commission Toolbox and Guidance

The European Commission has published a Common EU Toolbox on mobile contact tracing

Apps to support the fight against COVID-19, along with accompanying guidance. The toolbox and guidance set out a number of essential requirements for Member State's contact tracing Apps, including:

- voluntary use
- use Bluetooth proximity technology (not GPS location data)
- comply with the GDPR data protection principles
- have an appropriate legal basis for processing
- approved by the public health authority
- interoperable across the EU and
- dismantled when no longer needed.

EDPB Guidance

The EDPB published a letter welcoming the Commission's initiative to developing a pan-European coordinated approach to Apps supporting the fight against COVID-19. In addition, the EDPB published its own guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 pandemic. Its guidelines are in line with the European Commission's toolbox and guidance.

(i) EDPB Recommendations – Contact Tracing

The EDPB's guidelines set out a number of recommendations and requirements in regard to the development of contact tracing Apps, including:

- **Voluntary Use:** The systematic and large-scale monitoring of contacts between individuals is a grave intrusion into their privacy. It can only be legitimised by relying on voluntary adoption by users.
- **No location tracking:** Bluetooth data should be collected to determine the proximity between users of the App. Location tracking of individuals is not necessary for contact tracing purposes, and would violate the GDPR's data minimisation principle. It may also create major security and privacy risks.
- **Identify the controller:** The controller of any contact tracing App should be clearly identified. National health authorities may be controllers.
- **Data minimisation:** The App should not collect unnecessary information, such as call logs, location data, device identifiers, etc.
- **Purpose Limitation:** The purposes must be specific enough to exclude further processing for purposes unrelated to the management of the COVID-19 health crisis (e.g., commercial or law enforcement purposes).
- **Users and contacts should not be identifiable:** Use of the App should not allow the user or any contacts to be identified. Only pseudonymous identifiers should be collected and stored.
- **Implement a centralised or decentralised approach:** Data may be stored locally within individuals' devices (decentralised solution), or alternatively data may be stored on a centralised server. The EDPB is of the opinion that both are valid options, provided that adequate security measures are in place, but the decentralised solution is more in line with the GDPR data minimisation principle.
- **Security:** State of the art cryptographic techniques should be implemented to secure the data stored in servers and Apps, and any exchanges between Apps and the remote server. Mutual authentication between the App and server should also be performed.
- **Obtain user's consent to storage/access to information on user's device:** Storage and/or access to information already stored on the terminal equipment of the user, are subject to Article 5(3) of the ePrivacy Directive 2002/58/EC. If those operations are strictly necessary in order for the App provider to provide the service explicitly requested by the user, the processing would not require his/her consent (but the controller would still need to have a legal basis for processing the data under the GDPR/Data Protection Act 2018). For operations that are not strictly necessary, the App provider must obtain the user's prior consent.
- **Legal basis for processing personal data of users and contacts**: The mere fact that the use of contact tracing Apps takes place on a voluntary basis does not necessarily mean that the processing of personal data will be based on consent. Governments also, for example, have the option of relying on necessity for the performance of a task in the public interest (i.e. Art. 6(1)(e) GDPR). The basis for the

processing referred to in Art. 6(1)(e) must be laid down by EU or Member State law. The EDPB suggest that the enactment of national laws, promoting the voluntary use of the App could provide such a legal basis.

- **Legal basis for processing health data:** Where the App collects health data (for example the status of an infected person), the processing must meet one of the legal bases in Article 9 GDPR. The most relevant legal bases are: the processing is necessary for reasons of public interest in the area of public health under Article 9(2)(i) GDPR; or for health care purposes as described in Article 9(2)(h) GDPR. It might also be based on explicit consent under Article 9(2)(a) GDPR.
- **Storage limitation:** Timelines should consider medical relevance (incubation period etc.). Any data collected should be deleted as soon as possible, and once the crisis is over, the data should be erased or anonymised.
- **Accuracy:** The EDPB emphasises the importance of ensuring the accuracy of a declaration that a person is COVID-19 positive, as entering this information into the App may trigger notifications to individual contacts concerning the fact that they have been exposed. The EDPB suggest, as a solution, a one-time code that can be scanned by the person when the result of a test is given to him/her.
- **Privacy by design and by default:** Implement a data protection by design and by default approach when developing the App.
- **Source code:** An App's source code should be published for the widest possible scrutiny.
- **DPIA:** A DPIA should be carried out before implementing a contact tracing App and published, as the processing is likely high risk (i.e. health data; anticipated large-scale adoption; systematic monitoring; use of new technological solution).

