August 7, 2018

The Honorable Greg Walden
Chairman, House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Re: July 9, 2018 Letter to Mr. Tim Cook

Dear Mr. Chairman:

Thank you for your inquiry regarding the capabilities of Apple iPhone devices. Not all technology companies operate in the same manner — in fact, the business models and data collection and use practices are often radically different from one another. Apple's philosophy and approach to customer data differs from many other companies on these important issues.

We believe privacy is a fundamental human right and purposely design our products and services to minimize our collection of customer data. When we do collect data, we're transparent about it and work to disassociate it from the user. We utilize on device processing to minimize data collection by Apple. The customer is not our product, and our business model does not depend on collecting vast amounts of personally identifiable information to enrich targeted profiles marketed to advertisers.

Because we strongly believe the customer should control their personal information and the way it's used, we provide a number of easily accessible resources on our website so that they can make wise choices. Most of your questions are addressed in public-facing documents such as our privacy website, which can be found at www.apple.com/privacy. In addition, we recently answered similar questions from Senator Charles Grassley, and our responses are available online.[1]

Innovation at Apple means designing a new product or service with customer privacy as a key element of design, and not an obligation. We hope that the responses below are helpful in understanding these topics and make clear Apple's position that customers are entitled to transparency, choice, and control over their personal information. We would be pleased to brief Committee staff at your convenience.

Sincerely,

Timothy Powderly
Director, Federal Government Affairs
Apple

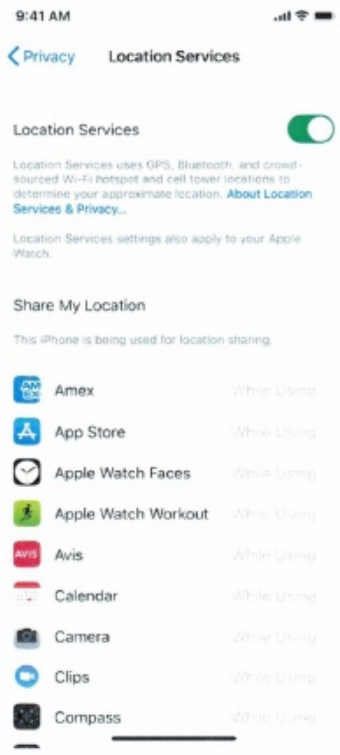
Apple
One Apple Park Way
Cupertino, CA 95014
T 408 996-1010
F 408 996-0275
www.apple.com

[1] Letter from Timothy Powderly, Director, Federal Government Affairs, Apple, to Senator Charles E. Grassley, United States Senate (July 3, 2018), available at https://www.judiciary.senate.gov/imo/media/doc/2018-07-03%20Apple%20to%20CEG%20(Data%20Privacy).pdf.

Background on Location Information

iPhone runs the iOS operating system, which provides users with granular tools to exercise control over the collection and use of location information. Unlike other companies, Apple does not retain a historical record of location data associated with a customer's name or AppleID for any of our services. Nor does Apple use identifiable location information for targeted advertising.

Consistent with Apple's position on privacy, the choice of whether to take advantage of location-based services is solely up to the user; iOS does not set a default choice. As part of the iPhone setup process, users are asked explicitly whether they wish to enable location-based services. After setup, users can easily turn on and off location-based services at any time by going to *Settings > Privacy > Location Services*.



Use of Location Services

If a user has iPhone Location Services turned off, then iPhone's location information stays on the device and is shared only to aid response efforts in emergency situations. For safety purposes, and aligned with legal and regulatory requirements, an iPhone's location information may be used when an emergency call is placed to aid response efforts regardless of whether Location Services is enabled.

When a user enables iPhone's Location Services for the first time, iOS allows the user to grant individual apps access to information on iPhone's location.[2] Users can control access to iPhone location information by individual apps when prompted by a notification or by visiting *Settings > Privacy > Location Services*.

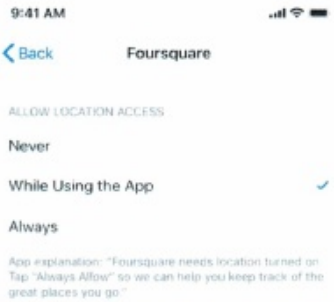
iOS requires that third party apps request access to location information via a just-in-time pop-up notification. iOS mandates those apps provide users with a choice to grant the app access to location information "always," "never," or "while using the app."[3]

[2] Apps downloaded while Location Services is disabled will not be able to request access to location information. Preferences for previously downloaded apps are saved and restored if a user later re-enables Location Services, but location information isn't available while Location Services is disabled. When Location Services is restored, apps that do not have a saved preference may prompt the user to select one using an in-app just-in-time pop-up notification, or the user can set a preference on the Location Services page in Settings.

[3] In iOS 11, Apple mandated that app developers provide users with the option to only share their location information with the app "while using the app" to help ensure that users were being provided with full and granular control over when and how to share their location information.

