IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

AVANT LOCATION TECHNOLOGIES LLC,	§	Case No.
Plaintiff,	§	**JURY TRIAL DEMANDED**
v.	§	
APPLE INC.,	§	
Defendant.	§	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Avant Location Technologies LLC ("ALT" or "Plaintiff") files this Complaint against Defendant Apple Inc. ("Apple" or "Defendant") for patent infringement under 35 U.S.C. § 271 and alleges as follows:

THE PARTIES

1. Plaintiff ALT is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business located at 104 E. Houston Street, Suite 140, Marshall, Texas 75670.

2. Defendant Apple is a corporation organized and existing under the laws of California. Apple is one of the leading smartwatch and mobile phone sellers in the United States and the world. Apple sells its products directly to consumers at physical Best Buy locations. There are multiple Best Buy locations in this District where Apple products are sold directly to customers, including at least: 823 North Creek Drive, Sherman, Texas 75092 (Grayson County), 2800 North Central Expressway, Plano, Texas 75074 (Collin County); 1751 North Central Expressway, Suite C, McKinney, Texas 75070 (Collin County); 3333 Preston Road, Suite 200, Frisco, Texas 75034 (Denton County); 5299 Eldorado Parkway, Frisco, Texas 75033 (Denton County); 1800 South

Loop 288, Suite 102 Building 1; Denton, Texas 76205 (Denton County); 6060 Long Prairie Road, Suite 500, Flower Mound, Texas 75028 (Denton County); 2601 South Stemmons Freeway, Suite 300, Lewisville, Texas 75067 (Denton County); 5885 East Freeway, Beaumont, Texas 77706 (Jefferson County); 8725 Memorial Boulevard, Port Arthur, Texas 77640 (Jefferson County); 869 NE Mall Boulevard, Hurst, Texas 76053 (Shelby County); 422 West Loop 281, Suite 100, Longview, Texas 75605 (Gregg County); 4210 Saint Michael Drive, Texarkana, Texas 75503 (Bowie County); 5514 South Broadway Avenue, Tyler, Texas 75703 (Smith County).[1]

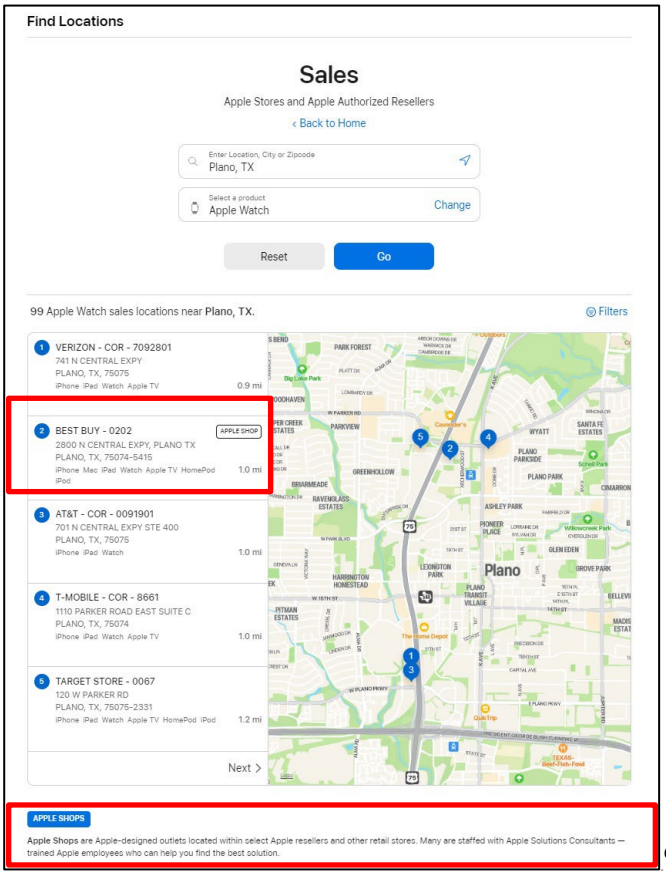
3. Further, certain Best Buy locations within this District contain Apple Shops. According to Apple's website, "Apple Shops are Apple-designed outlets located within select Apple resellers and other retail stores. Many are staffed with Apple Solutions Consultants—trained Apple employees who can help you find the best solution."[2] These Apple Solutions Consultants provide users and customers in this District with help connecting them with Apple products, find Apple products that meet their needs, and engage in the offer for sale of Apple's products from

[1] https://stores.bestbuy.com/tx/sherman/823-n-creek-dr-1023.html#shop;
https://stores.bestbuy.com/tx/plano/2800-n-central-expy-202.html;
https://stores.bestbuy.com/tx/frisco/3333-preston-rd-180.html;
https://stores.bestbuy.com/tx/frisco/5299-eldorado-pkwy-1773.html;
https://stores.bestbuy.com/tx/beaumont/5885-eastex-fwy-238.html;
https://stores.bestbuy.com/tx/denton/1800-s-loop-288-827.html;
https://stores.bestbuy.com/tx/flower-mound/6060-long-prairie-rd-1038.html;
https://stores.bestbuy.com/tx/lewisville/2601-s-stemmons-fwy-258.html;
https://stores.bestbuy.com/tx/longview/422-w-loop-281-594.html;
https://stores.bestbuy.com/tx/mckinney/1751-n-central-expy-196.html;
https://stores.bestbuy.com/tx/port-arthur/8725-memorial-blvd-1545.html;
https://stores.bestbuy.com/tx/texarkana/4210-saint-michael-dr-605.html;
https://stores.bestbuy.com/tx/tyler/5514-s-broadway-ave-246.html

[2] *See* https://locate.apple.com/sales?pt=6&lat=33.021827697753906&lon=-96.69925689697266&address=Plano%2C+TX

these locations.[3] Apple Solutions Consultants are employees of Apple and are provided training and resources by Apple.

4. Apple advertises on its website that the Best Buy located at 2800 North Central Expressway, Plano, Texas 75074-5415 (Collin County), contains an Apple Shop.[4] Apple further advertises on its website other Best Buy locations within this District that contain Apple Shops, including the store located at 190 East Stacy Road, Allen, Texas 75002-8734 (Collin County).[5]



[6]

[3] *See, e.g.*, https://www.linkedin.com/in/kyle-sailer-854770172 ("With my current role as an Apple Solutions Consultant, I help discover customers needs and help connect them with the latest products from Apple. I educate, train, and influence a team of partner employees. I focus on the sales, operations, and merchandising of the store's Apple shop/business.").
[4] *See* https://locate.apple.com/sales?pt=6&lat=33.021827697753906&lon=-96.69925689697266&address=Plano%2C+TX
[5] *Id.*
[6] https://locate.apple.com/sales?pt=6&lat=33.021827697753906&lon=-96.69925689697266&address=Plano%2C+TX

5. Best Buy also advertises on its website that the location in Plano, Texas, is an Apple Shop and that an Apple Shop is also located at the store in Allen, Texas.[7] The advertisement uses the Apple logo and touts that the Apple Shop sells "all things Apple," including popular Apple products, such as the Mac, iPad and iPhone.

[8]

6. These Apple Shops, located within Best Buy locations, are distinct from other areas within Best Buy locations. Similar to Apple Stores, Apple Shops prominently display Apple's logos and include sleek furniture and display fixtures. On information and belief, only Apple products are displayed within Apple Shops; products from other manufacturers may not be displayed within the Apple Shops.

7. Apple Shops are places of business of Apple. On information and belief, Apple exercises control over Apple Shops by: (1) dictating the look and feel of Apple Shops, including the furniture, display fixtures, and branding; (2) permitting only Apple products to be sold in Apple Shops; (3) requiring that Apple employees be permitted to regularly staff Apple Shops to assist in

[7] https://stores.bestbuy.com/tx/allen/190-e-stacy-rd-1780.html
[8] https://stores.bestbuy.com/tx/plano/2800-n-central-expy-202.html

sales and customer support. Apple conducts its business in Apple Shops by offering for sale and selling Apple products and by providing support for Apple products and customers.

8. Further, certain Best Buy locations, including those located in this District, are "Apple Authorized Service Providers."[9] The "Geek Squad Agents" at Best Buy locations are "Apple-trained and use genuine Apple parts on every repair."[10]

We are an Apple Authorized Service Provider.

Our Agents are Apple-trained, so you can trust us with all your Apple devices, no matter where you bought them.

[11]

Authorized Service Provider

We're an Apple Authorized Service Provider.

Guaranteed low price. Same-day services.

Our Geek Squad® Agents are Apple-trained and use genuine Apple parts on every repair.

[12]

[9] https://www.bestbuy.com/site/services/apple-service-repair/pcmcat1554741516170.c?id=pcmcat1554741516170
[10] *Id.*
[11] https://www.bestbuy.com/site/apple-service-repair/apple-watch-service-repair/pcmcat1554832617549.c?id=pcmcat1554832617549
[12] https://www.bestbuy.com/site/services/apple-service-repair/pcmcat1554741516170.c?id=pcmcat1554741516170

As an Apple Authorized Service Provider, we can repair many devices.

Devices we repair.

iPhone repair.
We can repair iPhone 15 Pro Max, iPhone 15 Pro, iPhone 15 Plus, iPhone 15, iPhone 14 Pro Max, iPhone 14 Pro, iPhone 14 Plus, iPhone 14, iPhone 13 Pro Max, iPhone 13 Pro, iPhone 13, iPhone 13 mini, iPhone 12 Pro Max, iPhone 12 Pro, iPhone 12, iPhone 12 mini, iPhone 11 Pro Max, iPhone 11 Pro, iPhone 11, iPhone XR, iPhone XS Max, iPhone XS, iPhone X, iPhone 8 Plus, iPhone 8, iPhone 7 Plus, iPhone 7, iPhone SE, iPhone 6s Plus, iPhone 6s, iPhone 6 Plus, iPhone 6, iPhone 5s, iPhone 5c, and iPhone 5, including iPhone screen repair.

Mac repair.
We can repair MacBook, MacBook Pro, MacBook Air and iMac.

Apple Watch repair.
We can repair Apple Watch and Apple Watch Sport, including watch screen repair.

iPad repair.
We can repair 9.7-inch iPad Pro, 12.9-inch iPad Pro, iPad Air 2, iPad Air, iPad mini 2, iPad mini 4 and more.

iPod repair.
We can repair iPod touch, iPod nano and iPod shuffle.

HomePod repair.
We can repair all HomePod speakers.

Apple TV repair.
We can repair Apple TV (4th generation) and Apple TV (3rd generation).

Repairs we perform.

- Fixing cracked screens and screen replacement
- General repairs
- Display issues
- Software issues
- Speaker replacement/audio issues
- Power/charging/battery issues
- Camera replacement
- Receiver/microphone replacement
- Vibe motor replacement
- Battery replacement
- Operating system upgrades
- Wi-Fi troubleshooting

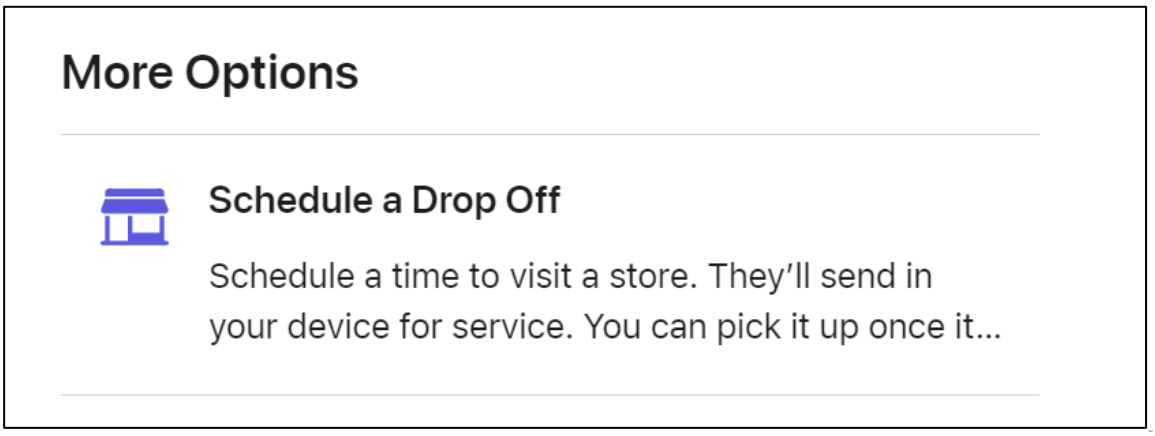
Screen replacement.
Cracked iPhone screen? We can repair your damaged screen and have your iPhone back the same day.* We use genuine Apple parts to deliver Apple-certified repairs that are backed by Apple, so you'll get your iPhone back and working exactly the way it should. Same-day service is available for iPhone 6s or newer models.

[13]

Apple touted the expansion of its "Apple authorized service network" at "nearly 1,000 Best Buy stores across the U.S. now providing expert service and repairs for Apple products."[14] Further, Apple states that "Apple-certified repairs at an Apple store or an authorized service provider are

[13] https://www.bestbuy.com/site/services/apple-service-repair/pcmcat1554741516170.c?id=pcmcat1554741516170
[14] https://www.apple.com/newsroom/2019/06/apple-partners-with-best-buy-for-expanded-repair-service/

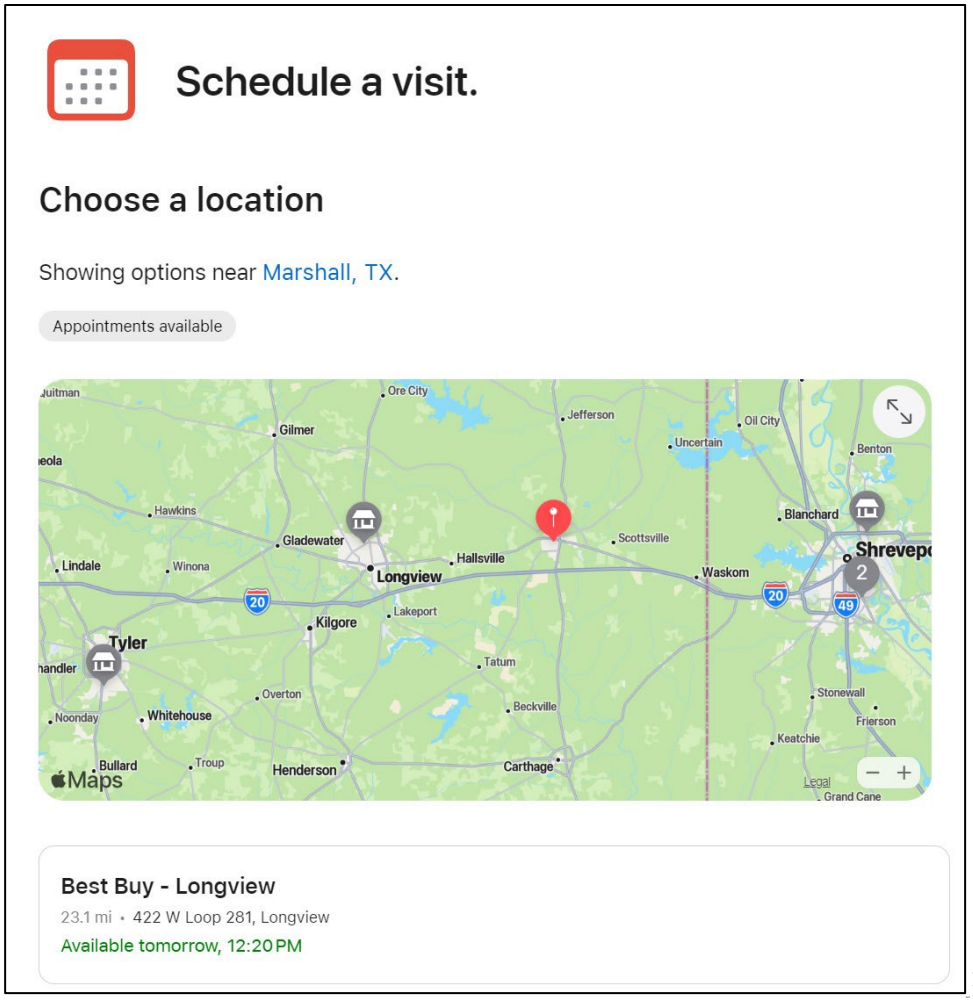
performed by trained experts who use genuine Apple parts. Every repair is backed by Apple."[15] When a customer or user seeks to schedule a repair from Apple's website, Apple directs its users to Best Buy locations within this District.



