COVID-19: PEOPLE: ICO OPINES ON APPLE AND GOOGLE'S CONTACT TRACING TECHNOLOGY (UK)

27 April 2020 | London
Legal Briefings – By **Miriam Everett, Hannah Brown and Ghislaine Nobileau**

On 17 April 2020, the ICO published an opinion by the Information Commissioner (the "**Commissioner**") on Apple and Google's joint initiative to develop COVID-19 contact tracing technology (the "**Opinion**", available here).

SUMMARY

- The Commissioner found the CTF to be aligned with principles of data protection by design and by default.
- Controllers designing contact tracing apps that use the CTF should ensure alignment with data protection law and regulation, especially if they process personal data (which the CTF does not require).
- The Commissioner raised concerns regarding individuals assuming that the CTF's compliance with data protection principles will extend to all aspects of the contact tracing app - which is not necessarily the case.
- Therefore, it should be made clear to any app users who is responsible for data processing, especially if the app processes data outside of the CTF's limited scope.
- Data controllers designing CTF-enabled contact tracing apps must be transparent with potential and actual app users on the type of information they will be processing.
- Finally, when it comes to a user's ability to disable Bluetooth, the Commissioner

observed that with regard to contact tracing apps in general: *"a user should not have to take action to prevent tracking*".

As set out in our previous blogpost (available here), contact tracing is one of the measures being contemplated or implemented by European governments (including in the UK and Germany) in order to be able to put an end to lockdowns while containing the spread of the virus.

The scope of the Opinion was limited to the design of the contact tracing framework which enables the development of COVID-19 contact tracing apps by public health authorities through the use of Bluetooth technology (the "**CTF**").

It is also worth noting that this Opinion has been published in the midst of a heated debate on contact tracing technology and fears that it may be used for mass surveillance - in an open letter published on 20 April 2020, around 300 international academics cautioned against creating a tool which will enable large scale data collection on populations.

HOW DOES THE CTF WORK?

The CTF is composed of "*application programming interfaces*" as well as "*operating system level technology to assist contact tracing*". The collaboration between Apple and Google will result in interoperability between Android and iOS devices of apps developed by public health authorities using the CTF.

When two devices with contact tracing apps come into proximity, each device will exchange cryptographic tokens (which change frequently) via Bluetooth technology. Each token received will be stored in a 'catalogue' on the user's device, effectively creating a record of all other devices a user has come into contact with. Once a user is diagnosed with COVID-19, and after they have given their consent, the app will upload the stored 'catalogue' of tokens to a server. Other users' devices will periodically download a list of broadcast tokens of users who have tested positive to COVID-19. If a match is found between the broadcast tokens and the 'catalogue' of tokens stored on each user's device, the app will notify the user that he/she has come into contact with a person who has tested positive and will suggest appropriate measures to be taken.

HOW DOES THE CTF COMPLY WITH DATA PROTECTION LAWS?

The Opinion finds that, based on the information released by Google and Apple on 10 April 2020, the CTF is compliant with principles of data protection by design and by default because:

1. **The data collected by the CTF is minimal**: The information contained in the tokens exchanged does not include any personal data (such as account information or usernames) or any location data. Furthermore the 'matching process' between tokens of

users who have tested positive for COVID-19 and tokens stored on each user's phone happens on the device and therefore does not involve the app developer or any third party.

2. **The CTF incorporates sufficient security measures:** The cryptographic nature of the token which is generated on the device (outside the control of the contact tracing app) means that the information broadcast to other nearby devices cannot be related to an identifiable individual. In addition, the fact that the tokens generated by one device are frequently changed (to avoid ultimate tracing back to individual users) minimises the risk of identifying a user from an interaction between two devices.

3. **The user maintains sufficient control over contact tracing apps which use the CTF:** Users will voluntarily download and install the contact tracing app on their phone (although this may change in 'Phase 2' of the CTF as discussed below). Users also have the ability to remove and disable the app. In addition, the process of uploading the collected tokens of a user to the app once he/she has tested positive by the developer requires a separate consent process.