Apple also requires and iOS enforces that apps requesting access to Location Services provide users with information on its proposed use of the location information so that users can make informed decisions about when and with whom to share their data.[4] Users can then tap to allow or deny access to their location information.

Users are always in control over these selections. Users can revisit them or make additional selections, by visiting Location Services within their Privacy Settings, tapping on the name of an individual app and tapping to indicate whether they would like to share their location information "always," "never," or "while using the app." If a user permits a third-party app to have access to their location, this location information is never accessed or processed by Apple.



If an app makes use of its permission to access location information while in background mode (i.e., not running in the foreground on the device), iOS reminds users that they selected "always," and users have an additional opportunity to review their choice and decide if they want to change the permissions they granted.

Calculating Approximate Location

Location-based services rely on a mobile device's ability to provide location information quickly and consumer expectations demand the ability to identify device location nearly instantaneously. Calculating a device's location using GPS satellite data alone can take minutes. iPhone uses an industry-standard practice called assisted GPS to reduce this

---

[4] If the app does not provide a purpose, iOS does not permit it to request location. *See also App Store Review Guidelines*, Section 5.1.5, available at https://developer.apple.com/app-store/review/guidelines.

time to just a few seconds by using Wi-Fi hotspot, cellular tower, and Bluetooth data to find GPS satellites or to triangulate location when GPS satellites are not available (such as when the user is in a basement). iOS calculates location on iPhone itself, using a crowdsourced database of information on cellular towers and Wi-Fi hotspots.

The crowdsourced database used by iOS to help quickly and accurately approximate location is generated anonymously by tens of millions of iPhones. Whether an iPhone participates in the creation of the crowdsourced database depends on whether the iPhone has enabled Location Services. iPhones with Location Services enabled collect information on the cellular towers and Wi-Fi hotspots that the iPhones observe. (iPhone does not crowdsource Bluetooth beacon information.) iOS saves this information locally on iPhone until it is connected to Wi-Fi and power, at which point the device makes an anonymous and encrypted contribution to the crowdsourced database. If iPhone cannot contribute the data to the crowdsourced database within seven days (if iPhone was not connected to Wi-Fi and power during this period), iOS permanently deletes the data.

As highlighted above, iPhone offers users a single simple and easy to use mechanism for controlling the collection and access of location information: the user's Location Services setting. Whether Location Services is enabled is the key determinant as to whether iPhone collects or uses location information, a fact that is clear in our responses to Questions 1 - 8, below. Unlike other companies, Apple does not retain a historical record of location data associated with a customer's name or AppleID for any of our services. Nor does Apple use identifiable location information for targeted advertising.

Responses to Questions 1 - 8

1. When an iPhone lacks a SIM card, is that phone programmed to collect and locally store information through a different data-collection capability, if available, regarding:

(a) Nearby cellular towers;

Yes, if Location Services is enabled and iPhone is not in Airplane Mode.

(b) Nearby WiFi hotspots; or,

Yes, if Location Services is enabled and iPhone has Wi-Fi enabled.

(c) Nearby Bluetooth beacons?

No.

2. If the answers to any of the preceding questions are "yes," are iPhones lacking SIM cards programmed to send this locally-stored information to Apple when one or more networking capabilities are established?

Yes, if a user has enabled Location Services and iPhone has collected and locally stored cellular tower or Wi-Fi hotspot data. iPhone will share this information with Apple in an anonymous and encrypted form if and when connected to Wi-Fi and power within seven days of collection. This anonymous data is not used to target advertising to the user.

If a user has disabled Location Services, locally-stored information about cellular towers and Wi-Fi hotspots is not sent to Apple.

3. When the WiFi capabilities on an iPhone are disabled, is that phone programmed to collect and locally store information through a different data-collection capability, if available, regarding:

(a) Nearby cellular towers;

Yes, if Location Services is enabled and iPhone is not in Airplane Mode.

(b) Nearby WiFi hotspots; or,

No.

(c) Nearby Bluetooth beacons?

No.

4. If the answers to any of the preceding questions are "yes," are iPhones with disabled WiFi programmed to send this locally-stored information to Apple when one or more networking capabilities are established?

Yes, if a user has enabled Location Services and iPhone has collected and locally stored cellular tower data. iPhone will share this information with Apple in an anonymous and encrypted form if and when connected to Wi-Fi and power within seven days of collection. This anonymous data is not used to target advertising to the user.

If a user has disabled Location Services, locally-stored information about cellular towers is not sent to Apple.

5. When the Bluetooth capabilities on an iPhone are disabled, is that phone programmed to collect and locally store information through a different data-collection capability, if available, regarding:

(a) Nearby cellular towers;

Yes, if Location Services is enabled and iPhone is not in Airplane Mode.

(b) Nearby WiFi hotspots; or,

Yes, if Location Services is enabled and iPhone has Wi-Fi enabled.