(ii) EDPB Recommendations – Use of location data

The EDPB separately considers the conditions for the proportionate use of location data "*to assess the overall effectiveness of confinement measures*". In some Member States, governments envisage using mobile location data as a possible way to monitor, contain or mitigate the spread of COVID-19. The GDPR and ePrivacy Directive both contain rules allowing for the use of anonymous or personal data.

The EDPB highlight that there are two principal sources of location data:

a. *Location data collected by electronic communication service providers (i.e. telcos) in the course of the provision of their service*

The EDPB note that location data collected from electronic communication service providers may only be processed within the remits of Articles 6 and 9 of the ePrivacy Directive. That means that telcos may disclose location data to public authorities or other third parties only if it is: (i) anonymised or, (ii) with the user's prior consent.

b. *Location data collected by information society service providers' (ISSPs) whose Apps require the use of such data (e.g. navigation, transportation services, etc.)*

In regard to location data collected directly by ISSPs from the user's device, Article 5(3) of the ePrivacy Directive applies. That provision provides that the storing of any information (whether personal data or not) on the user's device or gaining access to information already stored is allowed only if: (i) the user has given prior consent or (ii) the storage and/or access is strictly necessary for the service explicitly requested by the user. In addition, information collected in compliance with Article 5(3) can only be further processed with the additional consent of the user or on the basis of an EU or national law, which constitutes a necessary and proportionate measure in a democratic society.

Accordingly, if national health or law enforcement authorities want to obtain mobile location data of identifiable individuals from telcos, or ISSPs want to store/access location data (or any other data) on users' devices that is not necessary for the intended functioning of the App, then they must obtain the user's prior consent to do so, to ensure compliance with the ePrivacy Directive.

Article 15(1) of the ePrivacy Directive does, however, provide for derogations from the above obligations, subject to legislative measures safeguarding rights and freedoms. In Ireland, for example, the Communication (Retention of Data) Act 2011 permits law enforcement authorities to obtain access to location data from telcos for the purpose of investigation of a serious offence,

safeguarding the security of the State, or the saving of human life. This may provide a legal basis for law enforcement authorities to obtain location data from telcos in order to monitor, contain or mitigate the spread of COVID-19.

The Outlook

It is widely recognised that, when combined with other measures such as social distancing, contact tracing Apps can help in the fight against COVID-19. In a European context at least, acceptance and widespread voluntary use of these Apps will depend on the public trusting that any interference with their privacy and data protection rights by public authorities is kept to a minimum.

Even where strong privacy safeguards are implemented (as with the Apple and Google initiative), it is far from certain that the public will sign up in sufficient numbers to make Apps an effective contact tracing tool. In the face of low public acceptance, EU Member States will have to grapple with whether to switch to a mandatory App policy (similar to some Asian countries) or to abandon Apps as a part of their contact-tracing programmes, relying instead on traditional methods.

A mandatory App policy would clearly be at odds with existing European Commission and EPDB guidance, and any EU Member State law that imposed such a requirement would inevitably face a swift legal challenge. In any case, there does not appear to be an appetite among EU Member States to pursue a mandatory App policy.

The utility of contact tracing Apps in Europe very much hangs in the balance. To ensure success, governments will need to embark on a sustained public campaign of awareness and persuasion to convince their citizens that contact tracing Apps are a public good and that privacy safeguards are robust.

Our team

John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Claire Morrissey
Partner
+353 1 649 2246
cmorrissey@algoodbody.com

Andrea Lawler
Partner
+353 1 649 2351
alawler@algoodbody.com

Andrew Sheridan
Partner
+353 1 649 2766
asheridan@algoodbody.com

Davinia Brennan
Associate, Knowledge Lawyer
+353 1 649 2114
dbrennan@algoodbody.com