Location Services Privacy Overview

Learn how Location Services protects your privacy.

November 2019

Contents

Introduction

Key Location Privacy Features

Location settings, features, and controls
Location Services acts as a gatekeeper between the user and apps that want to use location data. Location settings, features, and controls help keep users in control of this data.

Significant Locations
The Significant Locations feature allows iPhone, iPad, Apple Watch, and iCloud to learn locations that are important to users in a way that can't be read by Apple.

Bluetooth and Wi-Fi privacy
iOS 13 and iPadOS include new protections that help prevent apps from using Bluetooth and Wi-Fi to track users without their consent.

iBeacon
Apple's iBeacon specification allows apps to provide location-based experiences while keeping users in control.

Your location reveals some of the most sensitive information about you. Where you live and work, shop and eat, where you travel, and even where you receive medical care—all can be inferred by tracking your location data. Although it is sensitive, this data helps developers build relevant, personalized software experiences that help you navigate, facilitate the discovery of nearby people, businesses, and events, and more through mapping and other applications. To help protect users from the misuse of their location data, Apple builds software that empowers users to stay in charge of whom they share their location data with, when they share it, and for how long.

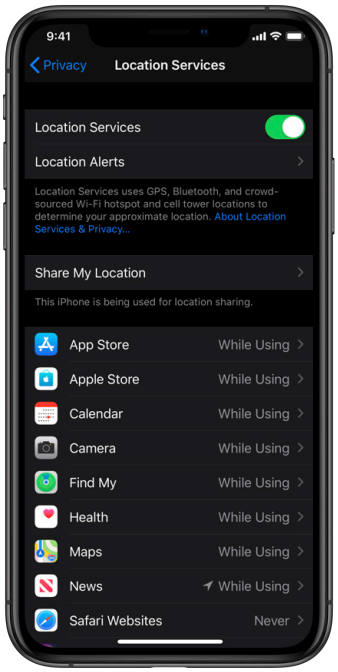
Privacy by design

Location Services in iOS, iPadOS, watchOS, and macOS provides a user's location. To determine this location, Apple devices leverage Global Positioning System (GPS) and Bluetooth beacons (where available) as well as crowd-sourced Wi-Fi hotspot and cell tower locations. Location Services has been designed from the ground up to protect user privacy. Data is processed on the user's device where possible, for example, in creating predictive traffic routing which displays estimated travel time on a device's lock screen. The architecture of Location Services helps minimize the amount of location data collected by Apple. When users choose to share identifiable location data with Apple or third parties, Apple designs features to give users transparency and control over how their data is being shared. And when non-personally identified location data is shared with Apple, techniques are used to help protect the identity of the user, such as with data used to improve Routing and Traffic. Finally, security best practices are integrated to protect data, for example using end-to-end encryption so that Apple can't read Significant Locations.

Control over Location Services

Location Services acts as a gatekeeper between a user's location data and the apps seeking to leverage this data. Location data enables a variety of personalized experiences. For example, an app might use a user's location along with the user's search query to help the user find nearby coffee shops or music venues. And the device can automatically set its time zone based on the current location so that alarms, appointments, and reminders remain accurate during international travel.

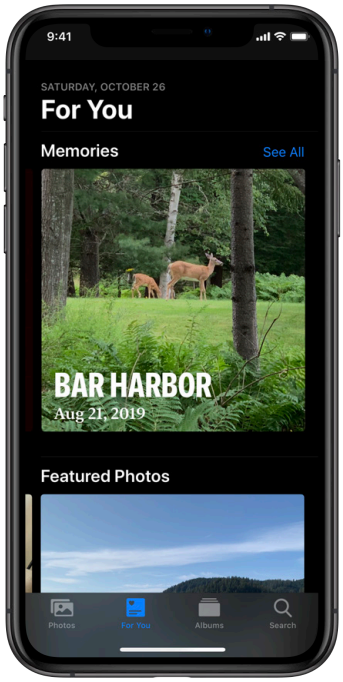
Users have the option of turning Location Services on during the Setup Assistant process when they're setting up a new device. After the Setup Assistant process, users can turn Location Services on or off in Settings. When Location Services is turned off, apps can't access the user's Location Services data at any time—this remains true whether an app is in use or not in use. Turning off Location Services will limit the ability of apps to provide relevant, location-based experiences. For example, if a mapping app doesn't have your location, it won't be able to give you turn-by-turn directions. For