(c) Nearby Bluetooth beacons?

No.

Question 6: If the answers to any of the preceding questions are "yes," are iPhones with disabled Bluetooth programmed to send this locally-stored information to Apple when one or more networking capabilities are established?

Yes, if a user has enabled Location Services and iPhone has collected and locally stored cellular tower or Wi-Fi hotspot data, iPhone will share this information with Apple in an anonymous and encrypted form if and when connected to Wi-Fi and power within seven days of collection. This anonymous data is not used to target advertising to the user.

If a user has disabled Location Services, locally-stored information about cellular towers and Wi-Fi hotspots is not sent to Apple.

Question 7: When the location services capabilities on an iPhone are disabled, is that phone programmed to collect and locally store information through a different data-collection capability, if available regarding:

(a) Nearby cellular towers;

No.

(b) Nearby WiFi hotspots; or,

No.

(c) Nearby Bluetooth beacons?

No.

Question 8: If a consumer using an iPhone has disabled location services for multiple apps, but then reenables location services for one app, are iPhones programmed to reenable location services for all apps on that phone?

No. iOS allows users to control access to location information on an app-by-app basis — if a user reenables access to location information for one app, that action does not reenable access to location information for all apps on the iPhone. For users that enable Location Services, preferences for each app that has requested access to location information can be reviewed and changed at *Settings > Privacy > Location Services.*

(a) If yes, how is this reenabling of location services for all apps disclosed to a user?

N/A.

Background on iPhone Microphone Functionality

iPhone is equipped with a microphone that is used to support many iOS features, as well as Apple and third party apps. We have worked to design iOS and Apple apps so that the processing of information collected by the microphone stays on the device where possible and the information is never shared with Apple or others unless the user takes an action to do so. Microphone access by Apple apps (such as Voice Memos) and third party apps requires an affirmative act by the user.

If a user has enabled "Hey Siri" functionality on their iPhone, Siri can be accessed using the clear, unambiguous audio trigger "Hey Siri."[5] A speech recognizer on iPhone runs in a short buffer on the device and listens for the two words "Hey Siri." The speech recognizer uses sophisticated local machine learning to convert the acoustic pattern of a user's voice into a probability that they uttered a particular speech sound and, ultimately, into a confidence score that the phrase uttered was "Hey Siri." Up to this point, all audio data is only local on the device in the short buffer. If the score is high enough, iOS passes the audio to the Siri app and Siri wakes up and appears on screen.

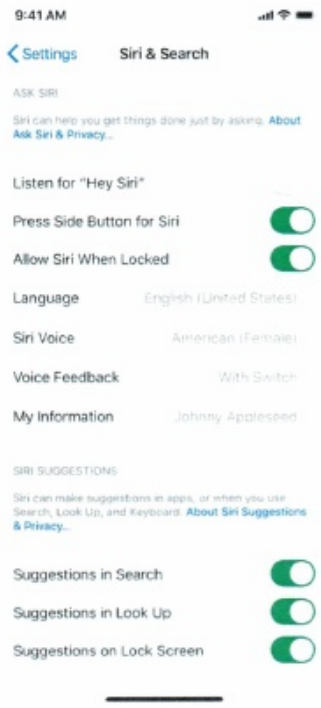
When Siri wakes up, its first task is to confirm that the speech recognizer correctly identified the audio trigger ("Hey Siri"). Unlike other similar services, which associate and store historical voice utterances in identifiable form, Siri utterances, which include the audio trigger and the remainder of the Siri command, are tied to a random device identifier, not a user's Apple ID. Siri utterances are sent to Apple and handled in accordance with Apple's Privacy Policy.[6] Users have control over the random device identifier associated with Siri utterances, which can be reset at any time by toggling Siri and Dictation[7] off and back on. When the identifier is reset, Apple deletes information it stores that is associated with the identifier.

---

[5] Siri can also be accessed through touch interactions between the user and device, such as when a user puts pressure on the home button.

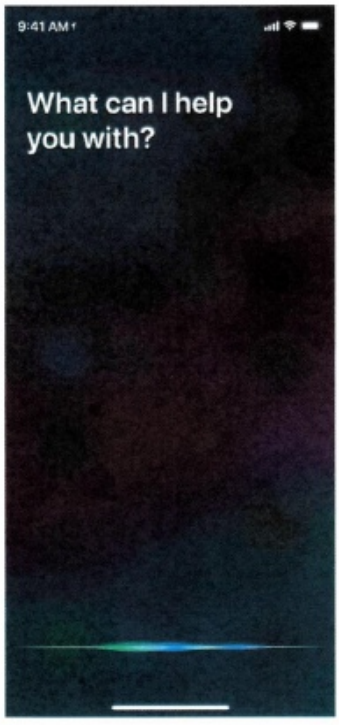
[6] Apple's Privacy Policy is available at https://www.apple.com/legal/privacy/en-ww.