[16]

[15] *Id.*

[16] https://getsupport.apple.com/solutions



[17]

Apple advertises on its website these Best Buy locations as Apple Authorized Service Providers as certified "so you get the same professionalism and quality of repair you'd expect from Apple."[18]

JURISDICTION

9. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1, *et seq*. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1332, 1338, and 1367.

[17] *Id.*

[18] https://getsupport.apple.com/solutions/schedule-repair/providers

10. This Court has specific and personal jurisdiction over the Defendant consistent with the requirements of the Due Process Clause of the United States Constitution and the Texas Long Arm Statute. Upon information and belief, the Defendant has sufficient minimum contacts with the forum because Defendant transacts substantial business in the State of Texas and in this Judicial District. Further, Defendant has, directly or through subsidiaries or intermediaries, committed and continues to commit acts of patent infringement in the State of Texas and in this Judicial District as alleged in this Complaint, as alleged more particularly below.

11. Venue is proper in this Judicial District pursuant to 28 U.S.C. §§ 1400(b) and 1391(b) and (c) because Defendant is subject to personal jurisdiction in this Judicial District, has committed acts of patent infringement in this Judicial District, and has a regular and established place of business in this Judicial District, including Apple Shops located in BestBuy stores in this Judicial District. Defendant, through its own acts, makes, uses, sells, offers to sell, and/or imports infringing products within this Judicial District, regularly does and solicits business in this Judicial District, and has the requisite minimum contacts with this Judicial District, such that this venue is a fair and reasonable one.

PATENTS-IN-SUIT

12. On May 27, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,738,040 (the "'040 Patent") entitled "Method and System for Monitoring a Mobile Station Presence in a Special Area." A true and correct copy of the '040 Patent is attached as Exhibit 1.

13. On June 26, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,009,720 (the "'720 Patent") entitled "Method and System for Monitoring a Mobile Station Presence in a Special Area." A true and correct copy of the '720 Patent is attached

as Exhibit 2.

14. On May 26, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,042,910 (the "'910 Patent") entitled "Method and System for Monitoring a Mobile Station Presence in a Special Area." A true and correct copy of the '910 Patent is attached as Exhibit 3.

15. On January 13, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,934,922 (the "'922 Patent") entitled "Method and System for Monitoring a Mobile Station Presence in a Special Area." A true and correct copy of the '910 Patent is attached as Exhibit 4.

16. On August 25, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,119,030 (the "'030 Patent") entitled "Method and System for Monitoring a Mobile Station Presence in a Special Area." A true and correct copy of the '030 Patent is attached as Exhibit 5.

17. On November 1, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,485,621 (the "'621 Patent") entitled "Method and System for Monitoring a Mobile Station Presence in a Special Area." A true and correct copy of the '621 Patent is attached as Exhibit 6.

18. On April 11, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,622,032 (the "'032 Patent") entitled "Method and System for Monitoring a Mobile Station Presence in a Special Area." A true and correct copy of the '032 Patent is attached as Exhibit 7.

19. ALT is the sole and exclusive owner of all right, title, and interest to and in the '040, '720, '910, '922, '030, '621, and '032 Patents (collectively, the "Patents-in-Suit"), and holds

the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. ALT also has the right to recover all damages for past infringement of the Patents-in-Suit as appropriate under the law.

20. ALT has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the Patents-in-Suit.

FACTUAL ALLEGATIONS

21. The Patents-in-Suit generally cover systems and methods for providing flexibility to mobile telephone networks by associating these networks with new special areas securely and without the need to modify any radio transmitting device.

22. The ’040 Patent generally relates to a method for monitoring a mobile station presence in a special area, and to a mobile system, a server, a radio transmitting device, and a mobile station suitable for carrying out such a method. The inventions described in the ’040 Patent were developed by Carlos A. Perez LaFuente of Afirma Consulting & Technologies, S.L.

23. The ’720 Patent generally relates to a method for monitoring a mobile station presence in a special area, and to a mobile system, a server, a radio transmitting device, and a mobile station suitable for carrying out such a method. The inventions described in the ’720 Patent were developed by Carlos A. Perez LaFuente of Afirma Consulting & Technologies, S.L.

24. The ’910 Patent generally relates to a method for monitoring a mobile station presence in a special area, and to a mobile system, a server, a radio transmitting device, and a mobile station suitable for carrying out such a method. The inventions described in the ’910 Patent were developed by Carlos A. Perez LaFuente of Afirma Consulting & Technologies, S.L.

25. The ’922 Patent generally relates to a method for monitoring a mobile station presence in a special area, and to a mobile system, a server, a radio transmitting device, and a

mobile station suitable for carrying out such a method. The inventions described in the ’922 Patent were developed by Carlos A. Perez LaFuente of Afirma Consulting & Technologies, S.L.

26. The ’030 Patent generally relates to a method for monitoring a mobile station presence in a special area, and to a mobile system, a server, a radio transmitting device, and a mobile station suitable for carrying out such a method. The inventions described in the ’030 Patent were developed by Carlos A. Perez LaFuente of Afirma Consulting & Technologies, S.L.

27. The ’621 Patent generally relates to a method for monitoring a mobile station presence in a special area, and to a mobile system, a server, a radio transmitting device, and a mobile station suitable for carrying out such a method. The inventions described in the ’621 Patent were developed by Carlos A. Perez LaFuente of Afirma Consulting & Technologies, S.L.

28. The ’032 Patent generally relates to a method for monitoring a mobile station presence in a special area, and to a mobile system, a server, a radio transmitting device, and a mobile station suitable for carrying out such a method. The inventions described in the ’032 Patent were developed by Carlos A. Perez LaFuente of Afirma Consulting & Technologies, S.L.

29. Defendant has infringed and continues to infringe the Patents-in-Suit by making, using, selling, offering to sell, and/or importing, and by actively inducing others to make, use, sell, offer to sell, and/or import products, including mobile phones and tablets that implement the technology claimed by the Patents-in-Suit. For example, the Accused Products are Apple products that implement Find My, which include, but are not limited to, iPhone, iPad, iPod Touch, Apple Watch, Mac, AirPods, AirTag, Apple Pencil, and Apple Vision Pro. Exhibit 8, https://www.apple.com/icloud/find-my/. The Find My feature has been available on the Accused Products as of 2019. Exhibit 9, https://apple.fandom.com/wiki/Find_My#:~:text=Find%20My%20is%20an%20app,and%20mac

OS%20Catalina%20(10.15). The Accused Products also include Apple products that implement or work with the Home App, which include, but are not limited to iPhone, iPad, HomePod, HomePod Mini, and Apple TVs. Exhibit 10, https://www.apple.com/home-app/.

30. Defendant has had actual notice of the Asserted Patents, at least as of the filing date of this Complaint.

31. ALT has, at all times, complied with the marking provisions of 35 U.S.C. § 287 with respect to the Asserted Patents.

COUNT I
(Infringement of the '040 Patent)

32. Paragraphs 1 through 31 are incorporated by reference as if fully set forth herein.

33. ALT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '040 Patent.

34. Defendant has and continues to directly infringe the claims of the '040 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, at least by making, using, offering to sell, selling, and/or importing into the United States products, such as the Accused Products, that satisfy each and every limitation of one or more claims of the '040 Patent, and by performing each and every limitation of one or more method claims of the '040 Patent.

35. The Accused Products each comprise the system of at least claim 13 of the '040 Patent: A mobile station, comprising: observing means to observe a channel and process any received signal in order to determine whether or not it is receiving a defining signal, a processor to process any received defining signal and to determine, based on a previously obtained checking data, whether or not the defining signal received is a distinctive defining signal that at least partially defines a special area, to determine whether or not it is present in one or more special areas, and

to send an updating signal at least one of (i) periodically, (ii) when the mobile station enters into or exits from one of the special areas, and (iii) when the mobile station remains into a special area to a mobile telephone network about its presence in one or more of the special areas, where said updating signal sending is uncorrelated to any mobile station phone call establishment and is based on the last determination performed by the mobile station about its presence in the special areas.

36. The Accused Products comprise an observing means to observe a channel and process any received signal in order to determine whether or not it is receiving a defining signal. For example, the Find My service includes the use of a mobile station that comprises observing means to observe a Bluetooth channel related to the offline finding service and process any received signal in order to determine whether or not it is receiving an offline finding service defining signal. Within the Find My service, a missing Bluetooth device that is part of the Find My network for offline finding transmits a BLE advertisement indicative that it is in an offline status (*i.e.*, it is lost). The mobile station observes a BLE channel corresponding to the offline finding service signals transmission and process any received signal to determine whether or not it is receiving an offline finding service defining signal that comprises an offline finding service identifier.

The Find My app makes it easy to keep track of your Apple devices — even if they're offline. You can also locate items using AirTag or Find My technology. Or pinpoint friends and family with Precision Finding. Everyone's location stays private every step of the way.

Find your stuff on iCloud.com ↗

Exhibit 8, available at https://www.apple.com/icloud/find-my/

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, available at https://www.apple.com/icloud/find-my/

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

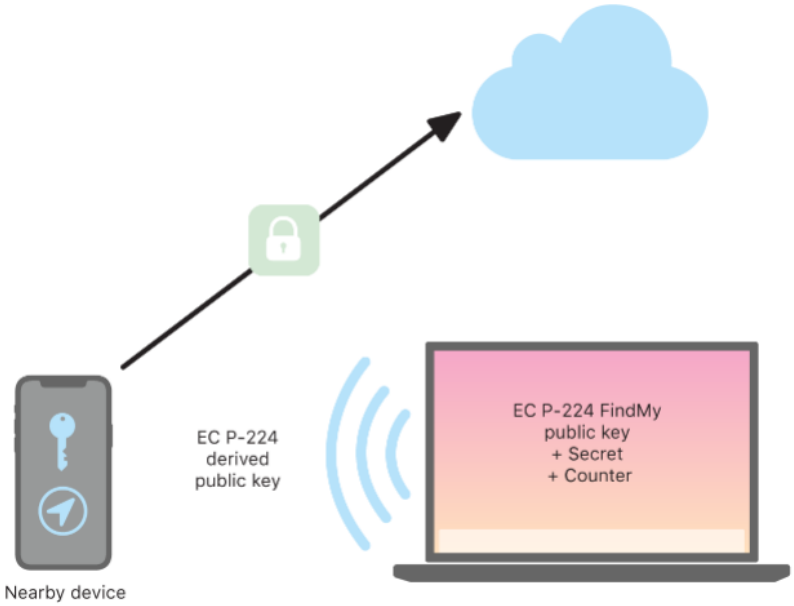


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

Find My security

The Find My app for Apple devices is built on a foundation of advanced public key cryptography.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

37. For example, within Find My, a user may register their Apple devices, such that they may keep them located when they are nearby, by using the Find My App. As illustrated below, Find My also provides an "offline finding" mode wherein users' lost Apple devices (iPhones, iPads, Macs, Apple Watches, AirPods, Apple Pencil, and Apple Vision Pro) that are registered within the Find My network for offline finding can be found with the help of devices (*e.g.*, iPhones, iPads, Macs) that observe a BLE channel wherein offline finding service signals are transmitted and processes the received signals. For example, the mobile station is an iPhone registered within the Find My servings and helps to find a missing Apple device that is offline and is part of the Find My network. The missing Apple device that is offline and is part of the Find My network for

offline finding is the radio communication defining device transmitting the distinctive defining signal.

Find My security

The Find My app for Apple devices is built on a foundation of advanced public key cryptography.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, available at https://www.apple.com/icloud/find-my/

38. For example, if an Apple device that is part of the Find My network for offline finding (*i.e.*, a radio communication defining device) has gone offline, it starts emitting a Bluetooth Low Energy signal (*i.e.*, a distinctive defining signal) that can then be picked up by any Apple device that is part of the Find My network for offline finding.

