



STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL

LETITIA JAMES
ATTORNEY GENERAL

June 15, 2020

VIA EMAIL

Ms. Katherine L. Adams
Senior Vice President and General Counsel
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014

Re: COVID-19 Smartphone Apps

Dear Ms. Adams:

I write to follow up on recent discussions my Office has had with Apple staff regarding COVID-19 smartphone apps that Apple has made or will make available in its App Store. One set of apps discussed uses an application program interface (“API”), jointly developed by Apple and Google, for notification of exposure to a COVID-19 positive individual (“exposure notification apps”). Also discussed were apps that purport to allow contact tracing, including by notifying a user that she has visited the same specific geographic location as a COVID-19 positive individual (“contact tracing apps”). Both types of apps have received substantial media attention, and public interest is likely to increase as the COVID-19 pandemic continues and such apps proliferate.

Apps can play an important role in helping stop the spread of COVID-19, but more needs to be done to protect consumers’ personal information and to minimize consumer confusion. It is imperative that apps that use sensitive health information be developed only by public health agencies, to ensure that appropriate protections are in place and to provide accountability. It is also critical that app developers provide clear disclosures that enable users to understand the differences between the two types of COVID-19 apps, so they can provide informed consent before downloading and using them.

I appreciate Apple’s efforts to address the privacy and implementation concerns outlined

in my Office's initial letter, which focused on exposure notification apps. Apple communicated that it has undertaken the following protective measures for exposure notification apps (those that use the exposure notification API):

- Only public health authorities (one per state) are allowed to develop the apps.
- No personally identifiable information can be exchanged via the apps, which exchange random, anonymous Bluetooth identifiers that are stored only on a user's device.
- The apps may not access the device's geolocation information, and allows the collection and use of other data only by public health authorities, solely for COVID-19 response efforts, after user consent.
- To activate the apps and thus exchange random, anonymous Bluetooth identifiers, users must consent at both the operating system and app levels.
- The apps will delete temporary exposure keys and random, anonymous identifiers from users' phones on a 14-day rolling basis, and the user can also delete the keys manually (including by deleting the app).

Apple staff confirmed that contact-tracing apps (those that do not use the exposure notification API) offered on the App Store are not subject to the same requirements, and so may have different or lesser privacy protections.

I continue to have concerns about the accuracy of exposure notification events communicated via exposure notification apps, as Apple has stated that it will not dictate to app developers:

- How the apps will verify the accuracy of COVID-19 diagnoses that the apps use to trigger exposure notifications.
- Specific parameters for defining an "exposure notification" event (developers will use time and distance variables within a certain range).

To ensure that both exposure notification apps and contact tracing apps protect consumer information, and that users can provide informed consent, I request that Apple take the following additional steps:

- Allow only public health authorities verified by Apple to make such apps available on the App Store.¹
- Require the apps to provide clear and conspicuous disclosures regarding:
 - Whether the app employs the exposure notification API or a different protocol, which may have different privacy protections.
 - The types of user information they collect.

¹ This request does not apply to apps that do not transmit personal health information, such as notifications about exposure to an individual who has tested positive for COVID-19. But Apple should verify the identity of developers of such apps.

Ms. Katherine L. Adams

June 15, 2020

Page 3 of 3

- The risk of false positive and false negative notifications of exposure to someone with COVID-19, in particular due to the limitations of how an “exposure event” is defined.
- The lack of a uniform method of verification of the positive COVID-19 diagnoses used to trigger exposure notifications, which may impact validity of those notifications.
- That a user consenting to download and use an app that uses the exposure notification API will provide anonymous identifiers to all nearby devices.
- Bar developers of such apps from using data from the app to identify users.
- Bar developers of such apps from using targeted advertising or in-app sales.
- Require such apps to delete users’ information on a rolling 14-day basis, and to provide consumers with an easy-to-use mechanism to delete all user information upon request.

Taking these steps will help protect consumers’ sensitive personal information, minimize the risk of consumer confusion, and potentially increase the use of reliable COVID-19 apps that can benefit public health by reducing the spread of COVID-19.

Please confirm your receipt of this letter by Friday, June 19. If you have any questions, please contact Michael Reisman at (212) 416-6269.

Sincerely,



Letitia James
New York Attorney General

cc: Fred Zeytoonjian, Senior Manager of State and Local Government Affairs, Apple Inc.
(fzeytoonjian@apple.com)