PAUL HASTINGS

STAY CURRENT

April 2020

Follow @Paul_Hastings

Do You Know Who You Came Into Contact With Today? Contact Tracing in the EU: A Guide

By Sarah Pearce & Ashley Webber

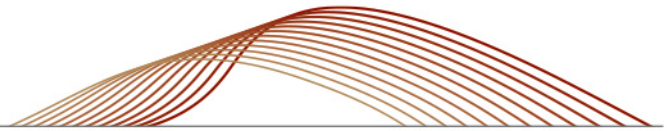
COVID-19 continues to have life-altering effects on individuals and businesses globally. A question asked daily by many is: how can we flatten the COVID-19 curve and ultimately, how can we defeat COVID-19? Several solutions have been posed in response to this with one such solution starting to see a lot of traction: **contact tracing**. Contact tracing is method of identifying and alerting people who have come into contact with a person infected with COVID-19. In the initial stages of the outbreak, this was carried out in many countries by speaking to patients and encouraging them to speak to those they had been in contact with. But of course, COVID-19 has developed at such a pace and magnitude that simply speaking to those infected would not be enough to help tackle the issue. The proposed alternative is to develop and use contact tracing apps which would allow smartphones to quickly and automatically determine whether somebody has been in contact with an infected person.

Using location tracking technologies within devices and apps to contact trace for COVID-19 purposes is currently being undertaken in certain countries around the world, including South Korea, China, Israel, and Singapore. It also being used, or is under consideration and likely to be used, in certain EU countries, including France, Italy, the Netherlands, and others. To do so, different methods have been adopted or are being considered including optional or necessary app plugins for existing apps, and the development of entirely new apps with the sole purpose of contact tracing.

Whilst experts in the use of contact tracing are confident in its benefits with respect to helping quash the spread of COVID-19, there are serious regulatory considerations that must be taken into account before contact tracing apps are to become the norm, largely in relation to data privacy and the protection of individuals' personal data. As discussed in a previous article, whilst regulators are sympathetic to the changing circumstances and do not want to hinder measures that are intended to help during the crisis, regulators across the UK and EU have been very clear in delivering the message that compliance with data privacy laws and principles should remain a key focus. And therefore, when developing and using contact tracing apps, data privacy should be at the forefront of developers and national authorities minds.

At What Stage Are We with Respect to Contact Tracing in the UK and Across the EU?

As noted above, contact tracing is already being used to differing degrees in EU member states. For example, the Czech Republic is piloting the use of location data from mobile operators to construct "memory maps" of where individuals have spent significant time within the last five



days, France is using Bluetooth to detect transmission chains for COVID-19 to help limit the spread, and Italy launched and completed an open call to assess the state of the mobile apps for contact tracing, and selected two candidate solutions, currently at the beta version stage, to be tested in the field, before national roll-out.

The Contact Tracing Toolbox

With this in mind, on 7 April 2020, the European Data Protection Board held a remote meeting focusing on processing personal data to fight COVID-19 in which a mandate was requested regarding geolocation and other tracing tools in the context of COVID-19. On 16 April 2020, the e-Health Network with the support of the European Commission (referred herein together as the EU Commission) published the Common EU Toolbox for Member States (the "Toolbox") related to mobile applications to support contact tracing in the EU's fight against COVID-19.

The aim of the first draft of the Toolbox is to set out the various relevant parameters to enable a coordinated development and use of officially recognised contact tracing applications and the monitoring of their performances: the "*pan-European approach for officially recognised COVID-19 mobile applications*". The Toolbox is intended to operate as a "common approach" across the EU to ensure interoperable and privacy-preserving digital contact tracing is applied consistently by all member states. Note that the Toolbox applies only to **nationally developed apps that are voluntarily installed** and alert people who have been in proximity with an infected person, the Toolbox does not consider covert-tracing or other involuntary tracing.

The Toolbox provides the following baseline requirements and functionalities (discussed further below) which it considers to be the essential minimum requirements for **nationally operated** contact tracing apps, namely they must be:

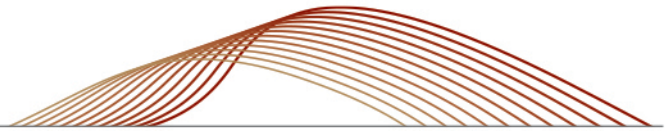
1. **Voluntary**;
2. **Approved** by the national health authority;
3. **Privacy-preserving**—personal data must be securely encrypted; and
4. **Dismantled** as soon as no longer needed.