4. **The CTF's purpose is limited:** Although the CTF is built for the limited purpose of notifying users who came into contact with patients who have tested positive for COVID-19, the Commissioner stresses that any expansion of the use of CTF-enabled apps beyond this limited purpose will require an assessment of compliance with data protection principles.

WHAT CLARIFICATIONS ARE REQUIRED?

The Commissioner raises a number of questions on the practical functioning of the CTF, especially in respect of collection and withdrawal of user consent post-diagnosis. It is unclear how the CTF will facilitate the uploading of stored tokens to the app. Although consent will be required from the user, clarity is needed on: (i) management of the consent signal by a CTF-enabled app and (ii) what control will be given to users in this respect. In addition, the Commissioner lacks information on how consent withdrawal will impact the effectiveness of the contact tracing solutions and the notifications sent to other users once an individual has been diagnosed.

ISSUES FOR DEVELOPERS

The Commission will pay close attention to the implementation of the CTF in contact tracing apps. In particular, the CTF does not prevent app developers from collecting other types of data such as location. Although reasons for collecting other types of user information may be "*legitimate and permissible*" in order to pursue the public health objective of these apps (for example to ensure the system is not flooded with false diagnoses or to assess compliance with isolation), the Commissioner warns that data protection considerations will need to be assessed by the controller - this includes the public health organisations which develop (or commission the development of) contact tracing apps.

Another issue raised by the Commissioner is the potential user assumption that the compliance by the CTF with data protection laws will radiate to all other functionalities which may be built into contact tracing apps. In this regard, the Commissioner reminds app developers that, in addition to assessing data protection compliance in relation to other categories of data processed by the app, they will need to clearly specify to users who is responsible for data processing - in order to comply with transparency and accountability principles.

Finally, the Commissioner stressed that data controllers, such as app developers, must assess the data protection implications of both (i) the data being processed through the app and (ii) data undertaken by way of the CTF in order to ensure that both layers of processing are fair and lawful.

WHAT HAS THE ICO SAID ABOUT 'PHASE 2' OF THE CTF?

'Phase 2' of development of the CTF aims to integrate the CTF in the operating system of each device. The Commissioner notes that users' control, their ability to disable contact tracing or to withdraw their consent to contact tracing should be considered when developing the next phase of the CTF.

With regard to user's ability to disable Bluetooth on their device, the Commissioner observes in respect of 'Phase 2' of the CTF, and contact tracing apps in general, that "*a user should not have to take action to prevent tracking*".

HOW DOES THIS OPINION AFFECT THE DEVELOPMENT OF DECENTRALIZED PRIVACY-PRESERVING PROXIMITY TRACING PROTOCOL?

The Opinion can be applied to Decentralized Privacy-Preserving Proximity Tracing (or DP-3T) protocol in so far as it is similar to the CTF. The Commissioner states that the similarities between the two projects gives her comfort that "*these approaches to contact tracing app solutions are generally aligned with the principles of data protection by design and by default*".

INSIGHT

This Opinion is an important step in the development and roll out of contact tracing apps in the UK. As mentioned above, contact tracing is one of the tools necessary for the UK Government to lift the lockdown measures while minimising the impact of a potential second wave of infections. This has an indirect impact on the private sector as it will affect how and when employees will be able to go back to work.

The fact that the principles on which the CTF is based are compliant with data protection laws is crucial to the successful roll out of contact tracing apps. In order for these apps to be effective, they must be voluntarily downloaded by a large number of mobile users. Given the concerns around letting governments accumulate data on the population under the guise of putting an end to the pandemic, trust is a determining factor in this equation. The fact that the Commissioner is approving the foundation for these contact tracing apps will certainly play a role in gaining the public's trust and its acceptance to give up some privacy rights in order to put an end to the current public health crisis.

[More on COVID-19]

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

MIRIAM EVERETT
PARTNER, LONDON

+44 20 7466 2378
Miriam.Everett@hsf.com

HANNAH BROWN
ASSOCIATE, LONDON

+44 20 7466 2677
hannah.brown@hsf.com

LEGAL NOTICE