s22 - irrelevant

Our Commissioner has suggested that two recently published pieces of work from the UK Information Commissioner's Office (ICO) are essential reading when considering the operation of contact tracing apps.

The first is the ICO's just-published Opinion which sets out Commissioner Denham's current thinking regarding the joint initiative by Apple and Google to enable the use of Bluetooth technology to help governments and public health authorities reduce the spread of the virus. https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf.

Explanation of model choice

Globally, there have been a number of models adopted for contact tracing COVID-19. One model is that which facilitates notification of a positive diagnosis between installers of the app who have been sufficiently proximate, without the intervention of a state authority or the collection of personal information into a centralised data store. While such a model may not be preferable in the Australian context, it would appear to offer stronger privacy protections than the model that which has been adopted in this case. We suggest that acknowledging this alternative model and explaining the reasons for the adoption of the proposed model may alleviate potential concerns or criticism of this choice.

s22 - irrelevant [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

s22 - irrelevant

Consideration of alternatives to the COVIDSafe app and the National COVIDSafe Data Store

- We note the discussion in Section D of the draft PIA which indicates that the Department of Health and the DTA have been actively considering whether new and alternative technologies can/should be adopted in Australia to enhance privacy whilst facilitating COVID-19 contact tracing. This ongoing consideration aligns with Recommendation 14 of the original PIA for COVIDSafe; that the Department of Health consider whether Bluetooth technology is the most appropriate available technology to use for the COVIDSafe app.

- **OAIC Recommendation 6:** We recommend that the draft PIA consider the Minister for Health's report on the operation and effectiveness of the COVIDSafe app and the National COVIDSafe Data Store, as described in section 94ZA of the Privacy Act 1988 (Cth). We consider that this report will provide important information which is relevant to the justification of the ongoing collection of personal information through the COVIDSafe app, and that relevant information obtained from the Minister's report should be added to section D of the draft PIA report.

s22 - irrelevant

- [redacted]

- [redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

Australian Government
Office of the Australian Information Commissioner

Memorandum

Responsible Executive Member:	Melanie Drayton
Prepared by:	Andre Castaldi
Through:	Kellie Fonseca
To:	Angelene Falk
File ref:	D2020/007356
Date:	18 April 2020
Subject:	**Summary of ICO opinion re the collaboration by Apple and Google on contact tracing technology**

Purpose and timing

This memo provides a summary of the ICO opinion regarding the collaboration by Apple and Google on contact tracing technology.

This brief also presents a plain language summary of how the Apple Google Contact Tracing Framework (CFT) is intended to operate as it has been described in the Opinion and in Apple Google's overview of the CTF.

Executive Summary

- The Opinion provides that
  - 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.
  - Clarification is needed for app users around who is responsible for data processing (for example where a contact tracing app is using CTF (which facilitates the collection of data from the user's device) however the data protection by design and by default principles may not extend to all aspects of the app.
  - This an evolving, complex and fast moving situation and is likely that additional questions regarding the use of technology and data for contact tracing will arise:
    - Apple and Google have earmarked phase 2 (operating system and device level functionality)

    - other contact tracing proposals exist such as the proposed DP-3T system, and
    - third parties are likely to develop apps using CTF.
  - Other questions may arise such as further functionality within apps or the use of other personal data to promote or mandate use of a particular contact tracing app

Summary

Plain language summary of how the CFT is intended to operate

- The CTF is intended to include application programming interfaces (APIs)[1] and operating system level technology to assist contact tracing.
- Apple and Google have announced that '*in May, both companies will release APIs that enable interoperability between Android and iOS devices using apps from public health authorities (PHAs). These official apps will be available for users to download via their respective app stores*'.[2]
- The CTF is not a contact tracing app. Apple and Google's aim is to enable third parties such as PHAs to develop contact tracing apps that exchange information via Bluetooth Low Energy between devices.[3]
- Apple and Google have released a simple explanation of how a contact tracing app is envisaged to work using the CTF.[4] In summary
  - Phones generate and exchange anonymous identifier beacons (keys)
    - When two individuals meet with each other (for a specified time, for example 10 minutes, and proximity, for example 2 metres) their phones exchange the keys. These keys change frequently (for example every hour)
  - If one individual is diagnosed with COVID-19, they enter the test result in an app developed by a PHA and with consent the phone uploads the last 14 days of keys to a cloud based temporary store.
  - Phones periodically download the keys of all individuals that have tested positive for COVID-19 and a match is created where an individual's phone has exchanged keys with an individual who has tested positive. A notification can be sent from the app host to the individual's phone regarding what to do next.

Summary of Contact tracing

Contact tracing:

- aims to identify if an individual has been in contact with an infected individual when that individual is possibly infectious
- is used to support swift communication with individuals to
  - alert them of the risk

[1] An application programming interface (API) is a computing interface to a software component or a system, that defines how other components or systems can use it (Wikipedia), 'In basic terms, APIs just allow applications to communicate with one another' (Medium, What exactly IS an API?)

[2] 10 April, see for example Apple announcement.

[3] Bluetooth Low Energy can be used to discover devices, query for services and transmit information, (Android developer).