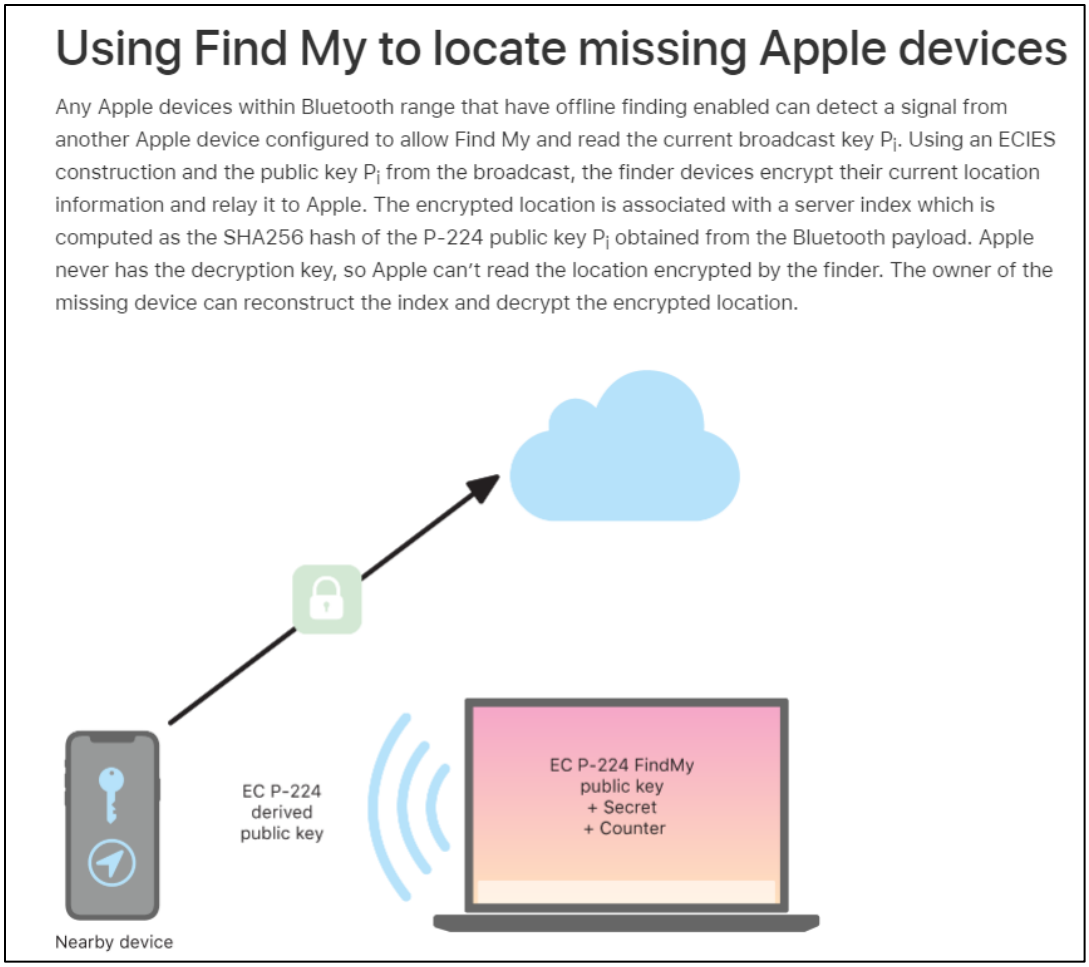


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

39. For example, the following table summarizes the key features of BLE signals. The mobile station receives BLE advertisement from lost Apple devices that are in range.

Table 2. OF advertisement format (with zero-indexed bytes).

Bytes	Content (details cf. [6, § 5.1])
0–5	BLE address $((p_i[0] \mid (0b11 \ll 6)) \mid\mid p_i[1..5])$
6	Payload length in bytes (30)
7	Advertisement type (0xFF for manufacturer-specific data)
8–9	Company ID (0x004C)
10	OF type (0x12)
11	OF data length in bytes (25)
12	Status (e.g., battery level)
13–34	Public key bytes $p_i[6..27]$
35	Public key bits $p_i[0] \gg 6$
36	Hint (0x00 on iOS reports)

Exhibit 13, available at https://arxiv.org/pdf/2103.02282

40. For example, the Apple Find My offline finding service involves the use of a mobile station (a *finder* device) and a BLE radio communication defining device (a *lost* device) that transmits a BLE distinctive defining signal (a BLE advertisement).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF

Exhibit 13, at 1, Introduction.

41. For example, a lost device emits a BLE advertisement indicative of the offline finding service (*i.e.*, a BLE advertisement containing a public key). This signal is a Bluetooth distinctive defining signal transmitted by the radio communication defining device (*i.e.*, transmitted by the lost Apple mobile station in this example). The distinctive defining signal also comprises an identifier of the lost device (*i.e.*, the public key).

6 Apple Offline Finding in Detail

This section describes and discusses the technical details of Apple's OF system. In reference to Fig. 1, we (1) explain the involved cryptography and the key exchange during initial device pairing, and then explain the protocols implementing (2) *losing*, (3) *finding*, (4) *searching* for devices.

In short, devices and accessories in lost mode send out BLE advertisements containing a public key. Finder devices receive them, encrypt their location by using the public key, and upload a report to Apple's servers. This results in an end-to-end encrypted location report that cannot be read by Apple or any other third-party that does not have access to the owner's private keys.

Exhibit 13, at 5, § 6.

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

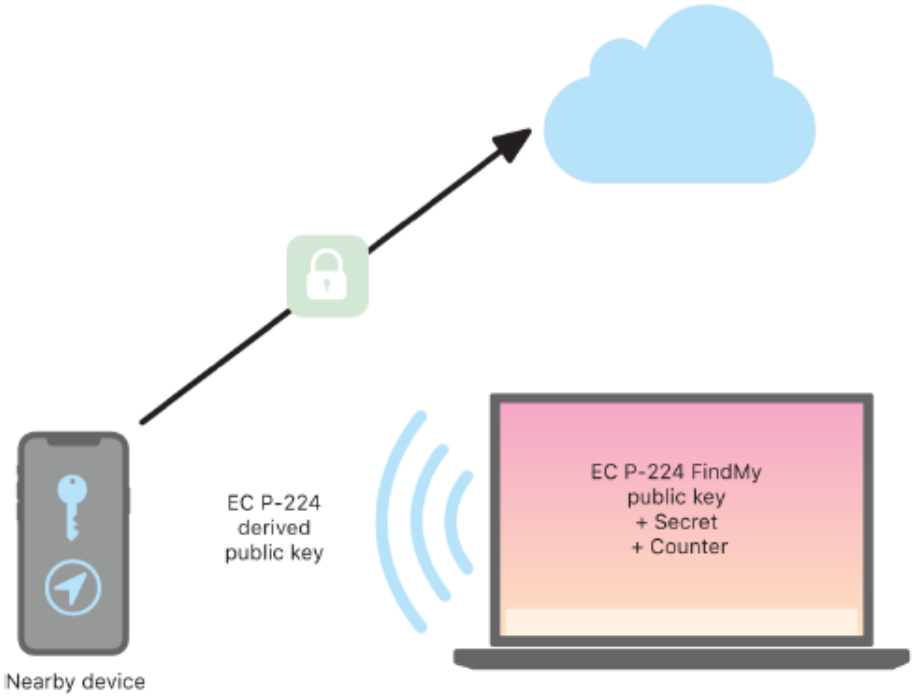


Exhibit 11, https://support.apple.com/en-au/guide/security/sece994d0126/web

42. For example, the mobile station observes a channel corresponding to the offline finding service BLE advertisements and processes any received signal to determine whether or not it is receiving an offline finding service defining signal that comprises an offline finding service identifier. If the signal comprises an offline finding service identifier, at that point it is a defining signal for the mobile station.

Table 2. OF advertisement format (with zero-indexed bytes).

Bytes	Content (details cf. [6, § 5.1])
0–5	BLE address $((p_1[0] \mid (0b11 \ll 6)) \mid\mid p_1[1..5])$
6	Payload length in bytes (30)
7	Advertisement type (0xFF for manufacturer-specific data)
8–9	Company ID (0x004C)
10	OF type (0x12)
11	OF data length in bytes (25)
12	Status (e.g., battery level)
13–34	Public key bytes $p_1[6..27]$
35	Public key bits $p_1[0] \gg 6$
36	Hint (0x00 on iOS reports)

Exhibit 13, at 6.

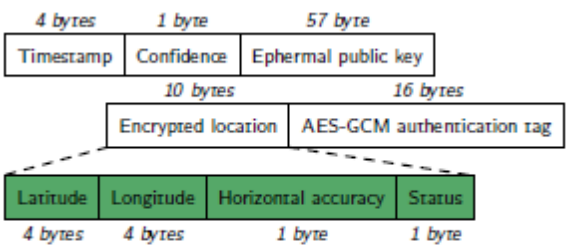


Fig. 2. Binary format of a location report.

Id., at 7.

43. The Accused Products comprise a processor to process any received defining signal and to determine, based on a previously obtained checking data, whether or not the defining signal received is a distinctive defining signal that at least partially defines a special area, to determine whether or not it is present in one or more special areas. For example, a processor within the mobile station processes any received defining signal and uses data previously stored in the mobile station (*i.e.*, checking data), to determine whether or not the BLE defining signal received is a distinctive defining signal that at least partially defines the offline finding service special area. If the mobile station determines that it is receiving a distinctive defining signal, it consequently identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it, as detailed below). Within Find My, every Apple device enabled for "offline finding" is

converted into a receiver and locator, which effectively crowdsources the search of a missing device. Any device registered within Find My for "offline finding" becomes a Find Node of the Find My network and may receive and process the offline finding BLE defining signals from lost Apple devices.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1.

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, available at https://www.apple.com/icloud/find-my/

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

44. For example, the special area can be defined by the area covered by the Bluetooth distinctive defining signals of all the radio communication defining devices that are part of the Find My network for offline finding and are in an offline status at a given time. So, the special area is a dynamic-crowdsourced special area. The area covered by a given Bluetooth distinctive defining signal from a lost radio communication defining device that is in an offline status at least partly defines the special area. As shown below, a user can register various Apple devices for offline finding. The user can locate the devices by using the Find My map.

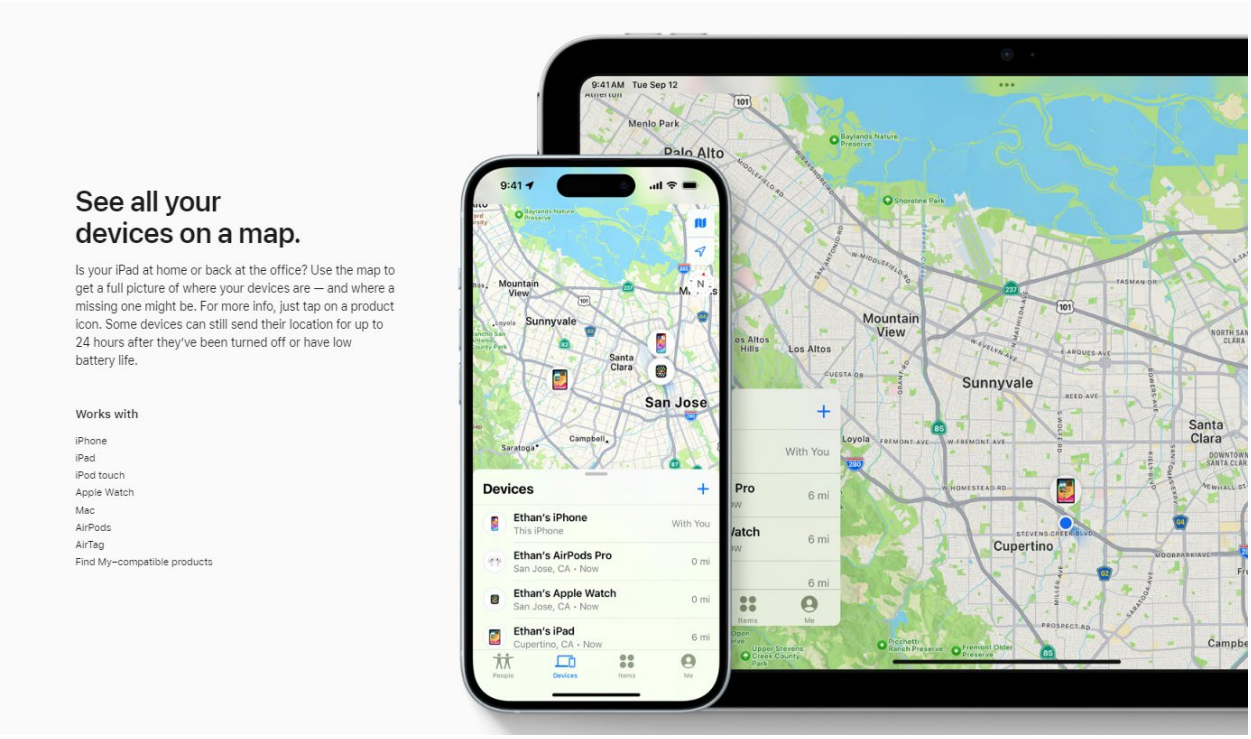


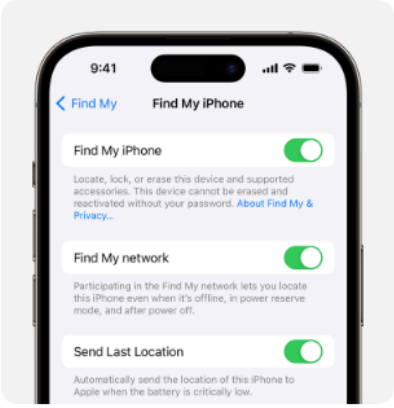
Exhibit 8, available at https://www.apple.com/icloud/find-my/

Set up Find My on your iPhone, iPad, or Mac

Set up Find My so that you can locate a lost device or item — such as your paired AirPods, Apple Watch, or a personal item with an AirTag attached.

How to turn on Find My for your iPhone or iPad

1. Open the Settings app.
2. Tap your name, then tap Find My.
3. If you want friends and family to know where you are, turn on Share My Location.
4. Tap Find My [device], then turn on Find My [device].



5. To see your device even when it's offline, turn on Find My network.*
   - To have the location of your device sent to Apple when the battery is low, turn on Send Last Location.

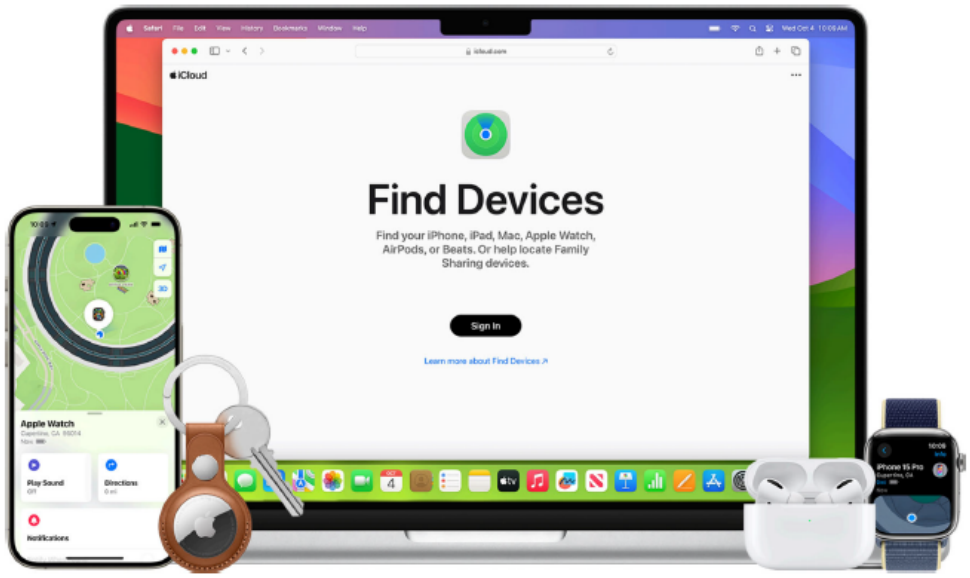
If you want to be able to find your lost device on a map, make sure that Location Services is turned on. To do this, go to Settings > Privacy & Security > Location Services, and turn on Location Services.