[7] Users can control Siri at *Settings > Siri & Search*, and Dictation by visiting *Settings > General > Keyboard > Dictation.*



Apple doesn't provide third-party app developers with access to Siri utterances. Detailed information about how Apple handles Siri data is presented to users when they activate Siri, and is available at *Settings > Siri & Search > About Ask Siri & Privacy*.

When Siri is listening to a user's request, a visual indicator is presented to the user.



Apple's Developer Guidelines require its developers to display a visual indicator when their app is collecting audio information from the microphone (see below).

Responses to Questions 9 and 10

Question 9: Do Apple's iPhone devices have the capability to listen to consumers without a clear, unambiguous audio trigger?

iPhone doesn't listen to consumers except to recognize the clear, unambiguous audio trigger "Hey Siri." The iPhone microphone can be activated by a clear user action, such as making a call or tapping the "Record" button. Apple's Developer Guidelines require its developers to display a visual indicator when their app is collecting audio information from the microphone.

(a) If yes, how is this data used by Apple? Please describe any use or storage of these data.

iPhone doesn't listen to consumers, except to recognize the clear, unambiguous audio trigger "Hey Siri." As described above, the on-device speech recognizer runs in a short buffer and doesn't record audio or send audio to the Siri app if "Hey Siri" isn't recognized.

(b) If yes, what access to this data does Apple give to third parties, including app developers? Please describe and include screen shots of disclosures or terms of service governing such access or use as appropriate.

N/A. Apple doesn't provide Siri utterances to third parties.

(c) If yes, has Apple considered using a visual, or other alert, to let consumers know when a device's microphone is recording? Please describe why, or why not, such an alert is, or is not, provided on iPhones or other smart devices running on an iOS operating system.

Apple provides a visual alert when Siri is listening to a user's request, and Apple's Developer Guidelines require its developers to display a visual indicator when their app is collecting audio information from the microphone.

10. Do Apple's iPhone devices collect audio recordings of users without consent?

No.

(a) If no, please include screen shots and links to public disclosures made to users about this collection.

N/A.

Responses to Questions 11 - 15

Question 11: Please provide copies of all of Apple's policies for data collection via the microphone, or via WiFi, Bluetooth, or cellular networking capabilities on Apple's iPhone devices.

Apple gives iPhone users control over the functionality of microphone, Wi-Fi, Bluetooth, and cellular capabilities on iPhone, including:

- The ability to view or revoke access by third-party applications that have requested access to the microphone at *Settings > Privacy > Microphone*
- The ability to enable or disable Wi-Fi by visiting *Settings > Wi-Fi*
- The ability to enable or disable Bluetooth by visiting *Settings > Bluetooth*
- The ability to enable or disable the use of cellular data, including on an app-by-app basis, by visiting *Settings > Cellular*

When users share information with Apple, it is handled in a manner that is consistent with the Apple Privacy Policy, which can be accessed at any time by visiting https://www.apple.com/legal/privacy/en-ww.[8] In addition to the Apple Privacy Policy, Apple employs the privacy best practice of providing users with layered notices about how we handle personal information, providing users with relevant information about Apple's privacy practices at the time they need it. We use this approach to provide additional information about Apple's privacy practices in a manner that is easily understandable and readily available to the user through placement in close proximity to relevant settings that provide control over iPhone functionality, including data collection and use.

For example, we make available a number of disclosures that provide information "About" the privacy practices of Apple products and services. These "Abouts" present users with details on how information, including user or device data, is used to provide certain services. "About" pages that include information on data collected via the microphone, or about iPhone Wi-Fi, bluetooth, or cellular networking capabilities, include pages on Siri, Dictation & Privacy; Siri Suggestions & Privacy; Wi-Fi Calling & Privacy; Location Services & Privacy; Device Analytics & Privacy; News & Privacy; and Emergency SOS & Privacy.

[8] Information about Apple's approach to privacy, how users can manage their privacy, and Apple's Privacy Policy are also easily accessible to users by visiting https://www.apple.com/privacy.

9:41 AM

Done

Ask Siri, Dictation & Privacy

Siri is designed to protect your information and enable you to choose what you share.

When you use Ask Siri and Dictation the things you say and dictate will be recorded and sent to Apple to process your requests. Your device will also send Apple other information, such as your name and nickname; the names, nicknames, and relationship with you (e.g., "my dad") of your contacts, music you enjoy, HomeKit-enabled devices in your home (e.g., "living room lights"), the names of your photo albums, the names of Apps installed on your device (collectively, your "User Data"). All of this data is used to help Ask Siri and Dictation on your iOS device and any paired Apple Watch understand you better and recognize what you say. It is not linked to other data that Apple may have from your use of other Apple services.