[4] https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf

  - provide them with information
  - ensure they take appropriate steps to protect themselves and others, and
  - receive support,
- may be used in conjunction with other measures and policies to manage social distancing and professional gatekeeping, potentially enabling measures to support the easing of lockdowns and other restrictions - for example immunity verification or immunity passport proposals, and
- may be undertaken manually and there is heightened interest in proposals to support contact tracing using automated tools.
- the Commissioner recommends transparency around initiatives linked to tracing apps and that any solution is privacy preserving in nature

Summary of the Opinion

- The Opinion sets out the Commissioner's current thinking regarding the CTF, joint initiative by Apple and Google.[5]
- The analysis is limited to information provided to date.
- The Opinion has been prepared for:
  - organisations involved in CTF development
  - organisations developing apps that may use the CTF
  - stakeholders wishing to understand the Commissioner's position on the initiative.
- The proposals for the CTF appear aligned to privacy by design and by default.

Data minimisation

- The CTF appears to comply with the data minimisation principle:
  - the exchange of information between devices does not include personal data
  - processing that match keys to identify contacts with infected individuals takes place on the phone (and not by the 'app host' or a third party)
  - location data does not form part of the CTF, either the exchange between phones, upload to the app host or notifications to users from the app host.
- The CTF may permit app developers to process more information that may be necessary for contact tracing purposes (considered further later)

User controls

- User controls include
  - For apps using CTF and proposals to date, app installation is voluntary and post-diagnosis upload of keys to the app developer requires user consent.
  - Apps will be provided by mobile operating system (OS) app stores and subject to the same requirements as other apps.
  - Users can remove or disable the app.

[5] The opinion is issued under Section 115(3)(b) of the Data Protection Act 2018 (DPA 2018).

  - Phase 2 involves CTF at the device operating system which and to prevent the CTF API from operating users would have to refuse or remove OS updates.
  - A user could disable Bluetooth to prevent tracking.
  - The Commissioner notes:
    - it should not be up to the individual to take action to prevent tracking, and
    - more general considerations are necessary regarding implications for individuals rights and freedoms if a user decides to disable Bluetooth, uninstalls etc apps, especially in terms of future proposals for immunity testing / passports.

Security

- The exchange of information is subject to security measures including cryptographic functions including:
  - Tokens are generated on the device (not under control of the App developer) to ensure information broadcast to another device if not directly related to an identifiable individual.
- Exchange of tokens between devices does not indicate COVID-19 status (though if a person had a small number of contacts with other people they could perhaps discern COVID-19 status):
  - A diagnosed individual consents to uploading the keys on their device via an encrypted communication channel to app host (for example the PHA) and the app host notifies an individual may have been near a diagnosed individual without identifying that individual. A technically advanced attacker could look up the keys of infected individuals, however this risk appears low.
  - Transfer of data to the app (i.e. the downloading of keys of COVID-19 diagnoses) is likely to be undertaken via transport layer security (TLS).[6]
  - No persistent ID is broadcast, instead pseudo random tokens representing changing user IDs are broadcast so there is low risk of identifying an individual from interaction between two phones.

Purpose limitation

- CTF is very new and evolving initiative and this risks expanding the use of CTF-enabled apps beyond the stated purpose of contact tracing and the Commissioner will monitor this area closely for developments.

DP-3T protocol

- The joint Apple Google initiative is not associated with the DP-3T protocol however they share similar underlying principles, and this gives the Commissioner further comfort.[7]

[6] Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website (Cloudflare, What Is Transport Layer Security (TLS)?)

[7] Decentralized Privacy-Preserving Proximity Tracing system aims to minimise privacy and security risks for individuals and communities and guarantee the highest level of data protection (Github Decentralized Privacy-Preserving Proximity Tracing).

Summary of key issues raised by third-party development of tracing apps using CTF as the API foundation

The Opinion also considers issues in relation to tracing apps using CTF for example:

- CTF may enable the development of apps that process more information than may be necessary for contract tracing purposes and it is possible for app developers to use location data.
  - The Commissioner acknowledges that the processing of additional data by apps that use the CTF may be legitimate and permissible, for example processing data to restrict the uploading of false positives or to assess compliance with isolation, but in each case the controller would need to undertake a separate assessment of data protection considerations.
- Contact tracing apps using the CTF may need to provide privacy notices that include information relevant to CTF.
- It is not clear if the CTF will facilitate the collection of consent for the upload of keys to the app host.
- With an app using CTF it is not clear how the app using CTF will manage consent and how control will be provided to users.
- The effect of consent withdrawal on effectiveness of contact tracing solutions and any notifications is unclear.
- There is a risk for apps using the CTF that users may presume that data protection by design and default principles extend to all aspect of the app using CTF.
- Use of the CTF by apps must be documented and auditable, and any controller processing personal data must comply with data protection law.

Considerations outside of the scope of this Opinion

- 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.

Australian Government
Office of the Australian Information Commissioner

Overview of Apple/Google contact tracing technology

Purpose and timing

Prepared by Andre Castaldi, Assistant Director, OAIC for the National COVID-19 Privacy Team Meeting on 30 April 2020. The following memo sets out taking points and background research in relation to the Apple and Google contact tracing solution.

Talking points

We thought that it would be helpful to share an overview of the Apple/Google collaboration in relation to contact tracing technology.

The collaboration has two phases:

1. **Phase 1**, May, Apple and Google will release application programming interfaces (APIs) to enable interoperability between Android and iOS devices, so that apps from public health authorities can use the contact tracing technology
2. **Phase 2**, Apple and Google will enable a broader Bluetooth-based contact tracing platform by building this functionality directly into iOS and Android software (including hardware).

So how does this work?