* The Find My network is an encrypted, anonymous network of hundreds of millions of Apple devices that can help you locate your device.

Exhibit 14, available at https://support.apple.com/en-us/102648

Find your lost Apple device or AirTag with Find My

If you lose your Apple device, personal item connected to an AirTag, or other Find My network accessory, use Find My to find it or mark it as lost to protect your device and personal information.



Find your stuff with Find My

If you've lost or misplaced an Apple device or personal item with an AirTag attached, use Find My to find your device or item on a map. You can get directions to its location and, when you're nearby, play a sound or even get help finding its exact location.

Exhibit 15, available at https://support.apple.com/en-us/104978

45. For example, a processor helps the mobile station in determining whether or not a received defining signal is a distinctive defining signal that at least partly defines a special area and whether or not the mobile station is present in the offline finding service special area. The result of the BLE advertisement scan by the mobile station that parses a "public key" from the advertisement allows the mobile station to determine that a received advertisement signal is distinctive through its unique key. The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station

obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **Finder devices.** Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Exhibit 13, at 3, § 3.

46. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal based on receiving a packet in the OF advertisement format) the mobile station must necessarily store data related to the OF advertisement (*i.e.*, store previous obtained checking data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **6.3 Finding**
>
> All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.
>
> **Generating Reports.** The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

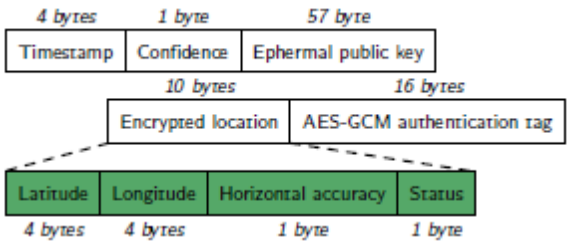


Fig. 2. Binary format of a location report.

ing the algorithm described in § 6.1. Finally, the finder creates a complete location report, including the current timestamp (in seconds since January 1, 2001), the ephemeral public key d', the encrypted message, and the AES-GCM authentication tag as shown in Fig. 2.

Exhibit 13, at 6-7, § 6.3.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0FBAE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Id., at 7, § 6.3.

47. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal with the OF advertisement), the mobile station must necessarily store data related to the location report (*i.e.*, store previous obtained checking data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station sends to a mobile telephone network, and the network routes to the Apple servers (Apple is a provider of presence-related services), a signal that identifies that the mobile station is nearby the missing device that is part of the Find My network (*i.e.*, it is present in the special area). Further, when nearby the lost radio communication defining device, the mobile station receives the distinctive defining signal. The mobile station is able to identify that the received defining signal is distinctive and to determine that it is present within the crowdsourced offline finding special area, as detailed above. The BLE distinctive signal must include a device identifier, such that the Find My services related to the found device can be later provided in connection to that device, as elaborated below.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

48. The Accused Products comprise a processor to send an updating signal at least one of (i) periodically, (ii) when the mobile station enters into or exits from one of the special areas, and (iii) when the mobile station remains in a special area to a mobile telephone network about its presence in one or more of the special areas. For example, as a result of the mobile station identifying that it is present in the crowdsourced special area the mobile station sends (encrypted and securely protected) a signal about the mobile station's presence in the special area to a mobile telephone network, and the mobile telephone network routes the presence updating signal to the Apple servers (Apple is the provider of Find My "offline finding" presence related services), the signal including the mobile station location, as detailed in the image above. Further, in connection to the sending of the presence updating signal to a mobile telephone network, it shall be noted that

the mobile station is not typically placed at the user's home when receiving the distinctive defining signal from a lost device, but in a public environment. So, in those scenarios the mobile station is usually not connected to the network via Wi-Fi but through mobile telephony communications (*i.e.*, the updating signal is sent to a mobile telephone network and further routed to the Apple iCloud servers). The presence signal must also include the device identifier, as it is required by iCloud to subsequently provide related presence related services (*e.g.*, the above-referred notification about the device location). The images below indicate that once a mobile station has identified that it is nearby a lost device that is in an offline status, the location of the mobile station and the device identifier of the lost device are collected to provide the Find My service (this information is sent to the Apple servers within the updating signal, as it is required to allow the device owner to locate the device, once found by the mobile station).

> **Advertising Interval.** The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

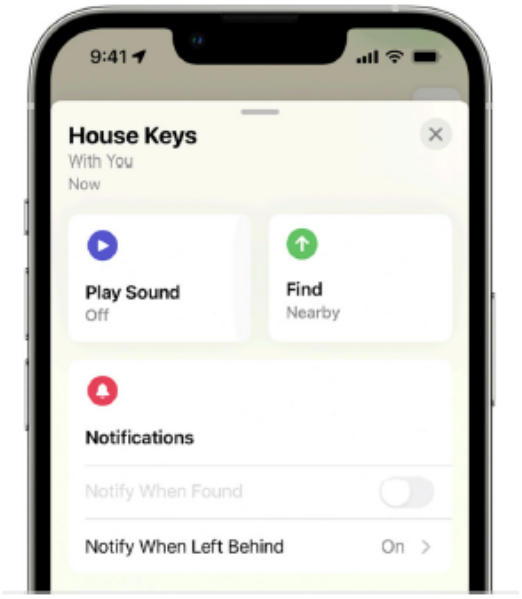
Exhibit 13, at 6, § 6.2.

> **Set up and use Notify When Left Behind in the Find My app**
>
> With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, available at https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

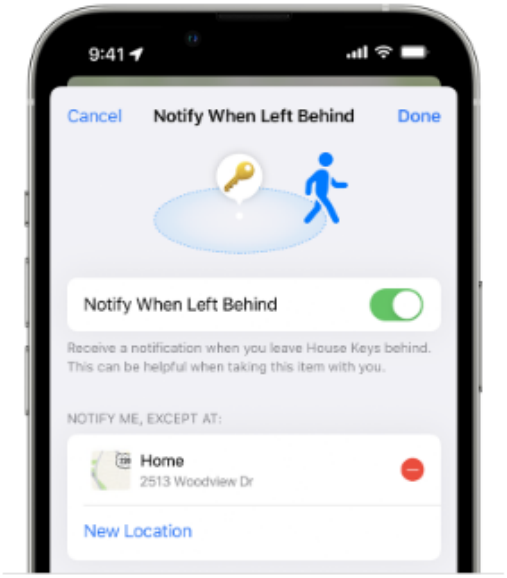
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Exhibit 16, available at https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

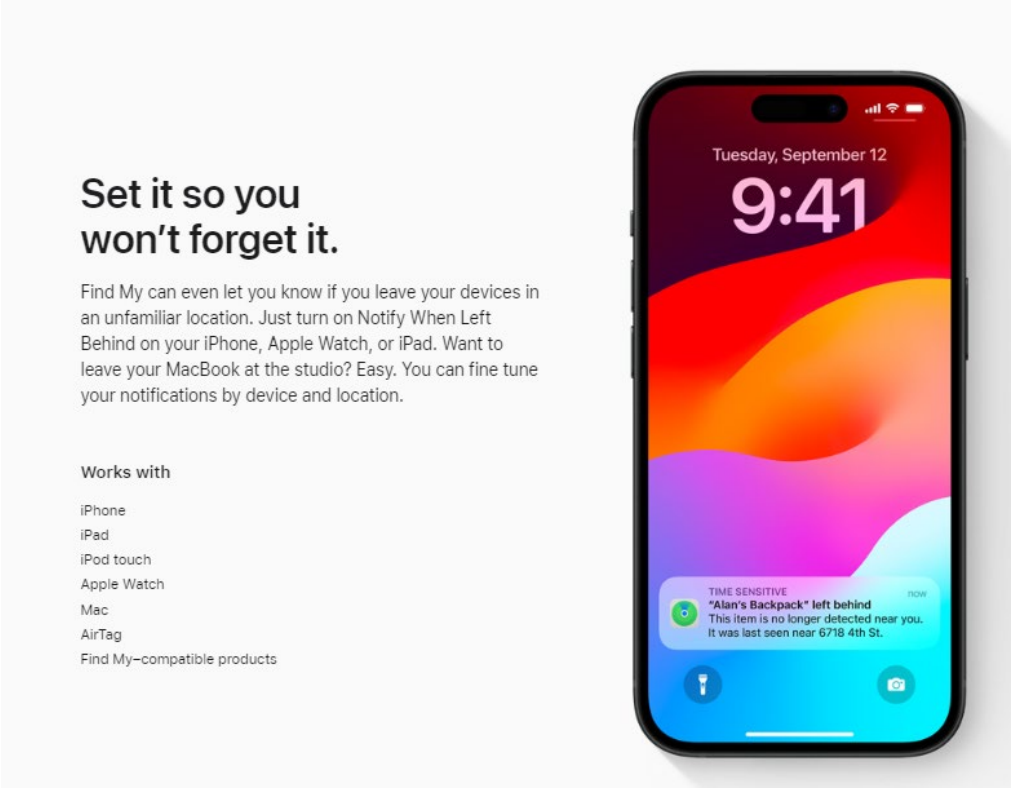
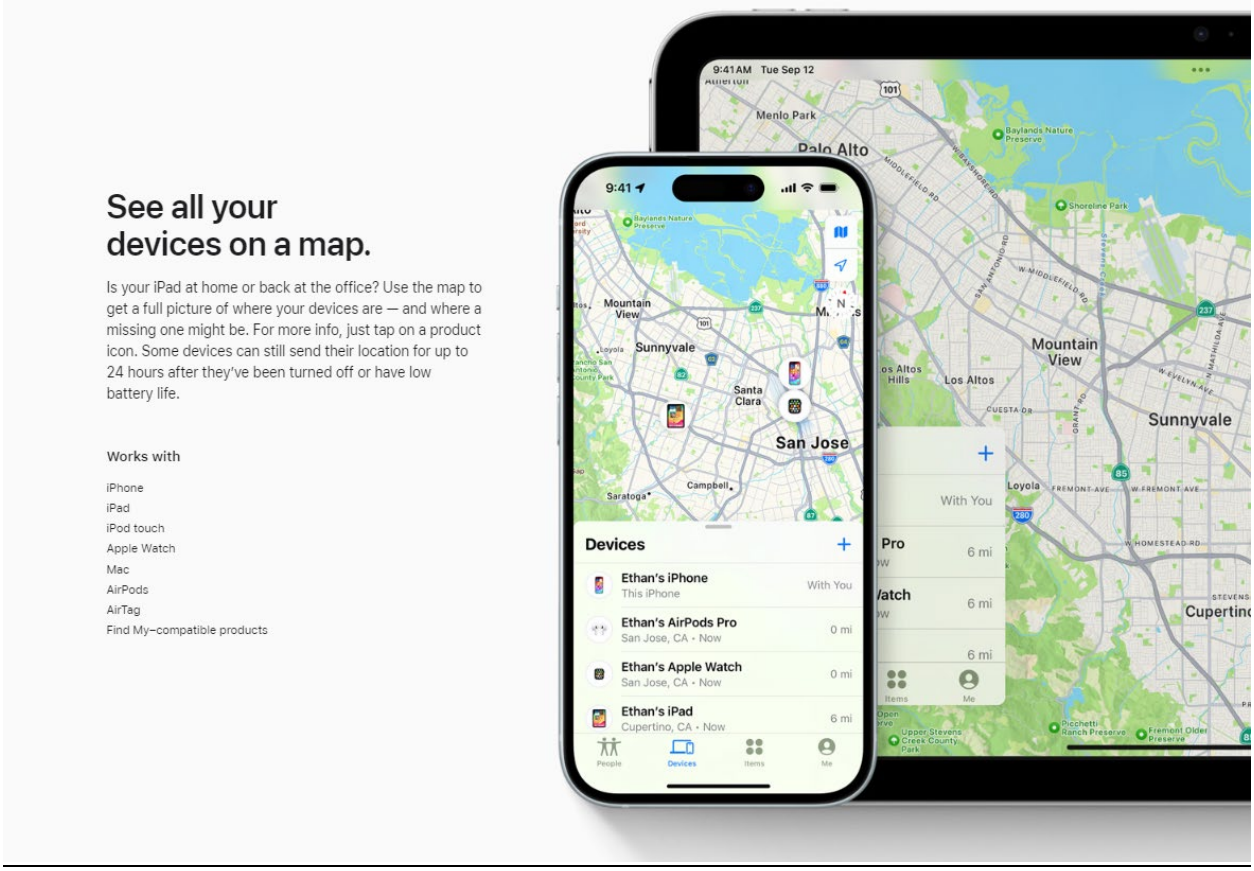
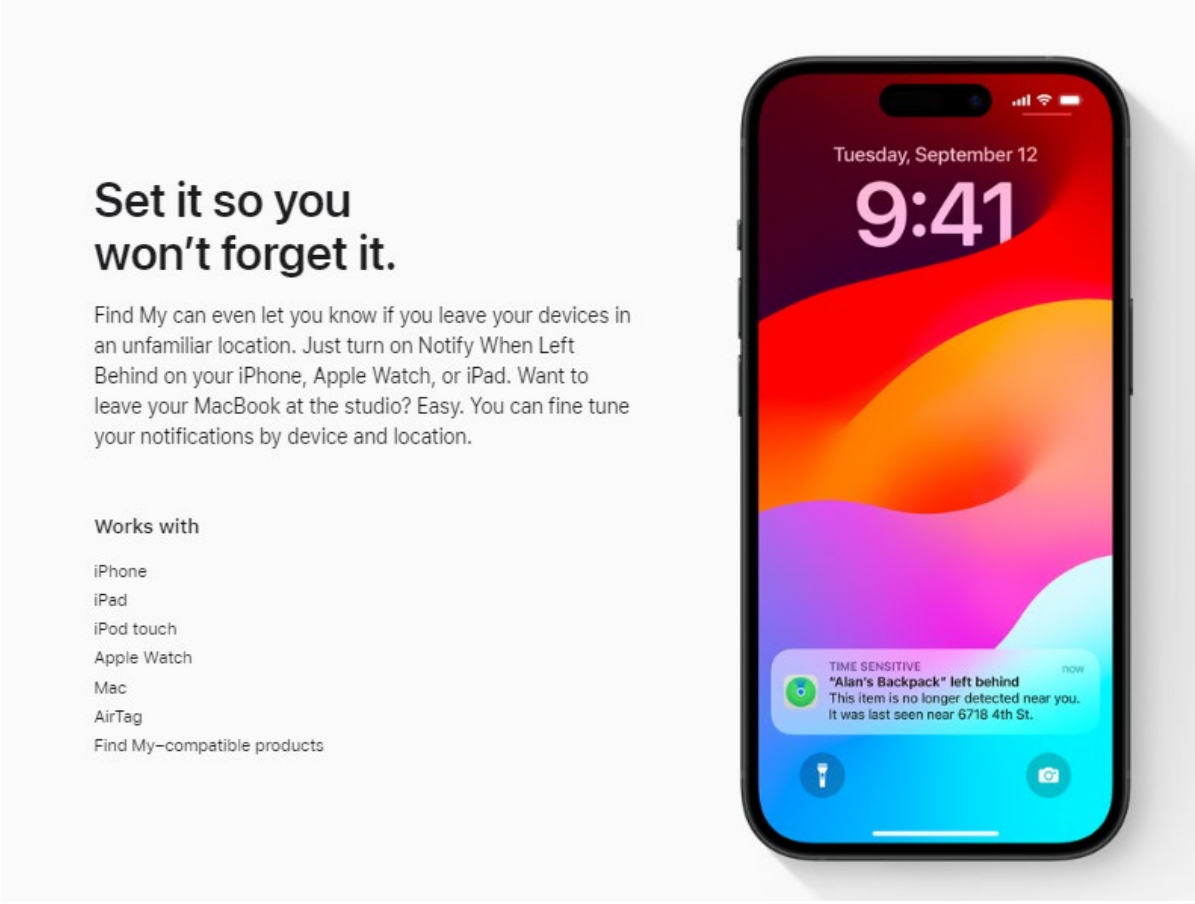