If you have Location Services turned on, the location of your device at the time you make a request will also be sent to Apple to help Ask Siri and Dictation improve the accuracy of its response to your requests. You may choose to turn off Location Services for Ask Siri. To do so, open Settings > Privacy > Location Services > Siri & Dictation and select Never. You may choose to turn off Location Services for your HomePod in the HomePod settings in the Home App on your paired iOS device.

If you choose to allow third party Apps to

9:41 AM

Done

Siri Suggestions & Privacy

Siri is designed to protect your information and enable you to choose what you share.

Siri analyzes how you use your device to provide personalized suggestions and better search

Siri learns how you use your devices in order to personalize your experience. Using information stored on your device, such as your Safari browsing history, emails, messages, and contacts, as well as information contributed by other installed apps, Siri can provide suggestions in searches, Look Up, News, Photos Memories, and more. You can see the full list of features that Siri personalizes in the Siri & Search section of Settings.

Personalization is synced across your devices with end-to-end encryption.

Siri securely syncs this information among your devices, to make your experience consistent on all of them. This sync is done using end-to-end encryption.

To make suggestions and search results more relevant, some information is sent to Apple and not associated with you.

In some cases, such as when you use Siri Suggestions in Search, Look Up, or Safari, generalized topics of interest that Siri has

9:41 AM

Done

Location Services & Privacy

Location Services is designed to protect your information and enable you to choose what you share.

Location Services allows Apple and third-party apps and websites to gather and use information based on the current location of your iPhone or Apple Watch to provide a variety of location-based services. For example, an app might use your location data and location search query to help you find nearby coffee shops or theaters, or your device may set its time zone automatically based on your current location.

To use features such as these, you must enable Location Services on your iPhone and give your permission to each app or website before it can use your location data. Apps may request limited access to your location data (only when you are using the app) or full access (even when you are not using the app).

For safety purposes, however, your iPhone's location information may be used when you place an emergency call to aid response efforts regardless of whether you enable Location Services.

Location Services uses GPS and Bluetooth (where those are available) along with crowd-sourced Wi-Fi hotspot and cell tower locations to determine your device's approximate

9:41 AM

Done

Device Analytics & Privacy

Analytics is designed to protect your information and enable you to choose what you share.

iOS Device Analytics

iPhone Analytics may include details about hardware and operating system specifications, performance statistics, and data about how you use your devices and applications. None of the collected information identifies you personally. Personal data is either not logged at all, is subject to privacy preserving techniques such as differential privacy, or is removed from any reports before they're sent to Apple. You can review this information by going to Settings on your iOS device, tapping Privacy, tapping Analytics and looking under Analytics Data.

If you have consented to provide Apple with this information, and you have Location Services turned on, the location of your devices may also be sent to help Apple analyze performance issues (for example, the strength or weakness of a mobile signal in a particular location). This analytics location data may include locations such as the location of your devices once per day, the location where a call ends or the location of a failed in-store transaction. You may choose to turn off Location Services for Analytics at any time. To do so, open Settings, tap Privacy, tap Location Services, tap System Services and turn off the

9:41 AM

Done

News & Privacy

News is designed to protect your information and enable you to choose what you share.

Protecting the privacy and security of your information is a priority for everyone at Apple. We work hard to collect only the data we need to make your experience better, and when we do collect data we believe it's important for you to know what we're collecting and why we need it, so you can make informed choices. Apple News, like every Apple product, is designed around these principles.

Apple collects information about how you use Apple News in order to tailor features to your personal interests. These features include For You — where you will find a personal news feed that highlights the best stories for you from your favorite channels or topics and Search— which includes suggested search topics based on trending issues. Apple is able to make these features possible by collecting information about which stories you read, save, or share, and the topics and publications you follow. When you enable notifications for a channel, we store that information as well as your subscriber status to that channel to notify you about breaking events.

We understand that the articles you read are personal, so we designed News so your reading activity is not linked to other Apple services

9:41 AM

Done

Emergency SOS & Privacy

Emergency SOS is designed to protect your information and enable you to choose what you share.

- When you use Emergency SOS, your device will attempt to call emergency services. To allow the dispatcher to assist you, this call may include your location, regardless of whether you enable Location Services.
- Once the call ends, you can choose to notify your emergency contacts with a message that says you have called emergency services. This message also includes your current location. You can manage your emergency contacts by editing your Medical ID in the Health app on iPhone.
- For a limited period of time, your device will send updates to your emergency contacts as your location changes.

When you use Emergency SOS, your device will attempt to call emergency services. To allow the dispatcher to assist you, this call may include your location, regardless of whether you enable Location Services. Once the call ends, you can choose to notify your emergency

Data collection by third party app developers is governed by the Apple Developer Program License Agreement ("PLA"), and the App Store Review Guidelines, available at https://developer.apple.com/app-store/review/guidelines, in addition to the privacy policies published by the individual third party app developers. Section 5 of the App Store Review Guidelines specifically addresses privacy, including data collection and storage (Section 5.1.1), data use and sharing (section 5.1.2), and location services (section 5.1.5). Further information about handling of data by third party app developers is addressed further in our responses to Questions 12 - 14, below.