- This is not a contact tracing app.
- Designed to enable public health authorities to develop apps that exchange information via Bluetooth Low Energy between devices.
- An app using this functionality is envisaged by Apple and Google to work as follows:
  - An individual installs an app (running the Apple Google API) and their phone generates and exchanges anonymous identifiers which change frequently (keys).
  - when two individuals, who both have the app installed meet with each other (for a specified time, for example 10 minutes, and proximity, for example 2 metres) their phones exchange the keys.
  - If an individual is diagnosed with COVID-19, they enter the test result in an app and with consent the phone uploads the last 14 days of keys to a cloud based temporary store operated by a public health authority.
  - Apps installed on phones periodically download the keys of all individuals that have tested positive for COVID-19 and a match is created (on the phone) where an individual's phone has exchanged keys with an individual who has tested positive.
  - A notification can be sent from the app host to the individual's phone regarding what to do next.

- This is a decentralises system that keeps data on users' devices.

COVIDSafe App Australia

- At a press conference on 27 April 2020[1]
  - Health spokesperson Daniel Keys indicated that The COVIDSafe app was developed on the basis that it needed to be 'moved forward to provide a capability that can support the Government's agenda' and build on 'the Apple and Google functionality when it comes in'.
  - The Government has also indicated that they are seeking to cater for the widest possible userbase and note that the Apple and Google functionality will require an operating system update, which may mean some older phones may not be able to take up the technology.

ICO Opinion

- On 17 April 2020 the ICO released an opinion which notes:
  - that the scheme broadly appears to comply with the data minimization principle, including that no location data is collected
  - user control include that
    - installation is voluntary
    - users can remove or the app

    once functionality is at the operating system level it will make it more difficult for users to opt-out and it should not be up to the individual to prevent tracking
  - security measures include that the information is subject to strict security measures including cryptographic functions and the exchange of keys / tokens between devices does not indicate COVID-19 status
  - In relation to purpose limitation, it was noted that this is an evolving area where there is a risk of expansion of the use of apps and data

International approaches

- There have been varying responses to this initiative:
  - with the United Kingdom, France and Norway moving forward with a centralised approach and
  - Czech Republic, Iceland, Indonesia, Israel and North Macedonia, Philippines, Switzerland, Austria and Germany seem to be largely aligned with the Apple Google contact tracing approach.

Most recent developments

- 29 April 2020 as part of the first phase: Apple and Google released the first versions of their Covid-19 contact-tracing tools to public health organizations so the agencies can start building applications ahead of the system's launch in mid-May.
- The tools include software updates for iOS and Android, and software development kits (SDKs) to help developers build and test their apps. Yahoo Finance

[1] Chief Medical Officer's press conference about COVIDSafe and COVID-19 on 27 April 2020

- Apple and Google typically release versions of for testing prior to wider release. It has been reported that more details will be released on Friday including the sample code. msn
- 6 May 2020, Apple and Google announce that their contract tracing technology will ban location tracking (MIT Technology Review)

Overview

- The collaboration has two phases.
  - In May, Apple and Google will release application programming interfaces (APIs) to enable interoperability between Android and iOS devices so that apps from public health authorities can use the contact tracing technology
  - In the following months, Apple and Google will enable a broader Bluetooth-based contact tracing platform by building this functionality directly into iOS and Android software (including hardware).
- So how does this work?
  - This is not a contact tracing app. Apple and Google's aim is to enable third parties such as public health authorities to develop contact tracing apps that exchange information via Bluetooth Low Energy between devices.
  - Apple and Google have released a simple explanation of how a contact tracing app is envisaged to work:
    - Once an individual installs an app (running the Apple Google API) then their phone generates and exchange anonymous identifiers which change frequently (keys)
    - When two individuals meet with each other (for a specified time, for example 10 minutes, and proximity, for example 2 metres) their phones exchange the keys.
    - If one individual is diagnosed with COVID-19, they enter the test result in an app developed by a public health authority and with consent the phone uploads the last 14 days of keys to a cloud based temporary store.
    - Phones periodically download the keys of all individuals that have tested positive for COVID-19 and a match is created where an individual's phone has exchanged keys with an individual who has tested positive.
    - A notification can be sent from the app host to the individual's phone regarding what to do next.

Comments from Daniel Keys (Department of Health) 27 April 2020[2]

Why didn't Australia release its own app before waiting for Apple's version?

"They are working to introduce a native function to perform contact tracing. ***That is some way away****. It is rumoured to be late May but there is no definitive date for release. We moved forward to provide a capability that can support the Government's agenda to allow us to then introduce a capability that we can build on when the Apple and Google functionality comes in. I'd also like to add that that capability that's being built into their operating systems will only be available to those people who upgrade. Now, for some people the phones will not handle an upgrade, so we need to cater for a diverse range of users out there and provide solutions for as many people as possible."*

From a technical point of view would that mean that iPhone users wouldn't need to have the app open in the background?

"It's unclear at this stage, so we are working with Apple and Google on their functionality to ensure that it can be consumed by the app to improve the app 's performance."