The Toolbox will be discussed further below but as a general comment, the Toolbox reminds us that whilst we are living in unprecedented times, the rights of individuals with respect to their personal data should not be overlooked, nor undermined. We have seen huge advances in recent years with respect to data privacy regulation globally and these should continue to be upheld. The EU Commission is continuing to further develop and implement the Toolbox, including addressing other types of apps and the use of mobility data for modelling to understand the spread of the disease and facilitate exit from the crisis.

Contact Tracing Framework

Whilst not a focus of this article, it is worth highlighting the joint initiative, referred to as the Contact Tracing Framework, launched by Apple and Google said to "*enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design*". The Framework comprises a two-stage plan to implement its solution:

1. In May, both companies will release APIs that enable interoperability between Android and iOS devices using apps from public health authorities. These official apps will be available for users to download via their respective app stores; and



2. In the coming months, the two companies will work to enable a broader Bluetooth-based contact tracing platform by building this functionality into the underlying platforms. According to the businesses, this is a "*more robust solution than an API and would allow more individuals to participate*" if they choose to.

The UK and the Information Commissioner's Office (the "ICO")

As discussed in a previous article, the ICO has been proactive during the COVID-19 crisis: its response has been swift and it continues to provide guidance with respect to the processing of personal data during this time. In line with this, the ICO has published its own views and recommendations with respect to using new technologies, such as contact tracing, to combat COVID-19. Such recommendations are considered further below but the overarching message from the ICO is consistent with that given since the start of the outbreak: new technologies must still be compliant with data privacy laws and principles, and the public needs to have confidence that this is the case.

In addition to issuing its own recommendations, the ICO has also published an official Opinion on the Contact Tracing Framework announced by Apple and Google (as permitted by Section 115(3)(b) of the Data Protection Act 2018 which allows the ICO to issue Opinions to Parliament, Government or other institutions and bodies as well as to the public on any issue related to the protection of personal data). The Opinion analyses the Contact Tracing Framework in light of data privacy principles and concludes that the Contact Tracing Framework is "*aligned with the principles of data protection by design and by default, including design principles around data minimisation and security*" and that any app developers seeking to use the Contact Tracing Framework to develop contact tracing apps should ensure the apps are subsequently developed in accordance with applicable data privacy laws and principles.

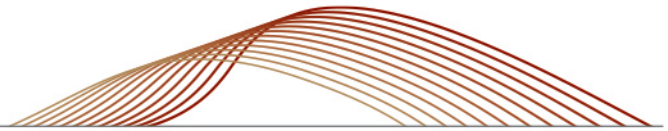
What Are Some of the Key Areas of Data Privacy Compliance That Should Be Considered?

Contact tracing collects a significant volume of personal data and naturally there are several areas of the data privacy law which should be highlighted as concerns and considered key when developing and operating national contact tracing applications.

Privacy by Design

Underlying all the points that follow is the principle of privacy by design which remains paramount. Whilst not a new principle or theory at the time, the General Data Protection Regulation ("GDPR") took the step to expressly include privacy by design as a requirement for all organisations processing personal data: privacy by design requires an organisation, "*both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures…which are designed to implement data-protection principles…in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of [the GDPR] and protect the rights of data subjects*".

Privacy by design therefore requires organisations, including national authorities, developing apps such as contact tracing apps to ensure they are developed in a manner which is compliant with the law—compliance should not be an afterthought. The ICO notes that, at an absolutely minimum, a data protection impact assessment should be prepared by each contact tracing app developer with respect to its technology. Both the ICO and the EU Commission are clear that privacy by design is key. The ICO states that privacy by design is "central to the law" and the EU Commission demonstrates its support by making it a requirement that contact tracing apps are developed and designed with the input of national health authorities. The national health authorities will be crucial



in determining several functionalities of the app including, for example, the form of message to be sent to those individuals who have found to have been in contact with an infected person.