Question 12: Please provide Apple's policies as they pertain to third party access and use, including but not limited to app developers and developer guidelines, of any data collected via the microphone on Apple's iPhone devices, particularly data not accompanied by a "trigger" phrase including "hey Siri."

Apple does not permit third party apps to collect microphone data without obtaining explicit user consent and providing a clear visual indicator.[9]

Consistent with Apple's view that privacy is a fundamental human right, we impose significant privacy-related restrictions on apps that are made available through the App Store. The App Store is a marketplace for third party apps and, when a customer chooses to download an app to an Apple device, the customer and app developer enter into a direct contractual relationship with one another governed by the terms of the developer's end user license agreement and privacy policy. Apple is not a party to these relationships; rather, developers are fully responsible for the content and services they provide in their apps. Notwithstanding the developer's responsibilities and direct relationship with customers, Apple requires developers to adhere to privacy principles, including consumer choice, and has implemented technical- and policy-level controls to help ensure those principles are respected.

Apple designs and builds technical controls into iOS and iPhone to help ensure customer data has strong protections. iOS has been a leading operating system in isolating user data in one application from other applications, as well as in protecting user data from unwanted access by any application.[10] Apple employs industry leading security and privacy design techniques to "sandbox"—or isolate—applications within containers. Third-party applications are required by policy and by technical controls built into iOS to obtain consent before accessing user data such as contacts, calendars, photos, location and health data, as well as the camera and microphone.[11]

---

[9] *See* App Store Review Guidelines, Section 2.5.14.

[10] iOS requires that all apps show that they come from a known and approved source and haven't been tampered with by having all executable code signed using an Apple-issued certificate. Once an app is verified to be from an approved source, iOS enforces security measures designed to prevent it from compromising other apps or the rest of the system. All third party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. System files and resources are also shielded from the user's apps and Apple APIs do not allow apps to grant themselves privileges to modify other apps or iOS itself.

[11] iOS prevents apps from accessing these and other data types without asking for and obtaining a user's explicit permission. If a customer provides an app with permission to access data in a protected data class, iOS extends the sandbox of the app to allow it to do so. iOS also gives customers control over their data by providing them with the ability to withdraw consent later.

iOS and iPhone technical controls are reinforced by a set of policies, rules, and guidelines. Apple sets certain baseline expectations for privacy and data use in the PLA and in the App Store Review Guidelines. App developers must meet these expectations before they can market an app on the App Store and must also provide users with their own disclosures. Together, these extensive and detailed requirements—which cover a broad range of privacy issues from data use, to notice, to appropriate consents—reflect our core belief that customers should be in the driver's seat when it comes to choosing what they share and with whom.

For example, the PLA provides that each app on the App Store must provide clear and complete information to users regarding its collection, use, and disclosure of user data and must have a privacy statement or privacy policy if it collects any user data. For example, Section 3.3.9 states:

> You and Your Applications (and any third party with whom You have contracted to serve advertising) may not collect user or device data without prior user consent, whether such data is obtained directly from the user or through the use of the Apple Software, Apple Services, or Apple SDKs, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising in accordance with Sections 3.3.12 and 3.3.13. You may not broaden or otherwise change the scope of usage for previously collected user or device data without obtaining prior user consent for such expanded or otherwise changed data collection. You may not use analytics software in Your Application to collect and send device data to a third party. Further, neither You nor Your Application will use any permanent, device-based identifier, or any data derived therefrom, for purposes of uniquely identifying a device.

The App Store Review Guidelines expand upon the PLA's requirements relating to customer privacy by, for example, requiring apps to include an easily accessible and understandable way for customers to withdraw their consent to any data collection from the iPhone. Apps that violate the App Store Review Guidelines may be removed from the App Store and egregious or repeated violations may result in termination of a developer's Apple Developer Program membership.

Those third party developers that comply with program requirements set forth in the PLA and the App Store Review Guidelines, including provisions on the collection and use of microphone data, may request permission to use the microphone in the context of their apps. For example:

- The PLA includes the following provision:

> 3.3.8 If Your Application captures or makes any video, microphone, or camera recordings, whether saved on the device or sent to a server (e.g., an image, photo, voice or speech capture, or other recording) (collectively "Recordings"), a reasonably conspicuous audio, visual or other indicator must be displayed to the user as part of the Application to indicate that a Recording is taking place.
>
> - In addition, any form of data, content or information collection, processing, maintenance, uploading, syncing, storage, transmission, sharing, disclosure or use performed by, through or in connection with Your

> Application must comply with all applicable privacy laws and regulations as well as any related Program Requirements, including but not limited to any notice or consent requirements.

- The App Store Review Guidelines include the following requirement:

> 2.5.14 Apps must request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity. This includes any use of the device camera, microphone, or other user inputs.