[2] Chief Medical Officer's press conference about COVIDSafe and COVID-19 on 27 April 2020

ICO opinion

- ICO has released an Opinion on the Apple Google collaboration[3] and notes that
  - CTF appears to comply with the data minimisation principle
    - the exchange of information between devices does not include personal data,
    - all processing (i.e. matching of keys to identify infected individuals) takes place on the phone
    - location data does not form part of the system
  - User controls include
    - Installation is voluntary and providing data post diagnosis requires user consent
    - Users can remove or disable the app
    - The ICO notes that phase two will move the functionality to the operating system level of the device which will make it more difficult for user to opt-out of using the system (effectively requiring them to remove OS updates. The Commissioner notes that it should not be up to the individual to take action to prevent tracking.
  - Security includes
    - The exchange of information is subject to security measures including cryptographic functions and the exchange of tokens between devices does not indicate COVID-19 status
    - No persistent ID is broadcast
  - Purpose limitation
    - This is an evolving area and there is a risk of expansion of the use of apps
  - The joint Apple Google initiative is not associated with the DP-3T protocol however

OECD GPA workshop

- Apple and Google attended the OECD GPA Online Workshop on Addressing the Data Governance and Privacy Challenges in the Fight against COVID-19 last Wednesday and gave a brief overview.

- William Malcolm, Director, Privacy, Google, with Gary Davis, Global Director of Privacy & Law Enforcement Requests, Apple.

- They described that the challenge to solve is around fragmentation across apps and Bluetooth interoperability for example between Apple and Android devices so that Bluetooth signals are operable, and this is done protectively and on device with transparency.

- It has been reported that the French government 'urged for more invasive measures in an effort to combat COVID-19, urging Apple and Google to ease privacy rules on contact tracing'. See The Guardian.

France Says Apple Bluetooth Policy Is Blocking Virus Tracker

- A privacy measure in Apple's operating system prevents contact tracing apps from running Bluetooth constantly in the background if data is going to be moved off the

[3] https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf

device. (The Google-Apple system, available May, keeps data on user devices i.e. decentralised system.)

- However, France (and EU) want to feed data to a central server (managed by state health services) to alert at risk individuals (i.e. centralised system). The Author argues centralised system is inherently less secure, and vulnerable to 'mission creep' (i.e. surveillance through large scale data collection) which undermines community trust and acceptance of the app.
- France to launch its own national contact-tracing app on May 11 and has requested Apple remove this technical obstacle. Implementation will be voluntary.
  - France to discuss app in Parliament on April 28. MPs will not have say over implementation of app.
  - France's privacy watchdog to review plan this week.

iOS a 'major hurdle' to contact tracing app

- Apple's technical obstacle (see above) will also affect Australian's gov contact-tracing app - similar to France's proposed app, and Singapore's TraceTogether app (which Aus app is largely based).
- Singapore app is also a centralised system – following diagnosis, data of close contacts sent to gov health authorities who then alert at risk individuals. As such, app runs when open and phone is unlocked.
  - Technical obstacle is 'major hurdle' for widespread adoption – Singapore uses push notifications to remind users to keep app running.
- Aus plans on launch next month with hopes to lift social restrictions, but it faces the same challenges as Singapore – it would be difficult to hit target of 40% adoption.
- Singapore warns contact tracing app should supplement and not replace manual contact tracing by health authorities.

International Snapshot (as at 30 April 2020)

- 19 contact-tracing apps launched in 23 countries (NS Tech)
- 20 apps centralised, 8 decentralised, 15 unknown (Top10VPN)
- 25% of apps have no privacy policy
- 57% use GPS, 15% use Bluetooth & 26% use both GPS and Bluetooth

See COVID-19 Digital Rights Tracker on Google Sheets (Top10VPN)[4]

- **France:** **Rejected** Apple and Google's contact tracing solution and decided to move forward with its own centralized approach. In anticipation of its May 11 launch, France requested Apple remove its technical obstacle which prevents Bluetooth running in the background. (21 April 2020, Bloomberg)
  - France's privacy watchdog CNIL on Sunday gave a conditional green light to app. (26 April 2020, The Local).

[4] Note this may not be the most current information compared to news articles due to delay in reporting. Additionally, the table incorrectly labels Australia as 'decentralised' see, e.g. Bank Info Security article.

- **UK: Rejected** Apple and Google's contact tracing solution and decided to move forward with its own centralized approach. The app should launch in 3 weeks, approx. 20 May 2020 (27 April 2020, Forbes; 29 April 2020, The Guardian)
- **Norway: Rejected** Apple and Google's contact tracing solution and decided to move forward with its own centralized approach. The app also tracks geo-location. (17 April 2020, The Star; Privacy International)
- **Czech Republic, Iceland, Indonesia, Israel and North Macedonia, Philippines**: **Aligned** with Google and Apple's contact tracing approach (22 April 2020, NS Tech; Top10VPN)
- **Switzerland and Austria: Aligned** with Google and Apple's contact tracing approach, with Switzerland saying it would launch an app on May 11 (23 April 2020, itnews)
- **Germany:** Has flipped and **aligned** with Google and Apple's contact tracing approach (27 April 2020, Channel News Asia)
- **NZ:** System **unknown**. The Ministry of Health plans to make a voluntary app available in the next fortnight to track the movements of people with the virus. (27 April 2020, RNZ)
- **Ireland:** System **unknown**. The Irish Health Service plans to launch a "pilot" version of a contact tracing next month, however, privacy advocates have raised that the HSE has not provided enough information. (27 April 2020, The Irish Times)
- **US:** System **unknown**. There are a few developments, but it is unclear how they align with Apple Google approach. These apps track geolocation:
  - North Dakota's Care 19 (28 April 2020, ND Response)
  - Utah partnering with geolocation social app Twenty to create app (Fox 13)

Apple Google technology updates (as at 30 April 2020)

