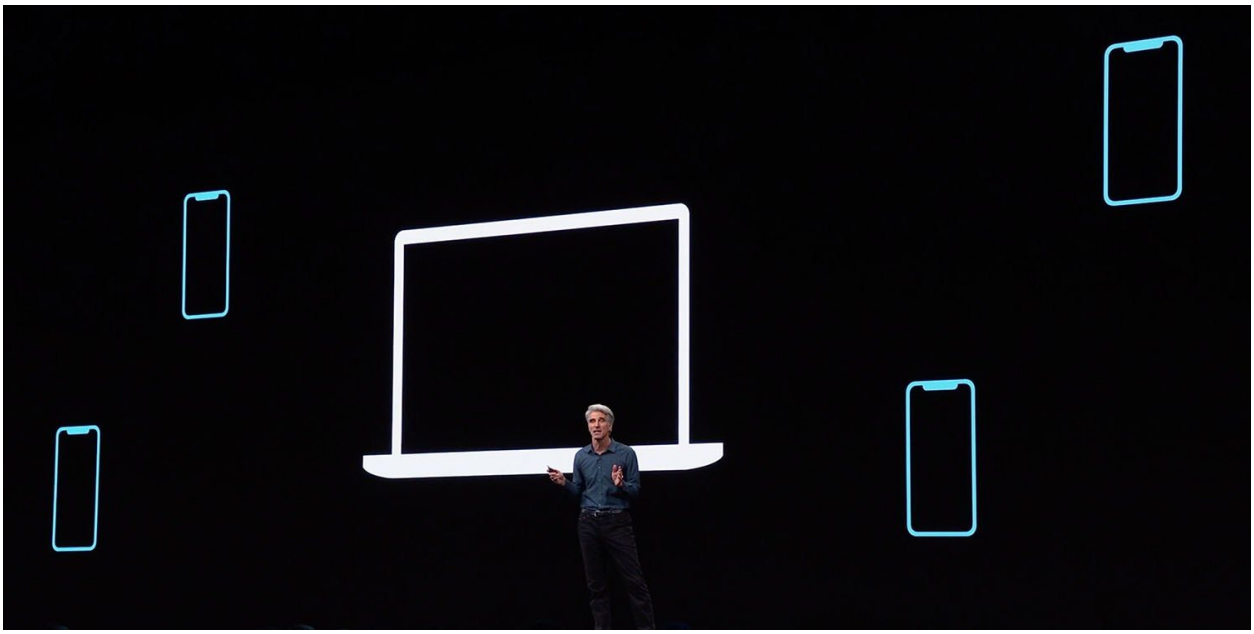
Apple details how offline location works in ‘Find My’ app, will require you own two Apple devices

Chance Miller
- Jun. 5th 2019 2:12 pm PT - 9to5Mac



One of the most intriguing changes in iOS 13 and macOS 10.15 is a merged Find My Friends and Find My iPhone application. The new app converts all of your Apple devices into Bluetooth beacons, enabling you to locate an offline device based on its proximity to any other Apple device. Now, Apple is offering up a bit more detail about the security features for the Find My application.

Here's how Apple describes offline location support in the new Find My app:

Locate a missing device even if it's not connected to Wi-Fi or cellular using crowd-sourced location. When you mark your device as missing and another Apple user's device is nearby, it can detect your device's Bluetooth signal and report its location to you. It's completely anonymous and encrypted end-to-end, so everyone's privacy is protected.

On stage at WWDC on Monday, Craig Federighi explained that the whole interaction involved in Find My's offline mode is "end-to-end encrypted and anonymous." Apple offered more details on the security aspect of the functionality to Wired this week.

One of the most interesting tidbits in the piece is that the find offline devices feature of iOS 13 requires that you own two Apple products. Essentially, that second Apple product is the one that holds the key to decrypt the location of an offline device:

Apple broke down that privacy element, explaining how its "encrypted and anonymous" system avoids leaking your location data willy nilly, even as your devices broadcast a Bluetooth signal explicitly designed to let you track your device.

The solution to that paradox, it turns out, is a trick that requires you to own at least two Apple devices. Each one emits a constantly changing key that nearby Apple devices use to encrypt and upload your geolocation data, such that only the

other Apple device you own possesses the key to decrypt those locations.

Furthermore, Find My's cryptography denies even Apple the ability to learn a user's location based on the Bluetooth beacon technology. This is actually an improvement over the Find My iPhone and Find My Friends individual applications.

Here's how the cryptography should work in the real world: *When you want to find your stolen laptop, you turn to your second Apple device—let's say an iPad—which contains both the same private key as the laptop and has generated the same series of rotating public keys. When you tap a button to find your laptop, the iPad uploads the same hash of the public key to Apple as an identifier, so that Apple can search through its millions upon millions of stored encrypted locations, and find the matching hash.*

The full Wired article is definitely worth a read.

original article:
https://9to5mac.com/2019/06/05/ios-13-macos-catalina-find-my/?utm_medium=40digest.7days3.20190605.carousel&utm_source=email&utm_content=&utm_campaign=campaign