Location Services lists the apps that have asked for permission to use location data, and users can control and edit these permissions. A hollow arrow next to the app indicates that location data may be used under certain conditions (users can tap on the app to learn more). A purple arrow indicates that location data has been used recently. A gray arrow indicates that location data has been used in the last 24 hours.

In the Maps interface, the blue dot marks your approximate location, while the blue halo is an indicator of precision.

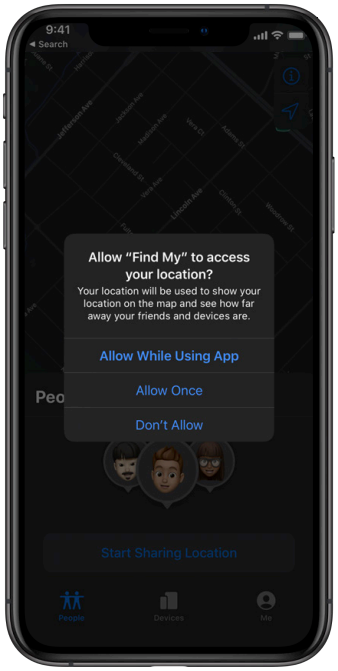
safety purposes, location information for an iPhone, iPad, or Apple Watch may be accessed to aid response efforts if the user places an emergency call, regardless of whether Location Services is enabled.



Location in the Photos app
When the user gives permission, the Camera app is granted permission to use location to geo-tag photos for suggesting Memories that intelligently complement where the user was when the photo was taken.

Location interface features

In addition to Location Services, there are other features that help users understand how their locations are being tracked. For example, the arrow in the status bar in iOS and iPadOS shows when Location Services is receiving location requests from apps asking for location data. If an app is actively locating the user, a black arrow appears in the status bar. In addition, users may be able to see at a glance how precisely their location is being measured by looking at an app interface that displays their location on a map. For example, Apple Maps shows your current location using a blue marker. Because the precision with which your location can be determined is limited, a blue halo will appear around this marker. The size of the halo shows approximately how precisely your location can be determined: the smaller the halo, the greater the precision. Third-party apps may adopt these design conventions in their apps as well.

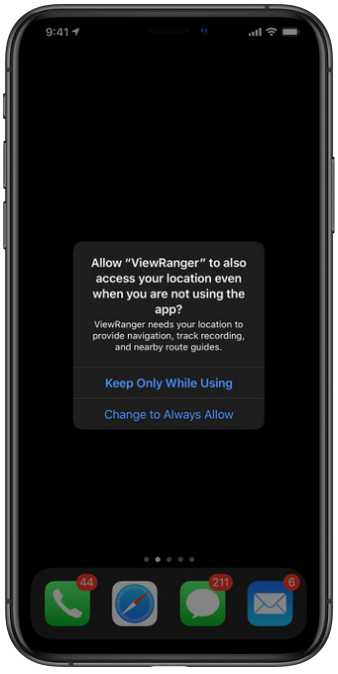


The location permission prompt in iOS 13 and iPadOS.

Location Services settings

In Location Services settings, users can see and control which Apple and third-party apps have permission to use data on the location of their iPhone, iPad, Apple Watch, or Mac. In iOS 13 and iPadOS, when an app makes its first location request, users are shown a prompt that informs them which app is making the request along with the developer’s explanation of how the app uses location data. Choosing Allow Once enables the app to access location data during that first session so a user can temporarily sample the app’s location-based services. Choosing Allow While Using App gives the app permission to access a user’s location data whenever the app is in use. Choosing Don't Allow prevents the app from accessing location data.