- Apple and Google have released the first version of their exposure notification API (which they previously called the contact tracing API). This is a developer-focused release, with the primary intent of collecting feedback from developers who will be using the API to create new contact tracing and notification apps on behalf of public health agencies. (30 April 2020, Tech Crunch)
  - Apple and Google say they will be providing this coming Friday [1 May 2020] additional details about the API and its release, including sample code to show how it operates in practice
- Apple and Google have tightened privacy measures in the contact-tracing scheme they are offering to health authorities and now intend to release a software building block to developers on Wednesday 29 April allowing them to build compatible apps. (24 April 2020, BBC News; 30 April 2020, Yahoo Finance) Changes include:
  - giving information about different devices' Bluetooth power levels, to help developers better estimate how far two handsets are from each other
  - letting developers decide for themselves how close together phones should be and for how long to trigger a handshake
  - preventing the phones from logging any meeting as having lasted longer than 30 minutes
  - encrypting data about the transmission power of the phones, to prevent anyone retrospectively using the logs to reveal what models had been involved
  - changing to a different encryption algorithm - AES - to reduce the toll on battery life

- Apple will require users to install a new version of iOS 13 to use the API. That means any handset older than the iPhone 6S - which was released in September 2015 - will be incompatible.
- Any Android device running version 6 of Google's operating system, which launched in October 2015, or higher will work without needing an update.
- Now it’s up to governments around the world to decide whether they’ll choose the Apple and Google approach, which has privacy and usability benefits, or whether they will create their own apps using their own technology to empower their public health departments with additional data. (29 April 2020, CNBC)
- 30 April 2020 Apple and Google have released the first version of their exposure notification API. (TechCrunch*)*

Australian Government
Office of the Australian Information Commissioner

Memorandum

To	Kellie Fonseca and Andre Castaldi
From	Lisa Liang
Copies	Sara Peel
File ref	D2020/006980
Date	14/04/2020
Subject	**Apple and Google - COVID-19 contact tracing technology**

Contact tracing

- Contact tracing is used by health professionals to trace the movements of the diagnosed person back to another confirmed case or high-risk activity from which they caught the virus. Then, those who may have been in contact with and infected by the diagnosed person are notified.
- Contact tracing will play a key role in managing COVID-19 post lockdown.
- Effective implementation of contact tracing technology involves high opt-in rates and community trust in the technological safeguards, and oversight by public health systems.
- Apple and Google operating systems power 99% of the world's smartphones. A collaboration between could accelerate the usage of apps to manage COVID-19 more quickly and reliably than existing systems.

Overview

Apple and Google will partner to launch an opt-in contact tracing technology to help governments and health agencies manage COVID-19, with user privacy and security central to its design.

- The contact tracing technology will be implemented in 2 stages:
  - In May, Apple and Google will release application programming interfaces (APIs) to enable interoperability between Android and iOS devices so that apps from public health authorities can use the contact tracing technology
  - In the following months, Apple and Google will enable a broader Bluetooth-based contact tracing platform by building this functionality directly into iOS and Android

software. This will allow more individuals to opt-in and enable interaction with a broader ecosystem of apps and government health authorities.

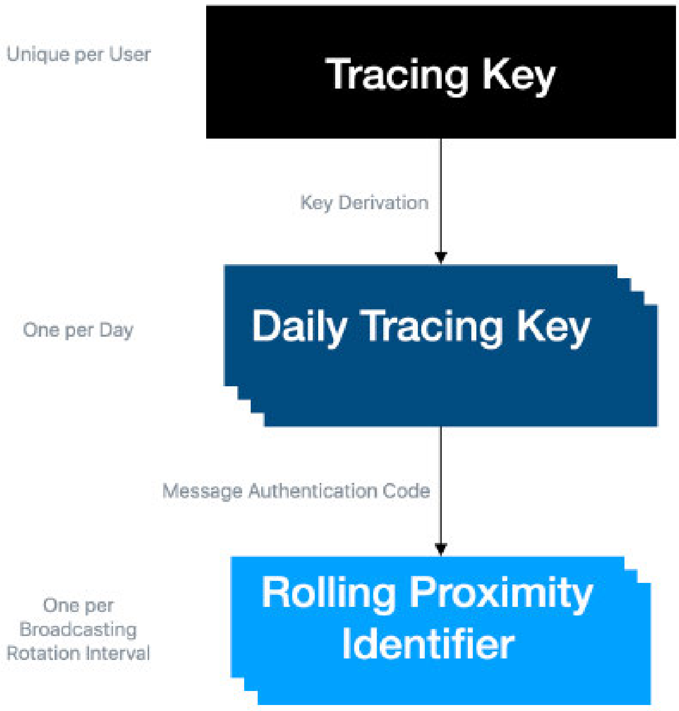
- Apple and Google will work in consultation with interested stakeholders and publish updates on this collaboration.
- For a summary of the ICO opinion regarding the collaboration by Apple and Google on contact tracing technology, see the memo at: D2020/007356.

How it works

- Users' phones with the contact tracing technology will emit unique Bluetooth signals. Each phone over time collects anonymous information/identifiers of all other phones within a six-foot (2-metre) vicinity.
- With public health authority sign off and the diagnosed individual's consent, the phone (using the contact tracing app) only publishes its own identifier, so all other phones can locally check that they have been in close contact with this device (using the local database of identifiers they saw recently).
- This will trigger alerts to potentially exposed users to seek more information.
- The logs will be scrambled to keep infected individuals' data anonymous to all parties.