Exhibit 8, available at https://www.apple.com/icloud/find-my/

49. For example, the Apple iCloud servers (Apple is the provider of presence related services) receives the presence updating signal, routed from a mobile telephone network, and uses it to provide presence related services, *e.g.*, displaying the device location on a map or, *e.g.*, sending a notification to the owner that a device has been left behind (Notify When Left Behind).



Id., available at https://www.apple.com/icloud/find-my/



Id., available at https://www.apple.com/icloud/find-my/

50. For example, the mobile station sends a presence updating signal to the Apple iCloud servers (via the mobile telephone network). As shown below, a mobile station (a *finder* device) identifies that it is present within the area of coverage of a device that is lost and is part of the Find My offline finding network and sends to a vendor controller server (*i.e.*, to the Apple iCloud servers in the case of Apple devices and Apple Find My offline finding ecosystem) an updating signal indicative of the presence status (the signal including the unique beacon data received from the lost device via BLE, together with the location of the device).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Id., at 3, § 3.

6.3 Finding

All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.

Generating Reports. The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

Id., at 6, § 6.3.

51. For example, the updating signal is sent to a mobile telephone network, and then routed to the Apple iCloud servers, when the mobile station enters into the special area and starts receiving the distinctive defining signal from the lost radio communication defining device. Also, if the mobile station remains nearby the lost device (*i.e.*, remains into the special area) it periodically sends a presence updating signal to a mobile telephone network (that routes it the Apple iCloud servers), as further elaborated below. For example, the mobile station stores in a local database the last determination performed by the mobile station about its presence in the special area, in connection to the found device public key identifier. If there is more than one found device, each last presence determination is stored in the database in connection to the corresponding found device private ID identifier. After the storage, the mobile station stops scanning (*i.e.*, stops the presence determination stops) and sends a presence updating signal containing the (each) lost device private ID and the location to a mobile telephone network (then routes it to the Apple iCloud servers). If it is the first (recent) reporting by the mobile station about the mobile station presence in the special area, the presence updating signal is then related to the mobile station entering into the crowdsourced offline finding special area.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

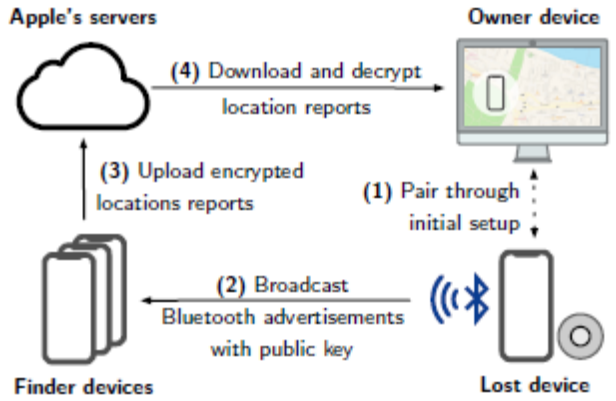


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

52. As another example, the mobile station receives an acknowledgment about the presence updating signal having been received in the Apple iCloud servers (via a mobile telephone network), as indicated in the image below. As also indicated in the image below, the presence determination process (*i.e.*, the scanning and filtering of OF advertisements in a certain format) is then reinitiated. If the mobile station remains in the special area in connection to a lost device it has already reported, then it may send (after 15 minutes) a new updating signal related to the mobile station presence in the special area (in connection to that lost device), *i.e.*, the presence updating signal is then related to the mobile station remaining into the crowdsourced offline finding special area.

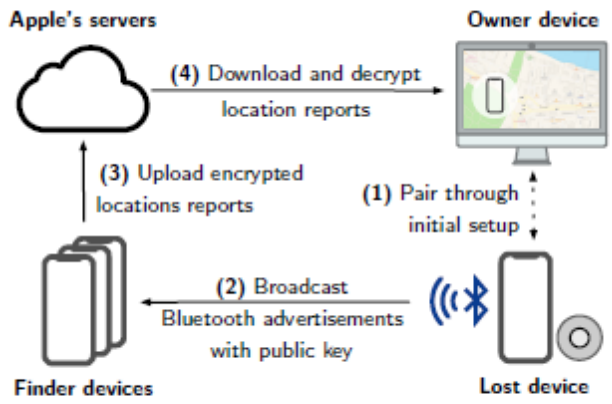


Fig. 1. Simplified offline finding (OF) workflow.

Exhibit 13, at 3, FIG. 1.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

53. For example, the mobile station stores in a local database the last determination performed by the mobile station about its presence in the special area, in connection to the found device public key. If there is more than one found device, each last presence determination is stored in the database in connection to the corresponding found device public key. After the storage, the mobile station sends a presence updating signal containing the recently found device(s) private ID(s) and the location to a mobile telephone network (then routes it to the Apple iCloud servers). If it is the first reporting by the mobile station about the mobile station presence in the special area, the presence updating signal is then related to the mobile station entering into the crowdsourced offline finding special area.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0F8AE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Exhibit 13, at 7, § 6.3.

54. The Accused Products comprise a processor to send an updating signal, where said updating signal sending is uncorrelated to any mobile station phone call establishment and is based on the last determination performed by the mobile station about its presence in the special areas. For example, the Apple device sends updating signals to the Apple servers, regardless of whether it is in range of Wi-Fi networks. Therefore, when out of range of Wi-Fi networks ,the device uses

the mobile network. Therefore, the updating signal is sent over a cellular data connection and is uncorrelated to any mobile station phone call establishment. The updating signal sending is based on the last determination performed by the mobile station about its presence in the crowdsourced offline finding special area. As already indicated above, the mobile station stores in a local database the last determination performed by the mobile station about its presence in the special area, in connection to the (each) found public key. After the storage, the mobile station stops the scanning (*i.e.*, the presence determination stops) and sends a presence updating signal that uses the information into the referred local database, *i.e.*, the information about said last presence determination.

Locating devices that are offline

If a user has Find My iPhone enabled on their device, offline finding is enabled by default when they upgrade a device to iOS 13 or later, iPadOS 13.1 or later and macOS 10.15 or later. This is designed to ensure that every user has the best possible chance to locate their device if it goes missing. However, if at any time the user prefers not to participate, they can disable offline finding in Find My settings on their device. When offline finding is disabled, the device no longer acts as a finder nor is it detectable by other finder devices. However, the user can still locate the device as long as it can connect to a Wi-Fi or mobile network.

When a missing offline device is located, the user receives a notification and email message to let them know the device has been found. To view the location of the missing device, the user opens the Find My app and selects the Devices tab. Rather than showing the device on a blank map as it would have prior to the device being located, Find My shows a map location with an approximate address and information on how long ago the device was detected. If more location reports come in, the current location and time stamp both update automatically. Although users can't play a sound on an offline device or erase it remotely, they can use the location information to retrace their steps or take other actions to help them recover it.

Exhibit 11.

55. For example, the mobile station stores in a local database the last determination performed by the mobile station about its presence in the special area, in connection to the (each)

found device public key. After the storage, the mobile station sends a presence updating signal that uses the information into the referred local database, *i.e.*, the information about said last presence determination.

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.3 Finding

All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.

Generating Reports. The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted using the algorithm described in § 6.1. Finally, the finder creates a complete location report, including the current timestamp (in seconds since January 1, 2001), the ephemeral public key d', the encrypted message, and the AES-GCM authentication tag as shown in Fig. 2.

Id., at 6-7, § 6.3.

56. Defendant has and continues to indirectly infringe one or more claims of the '040 Patent by inducing infringement by others, such as Defendant's customers and end-users, in this District and elsewhere in the United States. For example, Defendant's customers and end-users directly infringe, either literally or under the doctrine of equivalents, through their use of the inventions claimed in the '040 Patent. Defendant induces this direct infringement through its affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products, and providing instructions, documentation, and other information to customers and end-users suggesting that they use the Accused Products in an infringing manner, including technical support, marketing, product manuals, advertisements, and online documentation. *See, e.g.*, Exhibit 8, https://www.apple.com/icloud/find-my/ ("Find My"); *see also, e.g.,* Exhibit 15, available at https://support.apple.com/en-us/104978 ("Find your lost Apple device or AirTag with FindMy"); Exhibit 14, https://support.apple.com/en-us/102648 ("Set up Find My on your iPhone, iPad, or Mac"); Exhibit 16, https://support.apple.com/en-

us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind. ("Set up and use Notify When Left Behind in the Find My App").

57. Because of Defendant's inducement, Defendant's customers and end-users use the Accused Products in a way Defendant intends and they directly infringe the '040 Patent. Defendant performs these affirmative acts with knowledge of the '040 Patent and with the intent, or willful blindness, that the induced acts directly infringe the '040 Patent.

58. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the '040 Patent, as provided by 35 U.S.C. § 271(c), by contributing to direct infringement by others, such as customers and end-users, in this District and elsewhere in the United States. Defendant's affirmative acts of selling and offering to sell the '040 Accused Products in this District and elsewhere in the United States and causing the '040 Accused Products to be manufactured, used, sold, and offered for sale contribute to others' use and manufacture of the Accused Products, such that the '040 Patent is directly infringed by others. The accused components within the Accused Products including, but not limited to, software manufactured by Defendant, are material to the invention of the '040 Patent, are not staple articles or commodities of commerce, have no substantial non-infringing uses, and are known by Defendant to be especially made or adapted for use in the infringement of the '040 Patent. Defendant performs these affirmative acts with knowledge of the '040 Patent and with intent, or willful blindness, that they cause the direct infringement of the '040 Patent.

59. Because of Defendant's direct and indirect infringement of the '040 Patent, ALT has suffered damages in an amount to be proved at trial.

COUNT II
(Infringement of the '720 Patent)

60. Paragraphs 1 through 31 are incorporated by reference as if fully set forth herein.

61. ALT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’720 Patent.

62. Defendant has and continues to infringe the claims of the ’720 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, at least by performing each and every limitation of one or more method claims of the ’720 Patent by using the Accused Products.

63. The Accused Products practice the method of at least claim 1 of the ’720 Patent: A method associated with the use of a mobile station and a radio communication defining device that transmits a distinctive defining signal, the method comprising: receiving and processing the distinctive defining signal in the mobile station, the distinctive defining signal at least defining a special area by one or more of: (1) a coverage area of the distinctive defining signal; (2) a portion of the coverage area that intersects with another area of coverage of another radio communication defining device; and (3) a sum of the area of coverage and the another area of coverage, the distinctive defining signal including information indicating whether or not the radio communication defining device is in a predetermined environment; and sending from the mobile station via a mobile telephone network an updating signal to one or more servers of a provider of presence related services about the mobile station’s presence in the special area, the updating signal being useable by the one or more servers of the provider of presence related services to adjust an operating parameter, which comprises one or more of a tariff and a service flag, to adjust, activate, or deactivate the presence related services provided to the mobile station, and the updating signal comprising the information indicative of whether or not the radio communication defining device is located in the predetermined environment.

64. The Accused Products perform a method associated with the use of a mobile station

and a radio communication defining device that transmits a distinctive defining signal. For example, the Apple Find My service implements a method associated with the use of a mobile station and a missing Bluetooth device that is part of the Find My network for offline finding and that transmits a distinctive defining signal indicative that it is in an offline status (*i.e.*, it is lost).

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, available at https://www.apple.com/icloud/find-my/

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

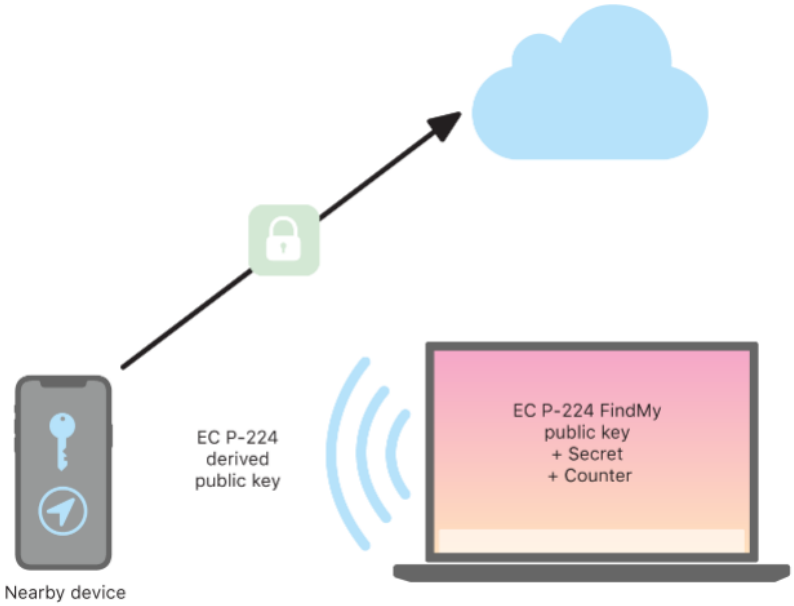


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

When a device goes missing and can't connect to Wi-Fi or cellular — for example, a MacBook Pro is left on a park bench — it begins periodically broadcasting the derived public key P_i for a limited period of time in a Bluetooth payload. By using P-224, the public key representation can fit into a single Bluetooth payload. The surrounding devices can then help in the finding of the offline device by encrypting their location to the public key. Approximately every 15 minutes, the public key is replaced by a new one using an incremented value of the counter and the process above so that the user can't be tracked by a persistent identifier. The derivation mechanism is designed to prevent the various public keys P_i from being linked to the same device.

