Information Commissioner's Opinion:

Apple and Google joint initiative on COVID-19 contact tracing technology

17 April 2020

Reference: 2020/01

Information Commissioner's Office

Summary

The Information Commissioner (the Commissioner) has previously provided guidance to organisations and to individuals regarding aspects of personal data processing and COVID-19.

This Opinion sets out the Commissioner's current thinking regarding a joint initiative by Apple and Google (which we are calling the Contact Tracing Framework (CTF)) to enable the use of Bluetooth technology to help governments and public health authorities (PHAs) reduce the spread of the virus.

Key messages

- The proposals for the CTF itself appear aligned with the principles of data protection by design and by default. This is based on the understanding that the CTF is designed to:
    - only generate a limited amount of data from the user's device, that is then made available via the CTF application programming interface (API). This data includes periodically-generated cryptographic tokens (we have used the term 'tokens' for clarity, noting that the Apple and Google documentation calls these numbers 'identifiers') created on that device, and stored tokens collected from nearby devices via Bluetooth. Tokens are not associated with other data that may further identify or locate the device user; and
    - support the use of these tokens as part of a specific methodology for contact tracing, through their upload from a COVID-19 diagnosed user to a central server and subsequent notification to other app users from that server, with this process only matching tokens stored on a particular device (with the match only occurring on the device), if it had been in the proximity of the diagnosed user's device.
- The CTF is therefore intended to support the development of apps that protect their users' identities, both before any risk of infection has been identified and when a COVID-19 infection notification is made via the app.
- However, it will be possible for those developing COVID-19 contact tracing apps – anticipated to be whitelisted PHAs and similar organisations – to design apps that use the CTF but also collect other data and use other techniques beyond those envisaged by the CTF.

- Organisations designing contact tracing apps are responsible for ensuring the app complies with data protection law where it processes personal data and the organisations are the controllers for that data. This is especially important because individuals may believe that the data protection by design and by default principles used in the development of the CTF extend to all aspects of a contact tracing app that is built to use the CTF, which may not necessarily be the case. If the app processes data outside the CTF's intended scope, then the controller should ensure it assesses the data protection implications of this processing (along with any undertaken by way of the CTF) and ensure that the processing is fair and lawful. It is also crucial that the processing is transparent.
- The Commissioner notes that the CTF's underlying principles are similar to the proposed 'Decentralized Privacy-Preserving Proximity Tracing' ('DP-3T') system. While this Opinion is about the CTF, where these similarities exist the Commissioner's views are equally applicable to the DP-3T proposals.
- This is a fast moving and highly complex situation. Apple and Google have stated that they acknowledge the CTF initiative is an ongoing project, that will doubtless evolve over time. There are also plans for a 'Phase 2' of the work that could see additional functionality. The Commissioner will remain engaged in this work as it continues.
- The Commissioner is pleased that the hard work, innovation and collaboration of many different parties is enabling these vitally important contact tracing solutions to be developed, while supporting data protection compliance and good practice. She agrees that apps should espouse robust security (including the use of encryption, and covering each stage of the data processing), data minimisation, transparency and user control, and that any supporting technology, including centralised processing to support contact tracing, should follow the same principles. She believes this work to be evidence that innovation and data protection are complementary concepts. The Commissioner will continue to promote and support data protection best practice across all initiatives seeking to address the COVID-19 pandemic.

About this Opinion

What is the status of this Opinion?

Section 115(3)(b) of the Data Protection Act 2018 (DPA 2018) allows the Commissioner 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 Commissioner can issue Opinions on her own initiative or on request.

The Opinion represents the Commissioner's view at the time of publication. It is based on the publicly available information about the CTF and the joint communications made by Apple and Google on 10 April 2020 (see Further Reading at the end of this Opinion), and only pertains to 'Phase 1' of the project as outlined in those documents.

The Commissioner reserves the right to make changes, publish new Opinions or form a different view based on further findings or other changes in circumstances.

Who is this Opinion for?