Privacy issues

- Apple and Google's technical specification documents outline the following privacy features:


Unique per User
Tracing Key
Key Derivation
One per Day
Daily Tracing Key
Message Authentication Code
One per Broadcasting Rotation Interval
Rolling Proximity Identifier

The ***Tracing Key*** is generated when contact tracing is enabled on the device and is securely stored on the device.

A ***Daily Tracing Key*** is generated for every 24-hour window where the protocol is advertising.

Advertising refers to sending out Bluetooth information to nearby devices. **Scanning** refers to receiving and reading other devices' advertisements.

The ***Rolling Proximity Identifiers*** are privacy-preserving identifiers that are sent in Bluetooth Advertisements

Bluetooth Specification (p. 6)

- Location is not used for proximity detection, only Bluetooth beaconing is
- Users decide whether to contribute to contact tracing

  - If diagnosed, users consent to sharing information with the server
  - A user's Rolling Proximity Identifiers changes approx. every 15min and needs the Daily Tracing Key to be correlated to the user
  - Proximity identifiers obtained from other devices are processed exclusively on device
- Cryptography Specification (p. 6)
  - Key schedule is fixed and defined by operating system components, preventing applications from including information that could be used for tracking
  - A server operator implementing this protocol does not learn who users have been in proximity with or users' location (unless it also has the unlikely capability to scan advertisements from users who recently reported Diagnosis Keys)
  - When reporting Diagnosis Keys, the correlation of Rolling Proximity Identifiers by others is limited to 24h periods due to the use of Daily Tracing Keys.
  - The server must not retain metadata from clients uploading Diagnosis Keys after including them into the aggregated list of Diagnosis Keys per day
- The American Civil Liberties Union's report warns that contact tracing apps could lead to increased government surveillance, particularly if data isn't properly protected, noting that:
  - "Any uses of such data should be temporary, restricted to public health agencies and purposes, and should make the greatest possible use of available techniques that allow for privacy and anonymity to be protected, even as the data is used." (p. 1)
  - The report also notes the limitations of Bluetooth location data, being not "accurate enough to identify close contact with sufficient reliability" (p. 4).
- Jennifer Granick, ACLU surveillance and cybersecurity counsel, says that:
  - Apple and Google appear to "mitigate the worst privacy and centralisation risks"
  - An effective system must be:
    - voluntary
    - decentralised (i.e. store data on an individual's device, not a centralised repository)
    - used only for public health purposes
    - used only for the duration of this pandemic
- Dutch Academic Jaap-Henk Hoepman notes that:
  - The incorporation of Bluetooth-based contact tracing into the operating system of Apple and Google devices means the use of data is no longer limited in time or for the purpose of COVID-19.
  - The remaining privacy safeguard is a decentralised system. However, any decentralised system can be turned into a centralised system. This is because while the platform itself may be decentralised; the app developed on top can enable centralised collection regardless.
    - Governments or companies create an app that forces the phone to report close contact(s) with an infected person (and users cannot prevent this).
    - When an individual opts to report as infected, all other phones in recent close contact will reveal themselves to the central server.
- The ICO UK has released an Opinion on the Apple Google collaboration, we have prepared a memo summarising this: D2020/007356

Australian Government
Office of the Australian Information Commissioner

Memorandum

To	Andre Castaldi
From	Andre Castaldi
Copies	Kellie Fonseca
File ref	D2020/008080
Date	30 April 2020
Subject	**Overview of Apple/Google contact tracing technology – speaking notes**

Purpose and timing

The following memo sets out taking points and background research in relation to the Apple and Google contact tracing solution for the purposes of the National

Talking points

We thought that it would be helpful to share an overview of the Apple/Google collaboration in relation to contact tracing technology.

The collaboration has two phases:

1. **Phase 1**, May, Apple and Google will release application programming interfaces (APIs) to enable interoperability between Android and iOS devices, so that apps from public health authorities can use the contact tracing technology
2. **Phase 2**, Apple and Google will enable a broader Bluetooth-based contact tracing platform by building this functionality directly into iOS and Android software (including hardware).

So how does this work?

- This is not a contact tracing app
- Designed to enable public health authorities to develop apps that exchange information via Bluetooth Low Energy between devices.
- An app using this functionality is envisaged by Apple and Google to work as follows:
  - An individual installs an app (running the Apple Google API) and their phone generates and exchanges anonymous identifiers which change frequently (keys)

  - when two individuals, who both have the app installed meet with each other (for a specified time, for example 10 minutes, and proximity, for example 2 metres) their phones exchange the keys.
  - If an individual is diagnosed with COVID-19, they enter the test result in an app and with consent the phone uploads the last 14 days of keys to a cloud based temporary store operated by a public health authority.
  - Apps installed on phones periodically download the keys of all individuals that have tested positive for COVID-19 and a match is created (on the phone) where an individual's phone has exchanged keys with an individual who has tested positive.
  - A notification can be sent from the app host to the individual's phone regarding what to do next.
- This is a decentralises system that keeps data on users' devices. (**Google-Apple memo**: D2020/006980)

COVIDSafe App Australia

- At a press conference on 27 April 2020
  - Health spokesperson Daniel Keys indicated that The COVIDSafe app was developed on the basis that it needed to be 'moved forward to provide a capability that can support the Government's agenda' and 'the Apple and Google functionality may be built on when it comes in'.
  - The Government has also indicated that they are seeking to cater for the widest possible userbase and note that the Apple and Google functionality will require an operating system update, which may mean some older phones may not be able to take up the technology.