Exhibit 12, https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

65. For example, within Find My, a user may register their Apple devices, such that they may keep them located when they are nearby, by using the Find My App. As illustrated below,

Find My also provides an "offline finding" mode wherein the user's lost Apple devices (iPhones, iPads, Macs, Apple Watches, AirPods, Apple Pencil, and Apple Vision Pro) that are registered within the Find My network for offline finding can be found with the help of other devices (*e.g.*, iPhones, iPads, Macs).

66. As a further example, the mobile station is an iPhone registered within Find My "offline finding" and helps to find a missing Apple device that is offline and is part of the Find My network. The missing Apple device that is offline and is part of the Find My network for offline finding is a radio communication defining device.

Find My security

The Find My app for Apple devices is built on a foundation of advanced public key cryptography.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, https://www.apple.com/icloud/find-my/

67. For example, if an Apple device that is part of the Find My network for offline finding (*i.e.*, a radio communication defining device) has gone offline, it starts emitting a Bluetooth Low Energy signal (*i.e.*, a distinctive defining signal) that can then be picked up by any Apple device that is part of the Find network for offline finding.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, https://arxiv.org/pdf/2103.02282, at 3, § 3.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Id., https://arxiv.org/pdf/2103.02282, at 3, § 3.

68. For example, the Find My offline finding service involves the use of a mobile station (a *finder* device) and a BLE radio communication defining device (a *lost* device) that

transmits a BLE distinctive defining signal (a unique beacon).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF

Exhibit 13, at 1, Introduction.

69. For example, a lost device advertises a signal indicative of the offline finding service (*i.e.*, a BLE advertisement containing a public key). This signal is a Bluetooth distinctive defining signal transmitted by the radio communication defining device (*i.e.*, transmitted by the lost Apple mobile station in this example). The distinctive defining signal also comprises an identifier of the lost device (*i.e.*, the public key).

6 Apple Offline Finding in Detail

This section describes and discusses the technical details of Apple's OF system. In reference to Fig. 1, we (1) explain the involved cryptography and the key exchange during initial device pairing, and then explain the protocols implementing (2) *losing*, (3) *finding*, (4) *searching* for devices.

In short, devices and accessories in lost mode send out BLE advertisements containing a public key. Finder devices receive them, encrypt their location by using the public key, and upload a report to Apple's servers. This results in an end-to-end encrypted location report that cannot be read by Apple or any other third-party that does not have access to the owner's private keys.

Exhibit 13, at 5, § 6.

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

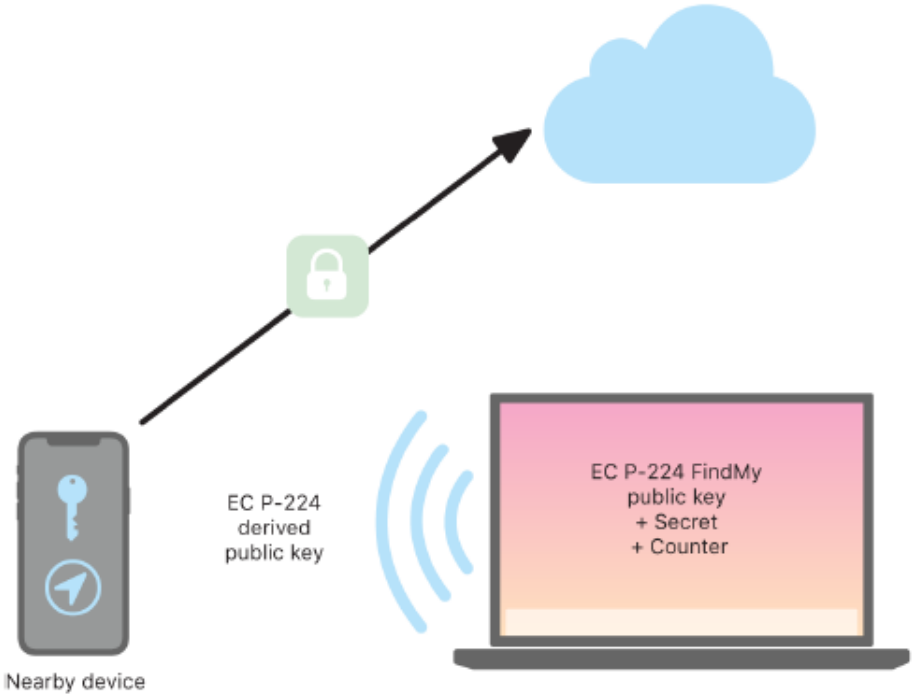


Exhibit 11, https://support.apple.com/en-au/guide/security/sece994d0126/web

70. The Accused Products perform receiving and processing the distinctive defining signal in the mobile station, the distinctive defining signal at least defining a special area by one or more of: (1) a coverage area of the distinctive defining signal; (2) a portion of the coverage area that intersects with another area of coverage of another radio communication defining device; and (3) a sum of the area of coverage and the another area of coverage, the distinctive defining signal including information indicating whether or not the radio communication defining device is in a

predetermined environment. For example, the mobile station receives and processes the signal from the Bluetooth missing device that is in an offline status (*i.e.*, the distinctive defining signal). For example, the special area can be defined by the area covered by the distinctive defining signals of all the radio communication defining devices (*e.g.*, N) that are part of the Find My network for offline finding and are in an offline status at a given time. So, the special area is a dynamic-crowdsourced special area. Within Find My, every Apple device enabled for "offline finding" is converted into a receiver and locator, which effectively crowdsources the search of a missing device. Any device registered within Find My for "offline finding" becomes a Find Node of the Find My network and may receive and process the offline finding signals from lost Apple devices.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1.

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, https://www.apple.com/icloud/find-my/

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

71. For example, if the radio communication defining device is device 1 of the Find My network (being in an offline status) and the rest are devices 2 to N of the Find My network (being in an offline status) the special area can be defined by: the Bluetooth coverage area of the distinctive defining signal (from device 1), and a sum with the area of coverage of Bluetooth radio communication defining device 2, and a sum with the area of coverage of Bluetooth radio communication defining device N.

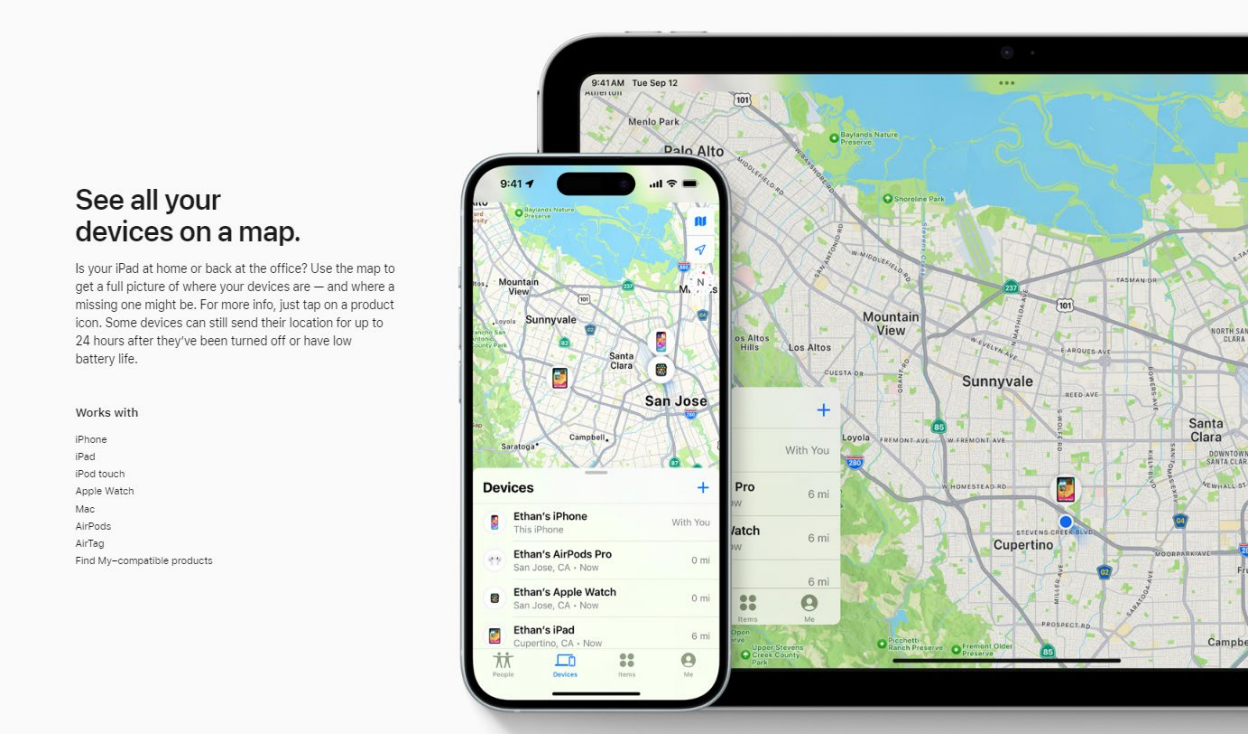


Exhibit 8, https://www.apple.com/icloud/find-my/

72. As a further example, a user can make their Apple devices join the Find My network by using the Find My App. As shown above, a user can register various Apple devices for offline finding. The user can locate the devices by using the Find My map.

73. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format (*i.e.*, the service identifier of the offline finding service for lost Apple devices) serves to the mobile station to determine that a received advertisement signal is distinctive through its unique key. The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the **public key**) by processing the distinctive defining signal.

> **Finder devices.** Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Exhibit 13, at 3, § 3.

74. For example, as the BLE distinctive defining signal is transmitted by the radio communication defining device when it has gone offline, the signal serves to identify (*e.g.*, using an "offline finding service identifier") that the device is in an offline status for offline finding. The offline status of the radio communication defining device (*e.g.*, an Apple device registered with Find My) implies that it is not located nearby any other Apple device of the device owner with capacity to update the location of the missing device and associated to the same Apple Account (*e.g.*, an iPhone registered within Find My in connection to the same account). If the radio communication defining device is not located nearby those other Apple devices, it means that it is located in an environment that is outside the environment defined as the sum of the volumetric spaces wherein the BLE signal from the missing user's device can be received in each of the other user's Apple devices (associated to the same user's account). Said outside environment is the

predetermined environment, and the fact that the distinctive defining signal identifies that the device is offline for offline finding serves to indicate to the mobile station that the device is in the referred predetermined environment. As the predetermined environment depends on the location of the other user's Apple devices, the predetermined environment changes when the location of the other Apple devices changes. As an example: a user has registered within Find My an iPhone 15, Apple AirPods Pro, and AirTags, and he has lost the AirTags. On the basis of the iPhone 15 being switched on and with the Bluetooth enabled, the AirTags being offline implies that the AirTags are located within an environment that is outside the volumetric space wherein the BLE signal from the lost AirTags can be received in the iPhone 15. Said outside environment is the predetermined environment. The following table summarizes the key features of BLE signals. The referred other user's Apple devices can receive a BLE signal from the Apple device when being in range. Otherwise, the Apple device is lost and it is in the predetermined environment.

Table 2. OF advertisement format (with zero-indexed bytes).

Bytes	Content (details cf. [6, § 5.1])
0–5	BLE address $((p_i[0] \mid (0b11 \ll 6)) \mid\mid p_i[1..5])$
6	Payload length in bytes (30)
7	Advertisement type (0xFF for manufacturer-specific data)
8–9	Company ID (0x004C)
10	OF type (0x12)
11	OF data length in bytes (25)
12	Status (e.g., battery level)
13–34	Public key bytes $p_i[6..27]$
35	Public key bits $p_i[0] \gg 6$
36	Hint (0x00 on iOS reports)

Exhibit 13, available at https://arxiv.org/pdf/2103.02282

75. For example, the mobile station sends via a mobile telephone network to the Apple iCloud servers (Apple is a provider of presence related services) a signal that identifies that the mobile station is nearby the missing device that is part of the Find My network (*i.e.*, it is present in the special area). Further, when nearby the lost radio communication defining device, the mobile

station receives the distinctive defining signal. The mobile station is able to identify that the received signal is distinctive in that it relates to the offline finding service (*e.g.*, may comprise an "offline finding service identifier") which means that it is transmitted by a BLE Apple device that is enabled for offline finding and is in an offline status. By determining that it is receiving the BLE offline finding signal the mobile station also identifies that it is present within the crowdsourced offline finding special area (as the device is part of the Find My network for offline finding and its BLE offline finding signal partly defines the special area). The BLE distinctive signal must include a device identifier, such that the Find My services related to the found device can be later provided in connection to that device, as elaborated below.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

76. For example, as a result of the mobile station identifying that it is present in the crowdsourced special area, the mobile station sends (encrypted and securely protected) a signal about the mobile station's presence in the special area to the Apple iCloud servers (Apple is the provider of Find My "offline finding" presence related services), the signal including the mobile station location, as detailed in the image above. A mobile station is not typically placed at the user's home when receiving the distinctive defining signal from a lost device, but in a public environment. So, in those scenarios the mobile station is not connected to the network via Wi-Fi but thought mobile telephony communications, *i.e.*, via a mobile telephone network. The presence signal must also include the device identifier, as it is required by Apple iCloud to subsequently provide related presence related services (*e.g.*, the above-referred notification about the device location). The images below indicate that once a mobile station has identified that it is nearby a lost device that is in an offline status, the location of the mobile station and the device identifier of the lost device are collected to provide the Find My service (this information is sent to the Apple servers within the updating signal, as it is required to allow the device owner to locate the device, once found by the mobile station).

> **Advertising Interval.** The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Exhibit 13, at 6, § 6.2.