The Location Services settings are built for user transparency and control. Their primary purpose is to inform users about when and how their location data is being used and to enable them to control access for each app. All apps that have made location requests appear on a list within the Location Services settings. To make a change to an app’s access to location data, users can simply find the app on this list, tap the app, and then select their preferred level of access to location data. The choices include the following: no access (choose Never), access while using the app (choose Allow While Using App), or decide later (choose Ask Next Time).



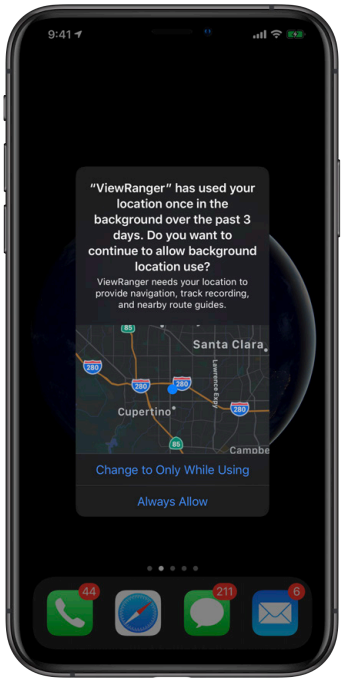
The background location prompt in iOS 13 and iPadOS.

Allowing location access in the background

Some apps use location data even while they are in the background. Upon an app’s first location request while it is in the background, the user will be notified that the app is requesting to use their location data and the app’s stated purpose for the request. Users have the option to Always Allow, enabling the app to access their location while in the background, or to Keep Only While Using, which would continue to prevent the app’s access while in the background and allow access only while the app is in use.

Background tracking notifications

When a user allows an app to always use their location and the app accesses their location in the background, the device will periodically show the user a notification prompt. This prompt reminds the user that their location is being shared in the background, displaying where their location was accessed while in the background, and giving them the ability to adjust their settings. Apps must comply with our App Store Guidelines for any such data use. To learn more, users can review the requesting app’s privacy policy to understand how their location data will be used, managed, and possibly shared with other entities.

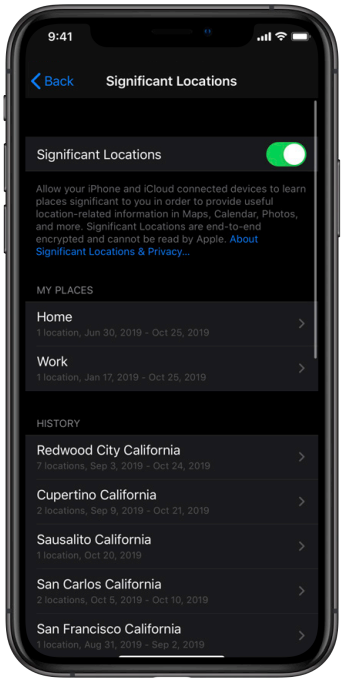


Background tracking notifications in iOS 13 and iPadOS.

On-device intelligence with Significant Locations

Significant Locations allows iPhone, iPad, Apple Watch, and iCloud to learn the places that are significant to a user in order to provide useful location-related features and information in a way that Apple can't read. Data collected about a significant location includes the address the user traveled to, when they traveled there, how long they stayed, the amount of time spent commuting to the location, the method used to reach the location (e.g., by car, by walking, etc.), and the total number of times the user has visited that place. This data is not shared with third parties, is fully encrypted, and can't be read by Apple. Features that leverage Significant Locations involve intelligent assistance and prediction, such as Memories in Photos and predictive traffic routing on the Lock screen. By processing Significant Locations on device, a device can provide personalized experiences without Apple or third parties learning sensitive details about your pattern of life.