This Opinion is primarily for organisations involved in the CTF's development, as well as organisations developing apps that may use the CTF and other stakeholders that wish to understand the Commissioner's position on this initiative. It may also be of interest to those involved in other contact tracing initiatives.

What is the purpose of this Opinion?

This Opinion summarises the Commissioner's view of the joint initiative by Apple and Google to enable the use of Bluetooth technology to help governments and health agencies use contact tracing to reduce the spread of COVID-19.

Background

COVID-19 contact tracing

Contact tracing techniques seek to ascertain whether any individual has been in contact with an infected person during the time they were possibly infectious. Contact tracing could be used to support prompt communications with individuals who may be at risk of infection to ensure they:

- are aware of the risk;
- are provided with the appropriate information;
- take the appropriate steps to protect themselves and others; and
- receive any other support they may need.

Contact tracing has the potential to be used effectively as part of a package of measures and policies to manage social distancing and social or professional gatekeeping. It may therefore enable any potential measures that would support the easing of lockdown or other restrictions (eg immunity verification or immunity passport proposals).

The Commissioner understands that a number of these proposals are being advanced, and recommends that there is transparency around initiatives that link to COVID-19 tracing apps and that any solution is privacy-preserving in nature.

Contact tracing may be undertaken manually, relying on information provided by the infected person and others regarding their movements and interactions, during the time they may have been infectious. Recently, there has been substantial focus on the possibility of supporting traditional contact tracing using automated tools, including the functionality available to many people on their mobile devices (eg their smart phone), as a means of addressing the COVID-19 pandemic.

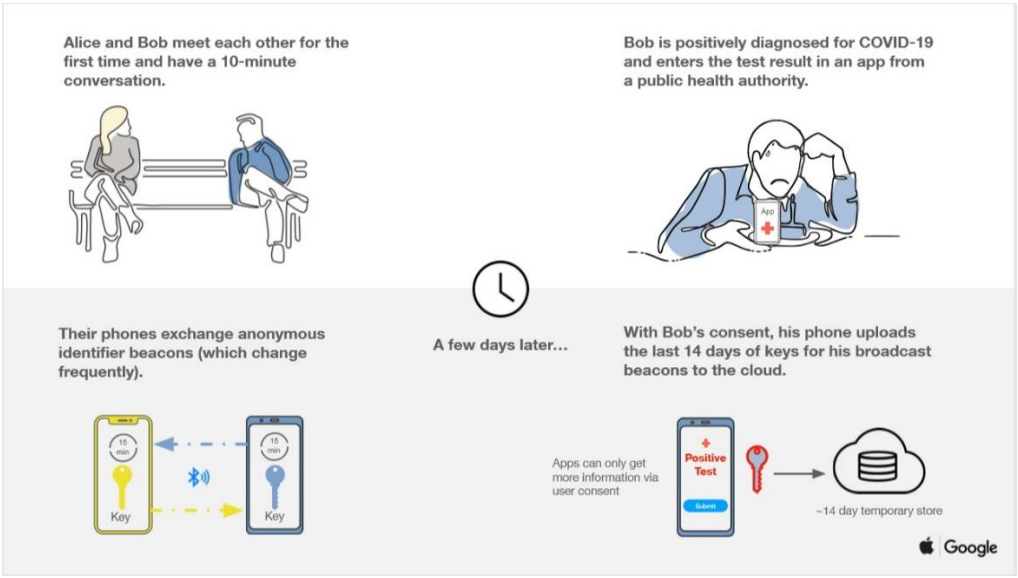
The Google and Apple initiative

On 10 April, Apple and Google announced they would be launching:

‘a comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing […] 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.’

The CTF is not itself a contact tracing app, and Google and Apple are not yet proposing to build such an app, although they have indicated that they intend to develop more functionality into their solution. For now, the aim is to enable third parties, such as PHAs, to create contact tracing apps that exchange information via Bluetooth Low Energy between devices.