ICO Opinion

- On 17 April 2020 the ICO released an opinion which notes
  - that the scheme broadly appears to comply with the data minimization principle, including that no location data is collected
  - user control include that
    - installation is voluntary
    - users can remove or the app

    once functionality is at the operating system level it will make it more difficult for users to opt-out and it should not be up to the individual to prevent tracking
  - security measures include that the information is subject to struct secirity measures including cryptographic functions and the exchange of keys / tokens between devices does not indicate COVID-19 status
  - In relation to purpose limitation, it was noted that this is an evolving area where there is a risk of expansion of the use of apps and data

International approaches

- There have been varying responses to this initiative:
  - with the United Kingdom, France and Norway moving forward with a centralised approach and

  - Czech Republic, Iceland, Indonesia, Israel and North Macedonia, Philippines, Switzerland, Austria and Germany seem to be largely aligned with the Apple Google contact tracing approach.

Most recent developments

- 29 April 2020 as part of the first phase: Apple and Google released the first versions of their Covid-19 contact-tracing tools to public health organizations so the agencies can start building applications ahead of the system's launch in mid-May.
- The tools include software updates for iOS and Android, and software development kits (SDKs) to help developers build and test their apps. Yahoo Finance
- Apple and Google typically release versions of for testing prior to wider release. It has been reported that more details will be released on Friday including the sample code. msn

Overview

- The collaboration has two phases.
  - In May, Apple and Google will release application programming interfaces (APIs) to enable interoperability between Android and iOS devices so that apps from public health authorities can use the contact tracing technology
  - In the following months, Apple and Google will enable a broader Bluetooth-based contact tracing platform by building this functionality directly into iOS and Android software (including hardware).
- So how does this work?
  - This is not a contact tracing app. Apple and Google's aim is to enable third parties such as public health authorities to develop contact tracing apps that exchange information via Bluetooth Low Energy between devices.
  - Apple and Google have released a simple explanation of how a contact tracing app is envisaged to work:
    - Once an individual installs an app (running the Apple Google API) then their phone generates and exchange anonymous identifiers which change frequently (keys)
    - When two individuals meet with each other (for a specified time, for example 10 minutes, and proximity, for example 2 metres) their phones exchange the keys.
    - If one individual is diagnosed with COVID-19, they enter the test result in an app developed by a public health authority and with consent the phone uploads the last 14 days of keys to a cloud based temporary store.
    - Phones periodically download the keys of all individuals that have tested positive for COVID-19 and a match is created where an individual's phone has exchanged keys with an individual who has tested positive.
    - A notification can be sent from the app host to the individual's phone regarding what to do next.

Comments from Daniel Keys (Department of Health) 27 April 2020

Why didn't Australia release its own app before waiting for Apple's version?

"They are working to introduce a native function to perform contact tracing. ***That is some way away****. It is rumoured to be late May but there is no definitive date for release. We moved forward to provide a capability that can support the Government's agenda to allow us to then introduce a capability that we can build on when the Apple and Google functionality comes in. I'd also like to add that that capability that's being built into their operating systems will only be available to those people who upgrade. Now, for some people the phones will not handle an upgrade, so we need to cater for a diverse range of users out there and provide solutions for as many people as possible."*

From a technical point of view would that mean that iPhone users wouldn't need to have the app open in the background?

"It's unclear at this stage, so we are working with Apple and Google on their functionality to ensure that it can be consumed by the app to improve the app 's performance."

ICO opinion

- ICO has released an Opinion on the Apple Google collaboration[1] and notes that
  - CTF appears to comply with the data minimisation principle
    - the exchange of information between devices does not include personal data,
    - all processing (i.e. matching of keys to identify infected individuals) takes place on the phone
    - location data does not form part of the system
  - User controls include
    - Installation is voluntary and providing data post diagnosis requires user consent
    - Users can remove or disable the app
    - The ICO notes that phase two will move the functionality to the operating system level of the device which will make it more difficult for user to opt-out of using the system (effectively requiring them to remove OS updates. The Commissioner notes that it should not be up to the individual to take action to prevent tracking.
  - Security includes
    - The exchange of information is subject to security measures including cryptographic functions and the exchange of tokens between devices does not indicate COVID-19 status
    - No persistent ID is broadcast
  - Purpose limitation
    - This is an evolving area and there is a risk of expansion of the use of apps
  - The joint Apple Google initiative is not associated with the DP-3T protocol however

OECD GPA workshop

- Apple and Google attended the OECD GPA Online Workshop on Addressing the Data Governance and Privacy Challenges in the Fight against COVID-19 last Wednesday and gave a brief overview

- William Malcolm, Director, Privacy, Google, with Gary Davis, Global Director of Privacy & Law Enforcement Requests, Apple

- They described that the challenge to solve is around fragmentation across apps and Bluetooth interoperability for example between Apple and Android devices so that Bluetooth signals are operable, and this is done protectively and on device with transparency.

- It has been reported that the French government ‘urged for more invasive measures in an effort to combat COVID-19, urging Apple and Google to ease privacy rules on contact tracing’. See The Guardian.