In addition to the provisions cited above, the PLA specifically provides that apps must comply with all applicable legal restrictions.

Question 13: Could Apple control or limit the data collected by third-party apps available on the App Store?

As noted above, iOS sandboxes third party apps so that they are restricted from accessing files stored by other apps and from making changes to the device. System files and resources are also shielded from the user's apps. Moreover, Apple APIs do not allow apps to grant themselves privileges to modify other apps or the iOS itself. Third-party applications are required by policy and by technical controls built into iOS to obtain consent before accessing user data such as contacts, calendars, photos, location and health data, as well as the camera and microphone.

Users also have control over targeted advertising through third-party apps by enabling Limit Ad Tracking. When a user enables Limit Ad Tracking, apps or advertisers that use Apple's Advertising Identifier are required to check the Limit Ad Tracking setting and are not permitted by Apple's guidelines to serve users targeted ads if they have Limit Ad Tracking enabled. When Limit Ad Tracking is enabled on iOS 10 or greater, this Advertising Identifier is replaced with a non-unique value of all zeros to prevent the serving of targeted ads. It is automatically reset to a new random identifier if a user disables Limit Ad Tracking.

(a) Please provide a list of all data elements that can be collected by a third-party app downloaded on an iPhone device about a user, including but not limited to contact lists stored on the iPhone device and location information generated by the iPhone device.

Users are provided with control to allow or deny access to information when applications request access to:

Location Services
Contacts
Calendars
Reminders
Photos
Bluetooth Sharing
Microphone
Speech Recognition
Camera

Health
HomeKit
Media & Apple Music
Motion & Fitness

Question 14: What limits does Apple place on third-party app developers' ability to collect information about users or from users' devices? Please describe in detail changes made in June 201[8] from prior policies.

Apple launched the App Store in 2008 and designed it with user privacy in mind. These values are reflected in the App Store's policies and we have not wavered from that position. Apple continually evaluates its technical and contractual controls relating to developer access to user data and refines its approach as appropriate. Developers look to collect and use data for evolving purposes, and Apple must learn and adapt as well in order to help protect its customers. To that end, we periodically update the iOS, PLA, and App Store Review Guidelines to address new privacy issues, such as the introduction of new APIs.

The PLA and App Store Review Guidelines were updated in June 2018, as part of our normal business practices, to provide additional clarity around the collection and use of user data in apps. For example, the updates include minimum requirements for the terms of an app's privacy policy, provisions to address developer compliance with the EU's recently enacted General Data Protection Regulation, and a codification of core privacy principles such as data minimization and transparency, among others.

We have also improved our iOS operating system over time to provide new technical protections for user data. For example, across multiple releases of iOS, we have created "just-in-time" pop-up notices, enforced via iOS security mechanisms, that require users to take an affirmative act to agree before an app can access certain user data, such as contacts, calendars, photos, the camera or microphone, location data, and health. We also started to require apps to include a clearly stated purpose for the collection of user data to be displayed when the app is requesting access to user data. We have changed location-access prompts—which require users to make an affirmative choice to share their location data—both to offer access only while the application is in use, or access "always" (even when the application is not visible). Users are free not to agree to provide developers with the data requested by the developer, and users can revisit their decisions at any time in their device Settings. Moreover, section 5.1.1 of the App Store Review Guidelines requires apps to respect user choice and prohibits behavior that attempts to manipulate users into granting consent:

> (iv) Access. Apps must respect the user's permission settings and not attempt to manipulate, trick, or force people to consent to unnecessary data access. For example, apps that include the ability to post photos to a social network must not also require microphone access before allowing the user to upload photos. Where possible, provide alternative solutions for users who don't grant consent. For example, if a user declines to share Location, offer the ability to manually enter an address.

Question 15: How does Apple monitor and evaluate whether third-party apps are following the App Store rules?

(a) Have any companies ever been suspended or banned from the App Store for violating the App Store rules?
(b) In those cases, if any exist, where users notified that their data was misused in violation of the App Store rules?
(c) If yes, please provide any screen shots of such notification and a description of the conditions under which such a notification would be sent by Apple.
(d) What recourse does Apple provide for users when their data is misused in such a case?

Apple enforces its rules and policies for third-party apps through the App Review process, in which all apps are reviewed by specialists for their compliance with the App Store Review Guidelines—which include rules concerning objectionable content, business model transparency, and malware, as well as user privacy, among other things—before they are made available on the App Store. Apps are assigned to specialists trained in the skills required to analyze those apps and who have access to software tools that identify certain processes and methods that are known to violate the App Store Review Guidelines. If needed, these specialists can escalate apps for enhanced review. Specialists reject apps they find to be out of compliance with the App Store Review Guidelines and provide their developers with an explanation of the issues and how they can be resolved. Developers can revise their apps to bring them into compliance and resubmit for review. The App Review team reviews more than 100,000 submissions per week, and rejects approximately 36,000 of those submissions due to various compliance issues.