A simple explanation of how an app is envisaged to work has been provided by Google and Apple. (The Commissioner notes that this explanation includes Google’s terminology for the proposals, which slightly differs from the terminology in this Opinion). This is reproduced below:

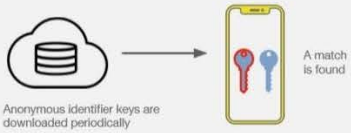


Alice continues her day unaware she had been near a potentially contagious person.

Alice sees a notification on her phone.

Sometime later...

Alice's phone periodically downloads the broadcast beacon keys of everyone who has tested positive for COVID-19 in her region. A match is found with the Bob's anonymous identifier beacons.



Alice's phone receives a notification with information about what to do next.

Additional information is provided by the health authority app or website

Google

Discussion

The first part of the following discussion deals with the CTF itself and the second with contact tracing apps that may be developed using the CTF.

Assessment of the CTF

Data minimisation

The CTF appears, based on this initial review, to comply with the data minimisation principle. Our review suggests:

- the exchange of information between devices does not include personal data such as account information or usernames;
- matching processes take place on-device and are not undertaken by the app host or with the involvement of any other third party; and
- the information required for the core functionality of contact tracing apps built using CTF does not use location data, either in the exchange between devices, the upload to the app host or subsequent notifications to other users from the app host.

However, the CTF provides the possibility for app developers to process more information than may be required for contact tracing purposes. This is discussed below.

User control over apps built using the CTF

The Commissioner notes that in the contact tracing proposals seen so far, app installation is voluntary and the post-diagnosis upload of stored tokens to the app developer requires a separate consent process.

Any app built using the CTF 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. The Commissioner is not suggesting that they need to, but that this should be noted.

The user can also disable Bluetooth on their device. The Commissioner observes that, with regard to the possible development of Phase 2 of the CTF, and also with regard to the development of contact tracing apps in general, and as with other cases where the onus is on a user to protect against being tracked, a user should not have to take action to prevent tracking.

Additionally, the Commissioner notes that more general considerations are required regarding the implications for individual rights and freedoms if the user chooses to not disable Bluetooth (or indeed uninstalls, or does not install, the apps envisioned here), particularly in terms of future proposals for immunity testing and immunity passports or access to services.

Security

As for the security principle, it appears that under the CTF, the exchange of information between devices and the upload of information to the app host incorporate a number of security measures. The CTF documentation indicates the use of appropriate cryptographic functions with additional safeguards. Cryptographic techniques are a means of mitigating risks to the security of the data being processed, for example:

- the generation of tokens takes place on the device and is not under the control of the contact tracing app utilising the API, using cryptographic techniques to ensure that information broadcast to other devices is not directly related to an identifiable individual. The exchange of tokens between devices do not indicate COVID-19 status, therefore the device-to-device level exchange of information does not directly result in app users knowing who has been diagnosed. While there may be circumstances where an individual could determine the identity of a diagnosed user (eg if they had only been in recent contact with a few people they know), these measures address risks about identification in circumstances such as public spaces;
- if a user is diagnosed they can voluntarily upload the stored tokens on their device to the app host (eg a PHA) via an encrypted communications channel. The app host in turn lets other app users know that they may be at risk because they had recently been in close proximity to the diagnosed user, but this does not directly identify the diagnosed individual. While this is not intended to enable users to look up the tokens of COVID-19-positive users, the Commissioner understands that this may be possible, but only for a

technically advanced attacker in specific circumstances, meaning this risk appears low;

- the second-stage transfer of data to the app host is likely to be undertaken via transport layer security (TLS), as is the case with most other contact tracing proposals, particularly given the requirements of the two mobile operating systems; and
- no persistent user ID is broadcast. Instead, a sequence of pseudo-random tokens representing changing user IDs are broadcast. This means that the risk of identifying a user from the interaction between phone A and phone B in the moment is likely to be low.

This analysis is limited to the information provided so far; the Commissioner may provide additional assessment of the security measures of any cloud-based infrastructure in due course.