Lawfulness, Fairness and Transparency

The principle of lawfulness, fairness and transparency covers a series of specific obligations, all of which should be complied with by organisations and member states developing and operating contact tracing apps. However, of such obligations, three merit further discussion:

1. the lawful basis relied upon to process the personal data: **consent**;
2. the requirement to **provide notice** to the data subjects; and
3. **data subjects rights**.

1. *Consent*

As noted above, the Toolbox requires that a contact tracing app is voluntary (at least at this stage, noting that the Toolbox is yet to consider involuntary contact tracing). From a legal perspective, this translates to the requirement under the GDPR to have a lawful basis to process personal data—**the lawful basis said to be required is the consent of the individual**.

The ICO touches on this discussion in its Opinion in which it analyses the phased approach considered in the Contact Tracing Framework. The ICO states:

> Any app built using the CTF [Contact Tracing Framework] will be provided via the applicable mobile Operating System ("OS") app store, and is subject to the same requirements as any other app within that app store. In addition, users have the ability to remove or disable the app. However we understand that in the 'Phase 2' plans the CTF API will form part of each mobile device's OS. This means that even a mobile device user who removes or disables an app will not be able to easily refuse or remove OS updates that continue to provide the CTF API, which enables apps to use this data. This might change but for the time being, across the EU and likely the UK, this should be the choice of the individual.

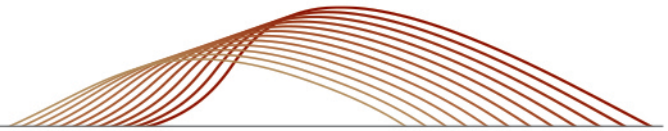
The Phase 2 plans do not coincide with the requirements of the EU Commission to ensure the contact tracing apps are voluntary. However it is worth reiterating that the Toolbox is in its first draft: the EU Commission is continuing to develop its recommendations and it is very likely that we will see recommendations in the near future that relate to involuntary, or partially involuntary, contact tracing.

That being said, the position in the UK and across the EU at this stage is fairly sound: contact tracing should be carried out with the consent of the individual only.

2. *Notice*

It is well established and understood in the UK and across the EU that when an organisation purports to process the personal data of an individual, it must provide specific information, normally in the form of a notice, to the individual concerned. This requirement will be no different for contact tracing apps and those in the processing of developing such apps should be preparing their notices simultaneously, with the requirements of the law and advice from regulators and EU authorities in mind.

It is briefly worth noting that the Toolbox also considers how notice should be given to those individuals who have come into account with an infected person. In doing so, the Toolbox provides flexibility for member states with respect to each of their own national health



authorities and diagnoses procedures but does make clear that national health authorities should always be at the core of designing this process, including the formulation of message to be provided to an individual found to have been in contact with an infected person.

In addition, the Toolbox considers options for how the notice should be provided in practice, for example whether this should come directly from the health authority or whether the health authority should instruct the app to do so on its behalf, using its approved message.

3. *Data Subject Rights*

The law provides a series of rights for data subjects to exercise with respect to their personal data—the core message of continued compliance in both the Toolbox and the ICO's publications means that such rights must continue to be exercisable by data subjects when operating the contact tracing apps. Particularly in light of voluntary opt-in, there should be an equal right to opt-out i.e. withdraw their consent. The individuals should also be able to, for example, request access to the data processed about them. Whilst this may change as contact tracing and the need for it evolves, app developers should ensure they are fully equipped to comply with such rights requests.

Data Minimisation

The GDPR states that organisations should only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed, and this principle of data minimisation is reiterated by the ICO and the EU Commission. Contact tracing apps should therefore only process the personal data which is required to meet the purpose of identifying whether an individual has come into contact with an infected person.

In order to comply with the principle and prevent the storing of unnecessary personal information, the Toolbox categorises contact tracing apps into two groups the first of which is referred to by the ICO in its publication. The Toolbox notes that any options where directly-identifiable data on every person downloading the app is held centrally by public health authorities, would have major disadvantages and likely not be in compliance with the law.

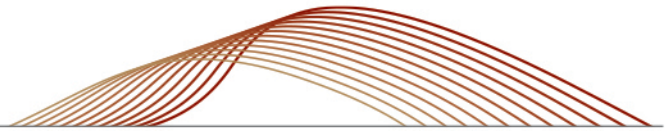
1. *Decentralised Processing*

This is the process of undertaking as much data processing as possible on the individual's device. The proximity data related to contacts generated by the app remains only on the device. The app generates an identifier of the device that is in contact with the user which is then stored on that device with no additional personal information. Unlike many other apps, the provision of mobile phone numbers or other personal data by the user at the time installation is not necessary, because an alert is automatically delivered via the app the moment a user notifies the app that they have tested positive.