Apple works to continually improve its app review tools. Apple also reviews its App Store Review Guidelines and modifies the Guidelines as appropriate to address new issues and types of violations. Moreover, our commitment to safety, security, and privacy does not end once apps are on the App Store. New versions of apps must again pass through the App Review process.

Apple also seeks to proactively address data use issues through its contractual relationships with developers and its App Review process. However, Apple does not and cannot monitor what developers do with the customer data they have collected, or prevent the onward transfer of that data, nor do we have the ability to ensure a developer's compliance with their own privacy policies or local law. The relationship between the app developer and the user is direct, and it is the developer's obligation to collect and use data responsibly, legally, and in accordance with the PLA and Guidelines. As described in the response to Question 12, iOS requires third-party apps to obtain explicit consent from users when those apps seek to access to certain types of user data.

However, when we have credible information that a developer is not acting in accordance with the PLA or App Store Review Guidelines or otherwise violates privacy laws, we will investigate to the extent possible, and take appropriate action, which may include removal of the app from the App Store and removal of the developer from the Apple Developer Program. Developers do violate the PLA and App Store Review Guidelines, although most violations are unintentional, unrelated to privacy issues, and easily corrected. And, we have removed apps for privacy violations. Furthermore, Apple re-

quires developers to understand and comply with applicable legal requirements, including notifying users if they are required to do so under data breach notification laws. Under the PLA, Apple has the right to terminate a developer's account immediately upon notice for engaging in prohibited behavior, including but not limited to impermissible uses of user data.

Background on the Enhanced Emergency Data Service

Apple cares deeply about the safety of our customers. Later this year, Apple will make available in the United States an Enhanced Emergency Data (EED) service in iOS 12 to provide first responders with more accurate information more quickly, in an effort to reduce emergency response times. EED supplements existing iPhone emergency call features; iPhones running iOS 12 will continue to deliver location data to emergency responders using methods present in iOS 11 and also share information through EED. Consistent with Apple's belief that individuals should be able to exercise choice around the handling of their data, iPhone users can disable EED at any time by visiting the Settings app on their iPhone.

EED works by providing information about an iPhone making an emergency call to a database relied on by first responders. When a 9-1-1 call is made from an iPhone running iOS 12, the iPhone will provide its estimated longitude and latitude (and how confident it is in this estimation), phone number, and mobile network to the database. Emergency responders can view this information in the database by entering the phone number of the emergency call they received.

Because emergency contexts are especially sensitive, Apple takes extra steps to ensure that our products and services protect the confidentiality, integrity, and availability of our users' data during an emergency call. Apple only sends the information to the database used by emergency responders, which is run by third party RapidSOS, if the emergency call is made from within an area where emergency responders rely on the database. If the call is made from a location where first responders do not use the database, no information is shared. Apple also requires that when RapidSOS receives the EED information it perform its own check that the emergency responders in the area where the call originated rely on the database; if they do not, Apple requires RapidSOS to immediately discard the information.

Apple also takes measures to protect the EED messages at rest and in transit. EED messages originate on iPhone and are never logged on Apple servers. EED messages are encrypted by Apple both in transit and at rest and Apple requires that RapidSOS do so as well. Apple relies on strong credentials to help ensure that EED messages are only transmitted between systems that have established their identities. And, Apple requires that RapidSOS delete EED messages no later than 12 hours after receipt. Apple has the right to audit RapidSOS to ensure that it is complying with its commitments regarding the handling of user data.

The response from the public safety has been overwhelming. Public safety agencies and associations have expressed great interest in expanding the adoption of this life-saving technology.

Response to Question 16

Question 16: Apple recently announced that it is entering into a partnership with a vendor called RapidSOS to provide enhanced location services for 9-1-1 calls to "public safety answering points" (PSAPs). Public statements from Apple reflect that this will be active later this year with iOS 12, the upcoming version of Apple's operating system. Please detail the data elements that will be shared with RapidSOS in this partnership.

iPhones with EED enabled will share the following information with RapidSOS upon initiation of an emergency 9-1-1 call: estimated longitude and latitude (and how confident it is in this estimation), phone number, and mobile network.

(a) What role will RapidSOS serve in the sharing and retention of this information?

RapidSOS provides emergency responders with access to a database of additional information on emergency callers (such as additional location information) designed to help emergency responders dispatch the response team best positioned to handle the incident. iPhones with EED enabled that initiate an emergency 9-1-1 call will share information on the device and location with RapidSOS for inclusion in the database used by emergency responders. Apple requires that RapidSOS delete EED messages no later than 12 hours following receipt.

(b) How will iOS 12 differ from iOS 11 and other previous Apple operating systems with respect to providing improved 9-1-1 call location services?

iOS 12 will offer EED in addition to the existing iPhone emergency call features.