In Settings > Privacy > Location Services > System Services > Significant Locations, users can turn Significant Locations off or on by tapping the toggle at the top of the page. They can scroll through their history of Significant Locations as well as clear this history by choosing Clear History at the bottom of the page. Users can also delete a specific location by tapping on that location and then choosing Edit and Delete.

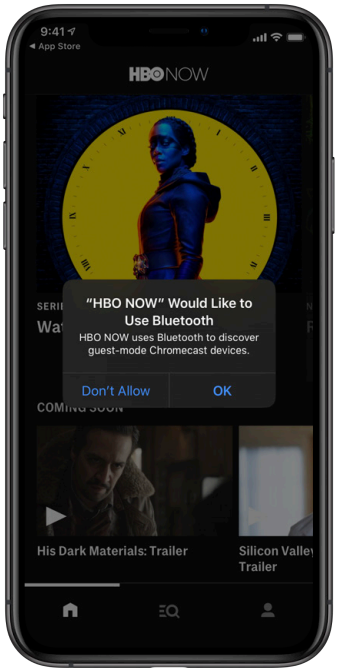


Significant Locations settings in iOS 13 and iPadOS. Significant Locations allows iPhone, iPad, Apple Watch, and iCloud to learn locations that are important to users in a way that cannot be read by Apple.

Bluetooth and Wi-Fi location privacy

Bluetooth and Wi-Fi enable helpful functionality by letting users connect to other devices and to the internet in the case of Wi-Fi. The locations of Wi-Fi networks and Bluetooth beacons are sometimes mapped and made publicly available, which means that the networks users connect to and beacons their devices discover might be used to track location. Some apps may have tried to circumvent the controls on location access that users have set up in Location Services by scanning for Bluetooth or Wi-Fi signals to infer the user's location. In iOS 13 and iPadOS, Apple is shutting such potential behavior down by introducing new controls for Bluetooth and limiting access to Wi-Fi networks by apps.

To protect users from Bluetooth location scanning, when an app requests Bluetooth access to a user's device with iOS or iPadOS, the user will be alerted about the request and how the app will use their Bluetooth data. Users can choose to allow or withhold access. Users can also visit the updated Bluetooth tab in Settings > Privacy to make a change to the access for each app that has requested it. Similar to Location Services, the Bluetooth tab enables users to see a comprehensive list of apps that have requested Bluetooth access and to individually turn each app's access on or off. Access to Bluetooth audio devices isn't impacted by these new controls and settings, so disallowing or disabling Bluetooth access will not prevent an app from playing audio to Bluetooth audio devices.



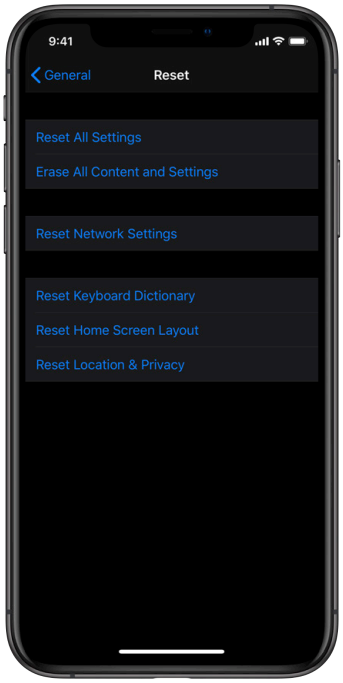
Bluetooth access prompt in iOS 13 and iPadOS.