According to the Toolbox, this approach would "*considerably reduce the risks to privacy as close contacts would not be directly identifiable and this option would thereby enhance the attractiveness of the application*." However, an apparent downside is that health authorities would not have access to any anonymised and aggregated information on social distancing, the effectiveness of the app or indeed the potential transmission of COVID-19. Such information could be seen as important to monitor the effectiveness of the apps and the spread of COVID-19.

2. *Backend Server Solution*

This is the process of using a backend server held by the public health authorities to store only the arbitrary identifiers generated by the app (whereby users cannot be identified). Unlike the decentralised system, this allows the data stored in the server to be anonymised by



aggregation and further used by public authorities as a source of important information on the effectiveness of the app in tracing and alerting contacts plus the aggregated number of people that could potentially develop symptoms.

Given the analytical benefits of the latter option, it seems likely this will be preferred by most countries.

Security

One of the key elements of the GDPR, and data privacy legislation globally, is security, and therefore it is unsurprising that both the EU Commission and the ICO have both expressly stated the importance of security in the development and operation of contact tracing apps. This is expressed clearly in the Toolbox: "*Cybersecurity for these mobile applications, as well as the backend and any associated services is critical. Member States' authorities and the developers of these applications should therefore take a series of measures to ensure adequate cybersecurity throughout the lifecycle of the applications*".

What measures are suggested to do so? Whilst the ICO does not go into specific detail, the Toolbox provides for recommended cybersecurity requirements that have been compiled by the European Union Agency for Cybersecurity. These include, but are not limited to, the use of encryption, communications security, secure development practices, and user authentication.

The responsibility of ensuring such security measures are in place falls to both the app developers and the national authorities of member states. In addition to the measures highlighted above, the Toolbox also recommends member states carry out a national risk assessment to identify and mitigate possible risks of abuse and ensure that, once the apps are deployed, the appropriate cybersecurity agencies are prepared to respond to any potential incidents and cooperate with other member state agencies.

Retention

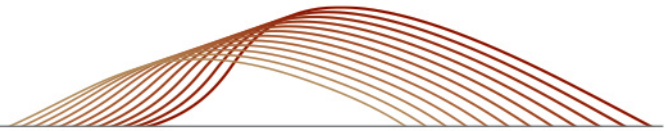
Personal data should be processed for no longer than is necessary for the purposes for which it was collected meaning contact tracing apps, or health authorities, should not process the data for longer than contact tracing is required and permitted.

As noted above, a baseline requirement under the Toolbox for contact tracing apps is that they include a function for "*Automated/gentle self-dismantling, including deletion of all remaining personal data and proximity information, as soon as the crisis is over*".

At this time, no one can confidently predict when the COVID-19 crisis will be over so in accordance with privacy by design, the developers should build the dismantling function into the apps in order to ensure that when the time does come, the privacy rights of the individuals are respected. Note this could equally apply to any health authorities or other such public bodies holding personal data related to contact tracing. The ICO encourages the continued preparation of privacy impact assessments during the operation of any contact tracing applications to ensure this obligation is met when the time comes.

What Should Be Taken Away from This?

Whilst at the start of 2020, the concept of contact tracing may have been alien to some, or viewed by privacy activists or privacy-conscious individuals as a concept which would not have been permitted by law, it is now something we will likely all begin to see rolled out in the countries in which we live, in varying forms.



The goal of contact tracing is to assist in slowing the spread of COVID-19 and ultimately defeating it. This is undeniably an EU—and global—mission, and the EU Commission's view is that this must be done in a cooperative manner across the EU.

Nevertheless, the authorities have confirmed in the discussed publications, and other statements, that pursuit of this mission by contact tracing should not be to the detriment of, and should not undermine, the rights of individuals with respect to their personal data and must always be in compliance with the law.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings London lawyers:

Sarah Pearce
44.020.3023.5168
sarahpearce@paulhastings.com

Ashley Webber
44.020.3023.5197
ashleywebber@paulhastings.com