**Written Evidence Submitted by Apple**
**(C190017)**

1. Apple thanks the Committee for its questions and is happy to help. We have laid out some answers in response to each question below. It might be helpful to the Committee for us in addition to outline our understanding of how contact tracing apps on our platform will work.

2. Contact tracing is a technique used by public health authorities to measure and slow the spread of infectious diseases. It requires gathering information from infected individuals about the people they've previously been in contact with. These people can then be notified by public health authorities to take appropriate safety measures, such as undertaking self-quarantine and getting tested.

3. Governments, public health authorities, and NGOs around the world are starting to deploy contact tracing as a valuable tool for managing the COVID-19 pandemic.

4. Technology can play an important role in those efforts. Mobile devices can be used in an automated and scalable way to help determine who has been exposed to a person that later tests positive, and sending a notification with instructions on next steps. Health authorities can then use this information to help control the spread of COVID-19.

5. The system that Google and Apple announced on April 10, 2020 and elaborate upon on April 24, 2020 plays a complementary role in this process through exposure notification using mobile devices and Bluetooth technology to determine if an individual has come in contact with someone affected by COVID-19. In May, we will deliver this capability as an operating system update. Once this update is installed, a user can download an app developed or authorised by a public health authority, which will then access the system.

6. Users are fully in control, as these apps will prompt them for consent before enabling Bluetooth for exposure notification, and once again before reporting a positive diagnosis in the event they declare themselves COVID-19 positive with verification by their public health authority.

7. Once enabled, the app will regularly send out a beacon via bluetooth that includes a privacy-preserving identifier called a ‘key’—basically, a string of random numbers that aren’t tied to the user’s identity. Other phones will be listening for these privacy-preserving beacons and broadcasting theirs as well. When a user's phone receives another beacon, it will record and securely store the key associated with that beacon on their device.

8. The public health authority will define the way in which the app determines if someone has been exposed. To support this the system provides and the app can use both an estimate of time the user has been in contact with someone who has tested positive for COVID-19 and the approximate distance between the users. Public health authorities will set a minimum threshold for time spent together, such that a user needs to be within Bluetooth range for at least five minutes to register a match. If the contact is longer than five minutes, the system will report time in increments of five minutes up to a maximum of 30 minutes to ensure privacy.

9. To approximate distance, the system compares the Bluetooth signal strength between the two devices in contact. The closer the devices are, the higher the signal strength recorded. This signal strength can vary significantly based on factors like how the device is being held and as such this only provides an estimate of distance.

10. At least once per day the app from their public health authority will download a private and secure list of keys that have been verified as belonging to people confirmed as positive for COVID-19. A user's device will check the list of keys it has recorded against the list downloaded from the server. If there is a match between the keys stored on their device and the positive diagnosis list, the app will notify the user and advise them on steps to take next. The nature of the notification is fully determined by the public health authority app.

11. If at some point a user is positively diagnosed with COVID-19 they may report that within the app from their public health authority. Only with their explicit consent will the list of keys they have stored on their device be shared with the public health authority app. Once shared, the public health authority can then use the keys from their device so that others' devices can determine whether they have come in contact with that user during the last 14 days. The user's identity is not shared with other users as part of this process and the keys are private and anonymous.

12. Turning to the Committee's questions:

- *What interactions Apple and Google have had with the UK Government regarding a contact tracing app;*

13. Over a period of weeks we have had several discussions with NHSx and their developers about their objectives for a contact tracing app and their suggested design, in a series of calls. We have kept officials elsewhere in the government informed of progress. Discussions initially included exploration of the requirements of App Store guidelines, and most recently our plans for the API. We would characterise our interactions as constructive and friendly.

14. We have additionally held discussions with the Information Commissioner's Office, which we touch on below.

- *What interactions Apple and Google have had with other national governments regarding a contact tracing app;*

15. Like the UK, many other governments or public health authorities have approached us for support or guidance as to how to place a contact tracing app on the App Store. They have also sought assistance with integration with our operating system so as to ensure optimal levels of contact tracing identifications. In this regard many of them have made suggestions for updates which were certainly a factor in our recent announcements. We have held similar discussions with many of these as we have with the UK.

- *Data privacy issues for contact tracing apps, and how Apple and Google's work addresses these issues;*

16. As you would expect given our commitment to privacy, Apple at all times considers that ensuring strong privacy protections is paramount and have developed the system with that fully in mind.

17. Privacy is at the forefront of the design and the technology will include a number of important user protections:

— This system never collects location data, and does not share information about the people you come in to contact with - your identity is not revealed to other users, Google or Apple
— Each user will have to make an explicit choice whether to turn on the technology, and it can be turned off by the user at any time
— The system is only used for contact tracing by public health authorities, and isn't monetised
— Privacy preserving beacons rotate every 10-20 minutes, to help prevent tracking
— Exposure notification is only done on device, under the user's control
— People who test positive are not identified to other users, Apple or Google
— You control any data you choose to share, and decide if you want to share it
— Google and Apple can disable the exposure notification system on a regional basis when it is no longer needed

18. In all such matters, we seek to take the utmost account of the views of Data Protection Regulators and accordingly actively sought the views of the Information Commissioner (ICO). We were pleased therefore to note that the Information Commissioner took the step on 17 April to publish a formal legal Opinion which examined the Apple Google Contact Tracing Framework and issued a positive conclusion - https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy/ - based on the information which we had made available at that time. We are continuing to keep in close contact with the ICO as our framework for Exposure Notifications develops.

- *What assessment Google and Apple have made of the uptake of contact tracing apps*

19. We haven't made specific assessments. We are very clear that we are not putting forward this framework in the belief that contact tracing apps are a silver bullet, but rather in response to the requests that we have received from public health authorities and Governments who have formed the view that they can be of assistance. We are seeking to amplify their efforts on relation to contact tracing.

- *What legislation and regulatory guidance, if any, would be required to support the development of contact tracing applications in the UK*

20. We are working within existing legislative rules, and are closely liaising with data protection authorities to ensure they understand our approach. As we outlined above we have had detailed dialogue with the Information Commissioner's Office, which has now published a legal Opinion. Part of the reason we approached the ICO (and other national data protection authorities) is to ensure the appropriate body can drive the legal guidance.

***(April 2020)***