To protect against Wi-Fi location scanning, iOS 13 and iPadOS limit the type of apps that can see the names of Wi-Fi networks the user connects to. Only apps that have already been granted user permission to access precise location data, that have been given permission to set up a virtual private network profile, or that have been given permission to configure a network on the system on the user's behalf will be able to see the names of Wi-Fi networks the user is connected to. In the case of apps that have permission to configure a network on the system on the user's behalf, the app will only be able to see the names and MAC addresses of Wi-Fi networks configured by the app itself.

iBeacon privacy

Beacons are devices that emit a Bluetooth Low Energy signal and are installed in a physical location. Once a beacon is set up, an app that has integrated a beacon protocol can push notifications to users who have downloaded the app and approach the beacon. Beacons are a small subset of Bluetooth technology applications, primarily used in online/offline retail and tourism experiences. For example, after beacons are set up in a store, an app could notify the user about a promotion related to the product that the user is walking by. Likewise, a sports league's app could surface seat information as the user moves through the stands, and a museum's app could offer information about each artwork as the user walks through the gallery.

In 2013, Apple created iBeacon, a protocol that has been adopted by beacon manufacturers and app developers to create personalized, relevant, location-based software experiences while respecting user privacy. Since apps that integrate iBeacon enable developers to know when an iPhone user is in close proximity to a beacon, iBeacon usage is considered location data and integrated with Location Services. This means that if a user installs an app that leverages iBeacon and goes to Location Services to give this app permission to use their location data While in Use, the app will also be able to access their location via iBeacon while the app is in use, but not when the app is in the background. If a user wants to turn off beacon access for a particular app, they can go to the Location Services tab within Privacy Settings and turn that app's location access to Never. Tying iBeacon to Location Services helps ensure that users have transparency and control over how their location data is used by beacons that implement iBeacon. And with Bluetooth controls starting in iOS 13 and iPadOS, apps are no longer able to use Bluetooth beacons that use other, less privacy-friendly protocols unless the user explicitly consents to Bluetooth access for the app.



Users can reset a device's location settings to the factory default by going to Settings > General > Reset and tapping Reset Location & Privacy. When location and privacy settings are reset, apps will stop using location data until a user grants them permission again.

Improving Location Services performance

Apple continuously improves the precision of inferences about device location through the crowdsourcing of non-personally identifying data from Apple devices. This data is transmitted from the device to Apple using encryption. If a user has turned on Location Services, their device will periodically send the geo-tagged locations of nearby Wi-Fi hotspots and cell towers to Apple to further improve Apple's database of Wi-Fi hotspot and cell tower locations. This helps Apple to provide real-time, localized services in more places around the world. To protect user privacy, the submission uses a random, rotating identifier so that Apple can't tie multiple submissions together or tie submissions to a user's identity.

In addition, when a device is physically moving (for example, when the user is walking or in a car), iOS periodically sends location and speed data to Apple, to help improve our location services for Routing and Traffic, including Siri and Maps. For example, if you're on a road trip and Location Services is turned on, your GPS-enabled iOS device will periodically send GPS locations and travel speed information to Apple to strengthen Apple's crowdsourced road traffic database—Siri and Maps will use this data to dynamically optimize your route.

To protect user privacy, this data is associated with an identifier that rotates at the conclusion of a trip, not with the user's Apple ID or any other account information. Rotating the ID at the conclusion of the trip makes it harder for Apple to piece together a history of any user's activity over time. On busy roads, data is also sent to Apple and partners as part of providing real-time traffic information. By analyzing historical traffic patterns, Apple developed a custom filter to protect user privacy that only shares data from small roads if those roads have more than a certain level of activity. Users can turn off Routing and Traffic collection in Settings.

Conclusion

Apple is committed to helping protect customers with leading privacy and security technologies that are designed to safeguard personal information. Location Services is built with that commitment in mind. The following Apple privacy principles are deeply integrated into Location Services:

- Process data on device where possible.
- Minimize the amount of data collected by Apple and shared with third parties.
- Provide transparency and control around data that is shared.
- Protect the user's identity when sharing sensitive information with Apple.
- Implement security best practices to protect user data.

To learn more about Apple's commitment to privacy, go to apple.com/privacy.