France Says Apple Bluetooth Policy Is Blocking Virus Tracker

- A privacy measure in Apple’s operating system prevents contact tracing apps from running Bluetooth constantly in the background if data is going to be moved off the

[1] https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf

device. (The Google-Apple system, available May, keeps data on user devices i.e. decentralised system.) (**Google-Apple memo**: D2020/006980)

- However, France (and EU) want to feed data to a central server (managed by state health services) to alert at risk individuals (i.e. centralised system). The Author argues centralised system is inherently less secure, and vulnerable to 'mission creep' (i.e. surveillance through large scale data collection) which undermines community trust and acceptance of the app.
- France to launch its own national contact-tracing app on May 11 and has requested Apple remove this technical obstacle. Implementation will be voluntary. (**EU standards memo**: D2020/007355 – voluntary, approved by national health authorities, preserve user privacy, dismantled once no longer needed.)
  - France to discuss app in Parliament on April 28. MPs will not have say over implementation of app.
  - France's privacy watchdog to review plan this week.

iOS a 'major hurdle' to contact tracing app

- Apple's technical obstacle (see above) will also affect Australian's gov contact-tracing app - similar to France's proposed app, and Singapore's TraceTogether app (which Aus app is largely based).
- Singapore app is also a centralised system – following diagnosis, data of close contacts sent to gov health authorities who then alert at risk individuals. As such, app runs when open and phone is unlocked.
  - Technical obstacle is 'major hurdle' for widespread adoption – Singapore uses push notifications to remind users to keep app running
- Aus plans on launch next month with hopes to lift social restrictions, but it faces the same challenges as Singapore – it would be difficult to hit target of 40% adoption.
- Singapore warns contact tracing app should supplement and not replace manual contact tracing by health authorities.

International Snapshot

- 19 contact-tracing apps launched in 23 countries (NS Tech)
- 20 apps centralised, 8 decentralised, 15 unknown (Top10VPN)
- 25% of apps have no privacy policy
- 57% use GPS, 15% use Bluetooth & 26% use both GPS and Bluetooth

See COVID-19 Digital Rights Tracker on Google Sheets (Top10VPN)[2]

- **France: Rejected** Apple and Google's contact tracing solution and decided to move forward with its own centralized approach. In anticipation of its May 11 launch, France requested Apple remove its technical obstacle which prevents Bluetooth running in the background. (21 April 2020, Bloomberg)

[2] Note this may not be the most current information compared to news articles due to delay in reporting. Additionally, the table incorrectly labels Australia as 'decentralised' see, e.g. Bank Info Security article.

  - France's privacy watchdog CNIL on Sunday gave a conditional green light to app. (26 April 2020, The Local).

- **UK: Rejected** Apple and Google's contact tracing solution and decided to move forward with its own centralized approach. The app should launch in 3 weeks, approx. 20 May 2020 (27 April 2020, Forbes; 29 April 2020, The Guardian)
- **Norway: Rejected** Apple and Google's contact tracing solution and decided to move forward with its own centralized approach. The app also tracks geo-location. (17 April 2020, The Star; Privacy International)
- **Czech Republic, Iceland, Indonesia, Israel and North Macedonia, Philippines**: **Aligned** with Google and Apple's contact tracing approach (22 April 2020, NS Tech; Top10VPN)
- **Switzerland and Austria: Aligned** with Google and Apple's contact tracing approach, with Switzerland saying it would launch an app on May 11 (23 April 2020, itnews)
- **Germany:** Has flipped and **aligned** with Google and Apple's contact tracing approach (27 April 2020, Channel News Asia)
- **NZ:** System **unknown**. The Ministry of Health plans to make a voluntary app available in the next fortnight to track the movements of people with the virus. (27 April 2020, RNZ)
- **Ireland:** System **unknown**. The Irish Health Service plans to launch a "pilot" version of a contact tracing next month, however, privacy advocates have raised that the HSE has not provided enough information. (27 April 2020, The Irish Times)
- **US:** System **unknown**. There are a few developments, but it is unclear how they align with Apple Google approach. These apps track geolocation:
  - North Dakota's Care 19 (28 April 2020, ND Response)
  - Utah partnering with geolocation social app Twenty to create app (Fox 13)

Apple Google technology updates

- Apple and Google have released the first version of their exposure notification API (which they previously called the contact tracing API). This is a developer-focused release, with the primary intent of collecting feedback from developers who will be using the API to create new contact tracing and notification apps on behalf of public health agencies. (30 April 2020, Tech Crunch)
  - Apple and Google say they will be providing this coming Friday [1 May 2020] additional details about the API and its release, including sample code to show how it operates in practice
- Apple and Google have tightened privacy measures in the contact-tracing scheme they are offering to health authorities and now intend to release a software building block to developers on Wednesday 29 April allowing them to build compatible apps. (24 April 2020, BBC News; 30 April 2020, Yahoo Finance) Changes include:
  - giving information about different devices' Bluetooth power levels, to help developers better estimate how far two handsets are from each other
  - letting developers decide for themselves how close together phones should be and for how long to trigger a handshake
  - preventing the phones from logging any meeting as having lasted longer than 30 minutes

  - encrypting data about the transmission power of the phones, to prevent anyone retrospectively using the logs to reveal what models had been involved
  - changing to a different encryption algorithm - AES - to reduce the toll on battery life

- Apple will require users to install a new version of iOS 13 to use the API. That means any handset older than the iPhone 6S - which was released in September 2015 - will be incompatible.
- Any Android device running version 6 of Google's operating system, which launched in October 2015, or higher will work without needing an update.
- Now it’s up to governments around the world to decide whether they’ll choose the Apple and Google approach, which has privacy and usability benefits, or whether they will create their own apps using their own technology to empower their public health departments with additional data. (29 April 2020, CNBC)
- 30 April 2020 Apple and Google have released the first version of their exposure notification API. (TechCrunch*)*