Purpose limitation and risks of scope creep

Purpose limitation is a core principle of data protection internationally. It is about limiting use of personal data to the purpose for which it was collected or purposes compatible with that purpose. As indicated earlier, the CTF is a very new initiative and there are already signs that it will continue to evolve. Third-party app developers may also develop functionality that involves collection of additional data or new uses of existing data. This risks expanding the use of CTF-enabled apps beyond the stated purpose of contact tracing for COVID-19 pandemic response efforts. The Commissioner will monitor all developments, with an eye to ensuring that this purpose does not expand outward, in the phenomenon known as scope creep.

Current alignment with the proposed DP-3T system

The CTF is a joint initiative of Apple and Google and is not directly associated with the DP-3T initiative of a separate expert group. However, the underlying principles of the CTF appear to be similar to those proposed in the DP-3T protocol. The similarities between the two projects give the Commissioner further comfort that these approaches to contact tracing app solutions are generally aligned with the principles of data protection by design and by default.

The Commissioner has not undertaken a detailed technical review of the proposed DP-3T system. As noted above, the review of the CTF is based on the information made available on 10 April 2020. As such, there may be differences in the detailed approach undertaken by the two proposals. In addition, as the two initiatives have different stakeholders and

governance, they may further diverge over time. However, at the date of publication of this Opinion the Commissioner believes that a number of the points included in this Opinion regarding the CTF are equally applicable to the DP-3T protocol.

Observations about contact tracing apps that use the CTF

This part of the Opinion offers observations about key issues raised by third-party development of tracing apps using CTF as the API foundation. These observations are not exhaustive and, as noted elsewhere, the Commissioner will consider the facts of each case in assessing compliance.

Roles of the app developer and the body controlling the contact tracing scheme, as controllers

The CTF as a technical matter enables development of apps that process more information than may be necessary for contact tracing purposes. The CTF documentation says that while the 'standard' means of operation does not use location data, it may be possible for app developers to do so, but that 'any use of location data is completely optional to the schema'.

The Commissioner acknowledges that the processing of additional data by apps that use the CTF may be legitimate and permissible. This may be needed to support the public health utility of a tracing app, and would need to be assessed on a case-by-case basis. For example, it may be necessary to process data to restrict the uploading of diagnosis keys by users, to ensure the system is not flooded with false positives. A more expansive example of where additional functionality beyond contact tracing could be sought would be to assess compliance with isolation. Where additional data processing takes place, a separate assessment of data protection considerations will need to be made by the controller, which may involve a separate data protection impact assessment if the threshold criteria are met.

Privacy information, lawful basis and consent management

While the existence of multiple different actors within the mobile app ecosystem likely means that data protection obligations rest upon multiple parties, the primary responsibility for providing privacy information rests with app developers (who create apps; this may include organisations, who outsource the actual app design to a third party) and app stores (who make apps available to users), particularly where app

developers are also controllers. This is however no different to normal apps.

While Google and Apple's app stores mandate specific requirements for the privacy information that apps must provide, it is at present not clear whether this would mean contact tracing apps utilising the CTF must include information relating to the CTF.

As stated above, the Commissioner understands that most current proposals for contact tracing apps would rely on consent as the lawful basis for processing any personal data, and that installation of the apps is also voluntary. However, the Commissioner also notes that at the present time some matters remain unclear and must be addressed before being rolled out.

First, it is not yet clear how the CTF will facilitate the collection of consent for the upload of stored tokens to the app host, although we are advised that the CTF will require the specific consent of the user at this point. Second, it is not clear how an app utilising the CTF will manage this consent signal and how the CTF and an app may between them provide control to users. Last, it is unclear what impact consent withdrawal may have both on the effectiveness of contact tracing solutions and any notifications provided to other app users once an individual is diagnosed. Each of these matters will have to be addressed moving forward.

User awareness and perception

It is possible that many users of a contact tracing app will have neither the time nor the expertise to determine that the CTF is facilitating the collection of some data from their devices, or that any app using it was designed by another party.

There is a risk that individuals believe that the data protection by design and by default principles incorporated by the CTF extend to all aspects of a contact tracing app that uses the CTF. If the app processes data outside the scope of what the CTF intends to cover, then the controller should ensure it has also assessed the data protection implications of this processing (along with the processing it undertakes using the CTF), ensuring that the processing is fair, lawful and transparent.

However, the responsibility cannot solely be placed on the user. While the Commissioner welcomes the transparency already shown by Google and Apple in this proposal, use of the CTF by apps must be documented and auditable, and any controller processing personal data has to comply with data protection law.

The Commissioner is a reasonable and pragmatic regulator, and does not operate in isolation from matters of serious public concern. Regarding compliance with data protection, the Commissioner will take into account the compelling public interest in the current health emergency. Controllers should refer to the ICO's guidance on COVID-19 that reflects this position.

Considerations outside of the scope of this Opinion

The scope of this Opinion is limited to consideration of the design of the CTF. A range of other concerns and considerations may arise pertaining to the broader area of COVID-19 contact tracing. For example, there may be more components of a contact tracing scheme that could give rise to other concerns for controllers, such as the association of other data generated by an app with centralised data held by the PHA or others, or measures taken by the PHA or Government to encourage or mandate use of the app. These will need consideration on a case by case basis as they arise.

Conclusions

The CTF is aligned with the principles of data protection by design and by default

The Commissioner has considered the concerns and considerations regarding the CTF, and believes the CTF is aligned with the principles of data protection by design and by default, including design principles around data minimisation and security.

Contact tracing apps that use the CTF should align with the principles of data protection by design and by default whenever personal data is processed

At present, the CTF is limited to the development of APIs and technical specifications for Apple and Google's mobile operating systems to facilitate the development of contact tracing apps on both platforms. Such apps may process other sets of personal data to support additional functionality. Each controller designing an app is responsible for ensuring the app is compliant with law and regulation.

Clarification is needed for app users around who is responsible for data processing

Many users of a contact tracing app will have neither the time nor the expertise to understand that the CTF is facilitating the collection of some data from the device, but that the app itself was designed by another party.

There is a risk that individuals believe that the data protection by design and by default principles being utilised by the CTF extend to all aspects of a contact tracing app utilising the CTF. If the app processes data outside the CTF's intended scope, however, the controller responsible must ensure it has also assessed the data protection implications of this processing (along with any it undertakes using the CTF), and ensure that it is compliant. It is equally important that this controller be transparent with potential and actual app users, noting the data protection principles of transparency and accountability.

Further questions are likely to arise over time

The COVID-19 pandemic continues to pose unique and urgent challenges to all aspects of society. This is a fast moving and complex situation, and it is likely that additional questions regarding the use of technology and data for contact tracing will arise over time.

This much is clear given the acknowledgement by Apple and Google that the CTF is will likely evolve over time. There are indications, for example, of a Phase 2 of the work that would see additional functionality. Moreover, other contact tracing proposals exist, such as the proposed DP-3T system. As noted above, third parties are likely to develop contact tracing apps that use the CTF and may also separately process personal data. Development of these apps may give rise to broader questions, such as around additional functionality within the app itself or the use of other personal data sets to promote or mandate usage of a particular contact tracing app. Existing ICO guidance will be sufficient to address many questions that developers and controllers may have, but the Commissioner will continue to identify ways to support controllers with questions about the processing of personal data during the COVID-19 pandemic.

Next steps

As suggested earlier, the Commissioner will carefully consider developments in this area, and may choose to issue further Opinions or other statements to address aspects of personal data processing during the COVID-19 pandemic.

Further reading

ICO guidance on COVID-19

https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/

Google and Apple announcements regarding the CTF (including links to technical documents)

https://www.apple.com/uk/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology

Other useful reading:

Further background on COVID-19:

https://www.gov.uk/coronavirus

Explanation of contact tracing:

https://publichealthmatters.blog.gov.uk/2020/02/13/expert-interview-what-is-contact-tracing/

Proposed DP-3T system:

https://dp-3t.github.io