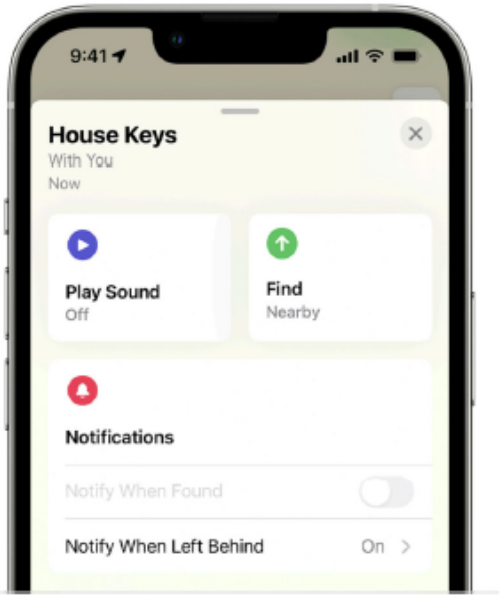
Set up and use Notify When Left Behind in the Find My app

With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

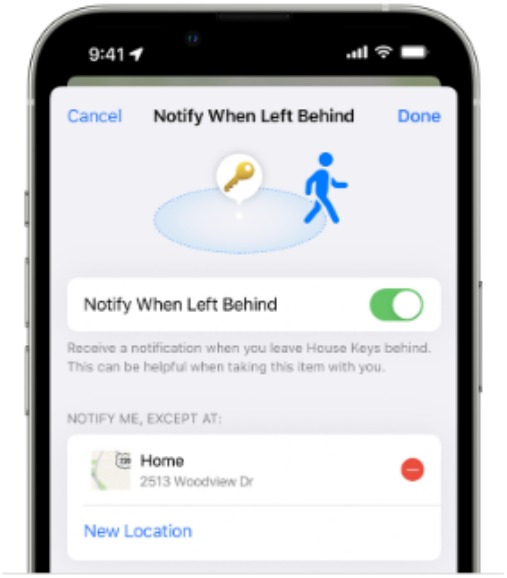
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Id.

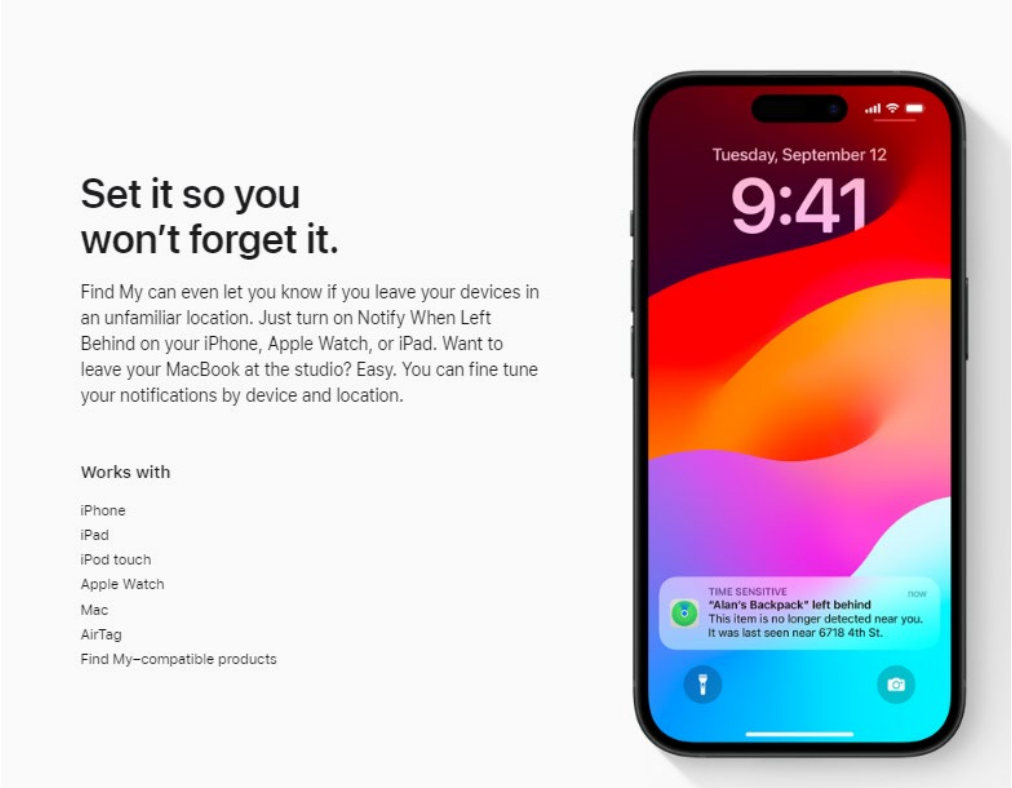


Exhibit 8, https://www.apple.com/icloud/find-my/

77. The Accused Products perform sending from the mobile station via a mobile telephone network, an updating signal to one or more servers of a provider of presence related services about the mobile station's presence in the special area, the updating signal being useable by the one or more servers of the provider of presence related services to adjust an operating parameter, which comprises one or more of a tariff and a service flag, to adjust, activate, or deactivate the presence related services provided to the mobile station, and the updating signal comprising the information indicative of whether or not the radio communication defining device is located in the predetermined environment. For example, a mobile station (a *finder* device) identifies that it is present within the area of coverage of a device that is lost and is part of the Find My offline finding network and sends to a vendor controller server (*i.e.*, to the Apple iCloud servers in the case of Apple devices and Find My offline finding ecosystem) an updating signal indicative of the presence status (the signal including the unique beacon data received from the

lost device via BLE, together with the location of the device).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Id., at 3, § 3.

78. For example, the mobile station identifier of the mobile station is included within the updating signal sent to the Apple iCloud.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

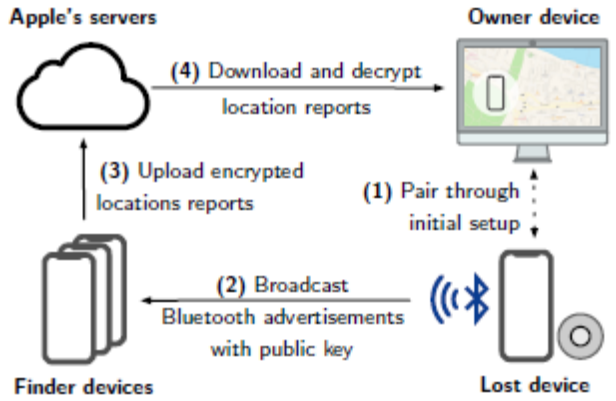


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

79. For example, the updating signal is usable by the Apple iCloud servers to adjust a [lost/found] service flag operational parameter to "found" and to adjust/activate the presence related services provided to the mobile station, as services requestor (as elaborated herein below). The Apple iCloud servers (Apple is the provider of presence related services) receives the presence updating signal and uses it to provide presence related services. When a Find "offline finding" registered device related to a given Apple Find My user's account is missing, a service flag operational parameter is set to "Mark as Lost" in the Apple iCloud, such that the device is displayed as "Activated" or "Enabled." In that situation the user can wait for a mobile station that is part of the Find My network for offline finding to help in finding it. The image below illustrates how the found device owner benefits from the visualization of an updated location within a Find My map, in connection to the device found by the mobile station (as a result of the activation or enabling referred to above). If the device owner selected the "Notify When Found" feature (*see* the first

image below) then they will be notified when the missing device is found.

See the location of your device on a map

You can see your device's current or last known location in the Find My app.

Tap Devices at the bottom of the screen, then tap the name of the device you want to locate.

- *If the device can be located:* It appears on the map so you can see where it is.
- *If the device can't be located:* You see "No location found" below the device's name. Below Notifications, turn on Notify When Found. You receive a notification when it's located.

  Important: Make sure you allow notifications for the Find My app. See Change notification settings on iPhone.

For troubleshooting steps, see the Apple Support article If Find My is offline or not working.

Exhibit 17, https://support.apple.com/guide/iphone/locate-a-device-iph09b087eda/ios

80. For example, when the user is nearby an Apple device, OF devices can use BLE advertisements to inform nearby finders about their presence. The following image further shows a Galaxy SmartTag located in a Find map thanks to offline finding (as a result of the activation (2) referred to above).

2.1 Bluetooth Low Energy

Bluetooth Low Energy (BLE) [19] is designed for small battery-powered devices such as smartwatches and fitness trackers with low data rates. Devices can broadcast BLE advertisements to inform nearby devices about their presence. The maximum BLE advertisement payload size is 31 bytes [19]. Apple heavily relies on custom BLE advertisements to announce their proprietary services such as AirDrop and bootstrap their protocols over Wi-Fi or Apple Wireless Direct Link (AWDL) [21, 36, 48]. OF devices also use BLE advertisements to inform nearby finders about their presence [6].

Exhibit 13, https://arxiv.org/pdf/2103.02282, at 2, § 2.1.

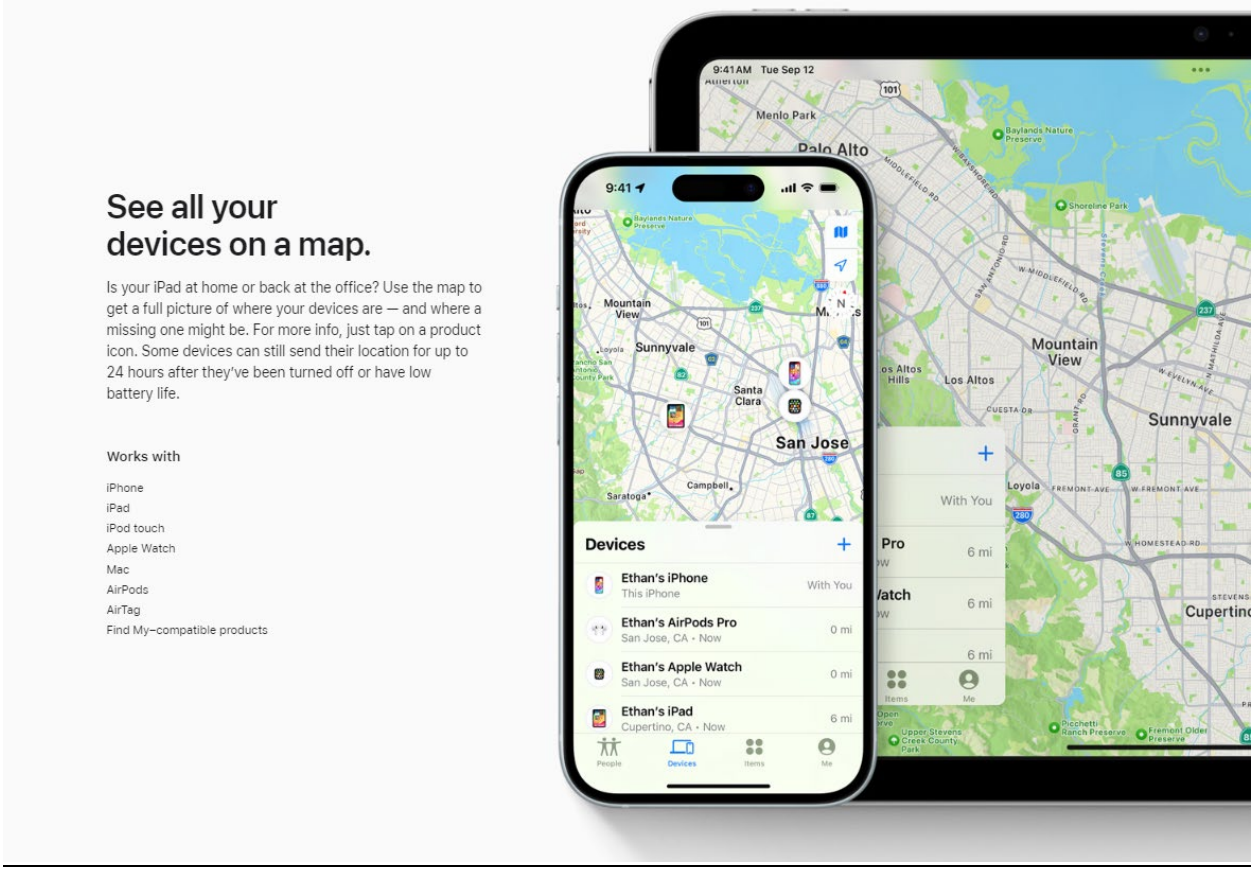


Exhibit 8, https://www.apple.com/icloud/find-my/

81. For a further example, when the Apple iCloud servers adjust the service flag operational parameter to Turn off Lost Mode, as a result of receiving the presence updating signal, the adjustment also serves to activate a presence related service related to the sending of an acknowledgment signal to the mobile station. As in the previous examples, the presence related service is provided to the mobile station as it is the entity triggering the updating signal, that is the service request. The acknowledgement presence related service is partly processed by the provider of presence related services, *i.e.*, by the Apple iCloud that generates the ack once the operation to update the device status to Turn off Lost Mode has been successful, and partly processed by the mobile station, that receives the ack.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Id., at 3, § 3.

82. For example, the beneficiary of the presence related service is the mobile station, that can adapt the reporting process based upon the received acknowledgement. The updating signal is triggered as a result of the mobile station receiving the distinctive defining signal

indicative that the lost device is in an offline status. Thus, the updating signal related to the offline finding service is, by its nature, indicative that the found device is in an offline status.

83. Defendant has and continues to indirectly infringe one or more claims of the '720 Patent by inducing infringement by others, such as Defendant's customers and end-users, in this District and elsewhere in the United States. For example, Defendant's customers and end-users directly infringe, either literally or under the doctrine of equivalents, through their use of the inventions claimed in the '720 Patent. Defendant induces this direct infringement through its affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products, and providing instructions, documentation, and other information to customers and end-users suggesting that they use the Accused Products in an infringing manner, including technical support, marketing, product manuals, advertisements, and online documentation. *See, e.g.*, Exhibit 8, https://www.apple.com/icloud/find-my/ ("Find My"); *see also, e.g.,* Exhibit 15, available at https://support.apple.com/en-us/104978 ("Find your lost Apple device or AirTag with FindMy"); Exhibit 14, https://support.apple.com/en-us/102648 ("Set up Find My on your iPhone, iPad, or Mac"); Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind. ("Set up and use Notify When Left Behind in the Find My App").

84. Because of Defendant's inducement, Defendant's customers and end-users use the Accused Products in a way Defendant intended and they directly infringe the '720 Patent. Defendant performs these affirmative acts with knowledge of the '720 Patent and with the intent, or willful blindness, that the induced acts directly infringe the '720 Patent.

85. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the '720 Patent, as provided by 35 U.S.C. § 271(c), by contributing to direct infringement

by others, such as customers and end-users, in this District and elsewhere in the United States. Defendant's affirmative acts of selling and offering to sell the '720 Accused Products in this District and elsewhere in the United States and causing the '720 Accused Products to be manufactured, used, sold, and offered for sale contribute to others' use and manufacture of the Accused Products, such that the '720 Patent is directly infringed by others. The accused components within the Accused Products including, but not limited to, software manufactured by Defendant, are material to the invention of the '720 Patent, are not staple articles or commodities of commerce, have no substantial non-infringing uses, and are known by Defendant to be especially made or adapted for use in the infringement of the '720 Patent. Defendant performs these affirmative acts with knowledge of the '720 Patent and with intent, or willful blindness, that they cause the direct infringement of the '720 Patent.

86. Because of Defendant'' direct and indirect infringement of the '720 Patent, ALT has suffered damages in an amount to be proved at trial.

COUNT III
(Infringement of the '910 Patent)

87. Paragraphs 1 through 31 are incorporated by reference as if fully set forth herein.

88. ALT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '910 Patent.

89. Defendant has and continues to directly infringe the claims of the '910 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, at least by making, using, offering to sell, selling, and/or importing into the United States products and actively inducing others to make, use, sell, offer to sell, and/or import products, such as the Accused Products, that satisfy each and every limitation of one or more claims of the '910 Patent, and by performing each and every limitation of one or more method claims of the '910 Patent.

90. The Accused Products each comprise the system of at least claim 7 of the ’910 Patent: A mobile station capable of receiving first and second distinctive defining signals, respectively, from first and second radio communication defining devices, the first and second distinctive defining signals at least partly defining a special area by a sum or intersection of their coverage, the first and second distinctive defining signals respectively including first and second data, the mobile station comprising: an electronic storage medium that stores at least a portion of the first and second data; and a processor adapted to process the first and second distinctive defining signals to determine, based on at least portion of one or both of the first and second data, whether or not the mobile station is present in the special area, the processor further adapted to send from the mobile station via a mobile telephone network an updating signal to one or more servers of a provider of presence related services about the mobile station’s presence in the special area, the sending of the updating signal being uncorrelated to any mobile station phone call establishment, the updating signal being sent at least one of (i) periodically, (ii) at times recent to when the mobile station enters into or exists from the special area, and (iii) when the mobile station remains in the special area.

91. The Accused Products comprise a mobile station capable of receiving first and second distinctive defining signals, respectively, from first and second radio communication defining devices, the first and second distinctive defining signals at least partly defining a special area by a sum or intersection of their coverage, the first and second distinctive defining signals respectively including first and second data. For example, Apple Find My “offline finding” service implements a method associated with the use of a mobile station and at least first and second Bluetooth radio communication defining devices that respectively transmit first and second Bluetooth distinctive defining signals that partly define an offline finding special area by a sum of

their coverage. The first Bluetooth distinctive defining signal includes first data that includes an "offline finding service identifier". The second Bluetooth distinctive defining signal includes second data that also includes an "offline finding service identifier." The service identifier within the first data may be the same or different than the one within the second data. As an example, the first data may include an offline finding service identifier related to a lost mobile device (*i.e.*, a public key, as detailed below), and the second data may include a different offline finding service identifier related to a lost smart tag (*i.e.*, a different public key, as detailed below). In more detail, within the Apple Find My offline finding service, a missing Bluetooth device that is part of the Apple Find My network for offline finding (*i.e.*, both the first and the second radio communication defining devices are part of the network) transmits a BLE distinctive defining signal indicating that it is in an offline status (*i.e.*, it is lost). The mobile station has the capability to determine whether or not it is receiving an offline finding service distinctive defining signal that includes an offline finding service identifier.

The Find My app makes it easy to keep track of your Apple devices — even if they're offline. You can also locate items using AirTag or Find My technology. Or pinpoint friends and family with Precision Finding. Everyone's location stays private every step of the way.

Find your stuff on iCloud.com ↗

Exhibit 8, available at https://www.apple.com/icloud/find-my/

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Id.

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

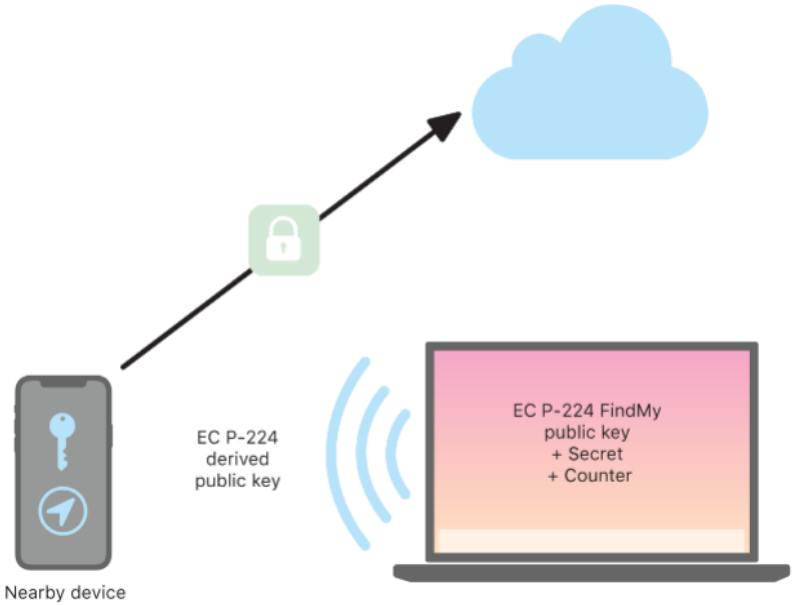


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

Find My security

The Find My app for Apple devices is built on a foundation of advanced public key cryptography.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

92. For example, within Apple Find My, a user may register their Apple devices such that they may keep them located when they are nearby, by using the Find My App. As illustrated below, Find My also provides an "offline finding" mode wherein user's lost Apple devices (iPhones, iPads, Macs, Apple Watches, AirPods, Apple Pencil, and Apple Vision Pro) that are registered within the Find My network for offline finding can be found with the help of other devices (*e.g.*, iPhones, iPads, Macs) that process received offline finding distinctive defining signals. The mobile station can be an iPhone registered within Find My "offline finding" and helps to find missing Apple devices that are offline and are part of the Find My network. The missing Apple devices that are offline and are part of the Find My network for offline finding include the

first and second radio communication defining devices, which transmit, respectively, the first and second distinctive defining signals.

Find My security

The Find My app for Apple devices is built on a foundation of advanced public key cryptography.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Id., available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, https://www.apple.com/icloud/find-my/

93. For example, if an Apple device that is part of the Find My network for offline finding (*i.e.*, the first and second radio communication defining devices) has gone offline, it starts emitting a Bluetooth Low Energy signal (*i.e.*, a distinctive defining signal) that can then be picked up by any Apple device that is part of the Find network for offline finding.

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

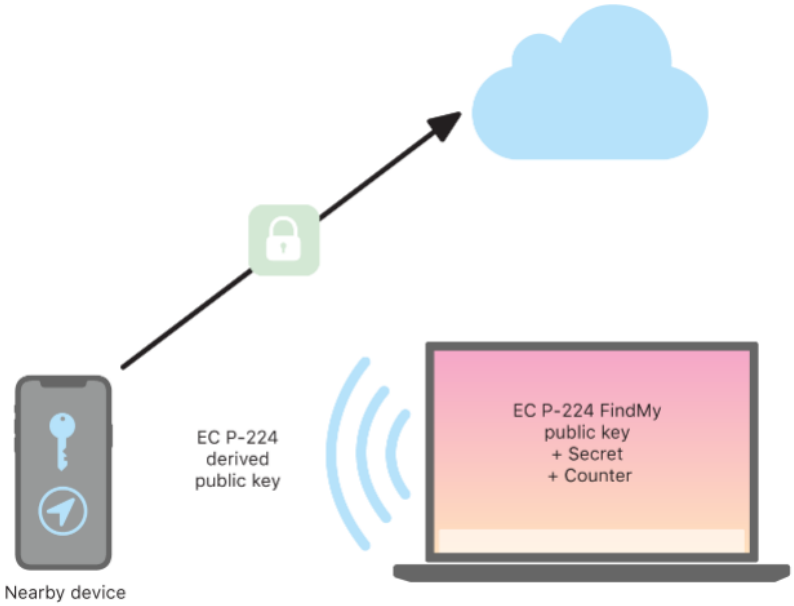


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

94. For example, the Apple Find My offline finding service involves the use of a mobile station (a *finder* device) and BLE radio communication defining devices (*lost* devices) that transmit a BLE distinctive defining signal (a unique beacon).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF

Exhibit 13, at 1, Introduction.

95. For example, a lost device emits a BLE advertisement indicative of the offline finding service (*i.e.*, a BLE advertisement containing a public key). This signal is a Bluetooth distinctive defining signal transmitted by the radio communication defining device (*i.e.*, transmitted by the lost Apple mobile station in this example). The distinctive defining signal also comprises an identifier of the lost device (*i.e.*, the public key).

6 Apple Offline Finding in Detail

This section describes and discusses the technical details of Apple's OF system. In reference to Fig. 1, we (1) explain the involved cryptography and the key exchange during initial device pairing, and then explain the protocols implementing (2) *losing*, (3) *finding*, (4) *searching* for devices.

In short, devices and accessories in lost mode send out BLE advertisements containing a public key. Finder devices receive them, encrypt their location by using the public key, and upload a report to Apple's servers. This results in an end-to-end encrypted location report that cannot be read by Apple or any other third-party that does not have access to the owner's private keys.

Id., at 5, § 6.

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

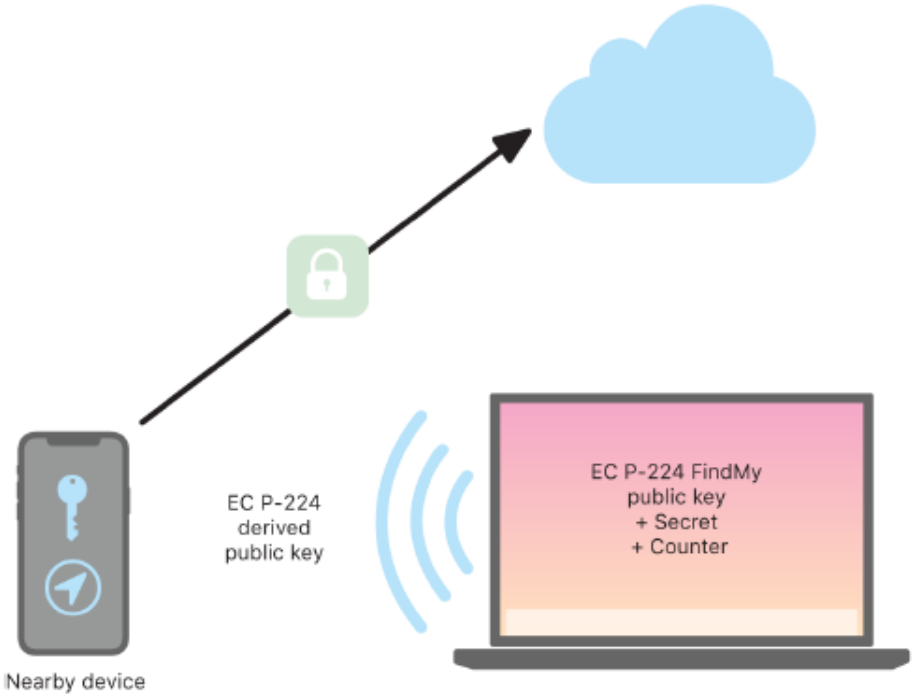


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

96. The Accused Products include an electronic storage medium that stores at least a portion of the first and second data; and a processor adapted to process the first and second distinctive defining signals to determine, based on at least portion of one or both of the first and second data, whether or not the mobile station is present in the special area. The mobile station determines if it is receiving one or both of the first and second Bluetooth distinctive defining signals by using previously obtained at least portion of one or both of the first and second data (*i.e.*, previously obtained "offline finding service identifiers). If the mobile station receives an "offline finding service identifier" from a first lost radio communication defining signal (identified by its corresponding public key) then it determines that it is receiving a first distinctive defining signal (that partly defines the "offline finding" special area by its coverage).

Table 2. OF advertisement format (with zero-indexed bytes).

Bytes	Content (details cf. [6, § 5.1])
0–5	BLE address $((p_i[0] \mid (0b11 \ll 6)) \mid\mid p_i[1..5])$
6	Payload length in bytes (30)
7	Advertisement type (0xFF for manufacturer-specific data)
8–9	Company ID (0x004C)
10	OF type (0x12)
11	OF data length in bytes (25)
12	Status (e.g., battery level)
13–34	Public key bytes $p_i[6..27]$
35	Public key bits $p_i[0] \gg 6$
36	Hint (0x00 on iOS reports)

Exhibit 13, https://arxiv.org/pdf/2103.02282 at 6.

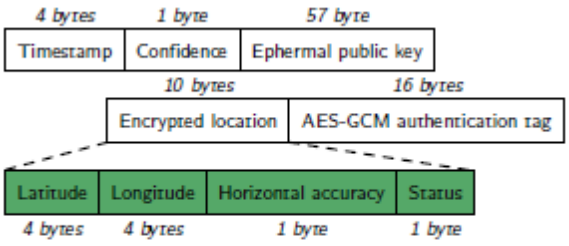


Fig. 2. Binary format of a location report.

Id., at 7.

97. Further, if the mobile station receives an "offline finding service identifier" from a second lost radio communication defining signal (identified by its corresponding public key), then it determines that it is receiving a second distinctive defining signal (that also partly defines the "offline finding" special area by its coverage). If the mobile station determines that it is receiving either one or both of the first and second distinctive defining signals, it consequently identifies that it is present within the "offline finding" special area. And each of the first and second distinctive defining signals partly define the special area.

98. As a further example, determining whether a received signal is a first/second distinctive defining signal is based on a previously obtained at least portion of the first/second data. Therefore, the presence determination is also based on the first and/or second data. Within Find My, every Apple device enabled for "offline finding" is converted into a receiver and locator to help search for missing devices. Any device registered within Find My for "offline finding" becomes a Find Node of the Find My network and may receive and process the offline finding BLE defining signals from lost Apple devices.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1.

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, https://www.apple.com/icloud/find-my/

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

99. As a further example, the special area can be defined as the area covered by the Bluetooth distinctive defining signals of all the radio communication defining devices that are part of the Find My network for offline finding and are in an offline status at a given time. Therefore, the special area is partly defined by a sum of the coverage of the first and the second Bluetooth distinctive defining signals from the first and second Bluetooth radio communication defining devices (that are part of the Find My network and are lost). As shown below, a user can register various Apple devices for offline finding. The user can locate the devices by using the Find My map.

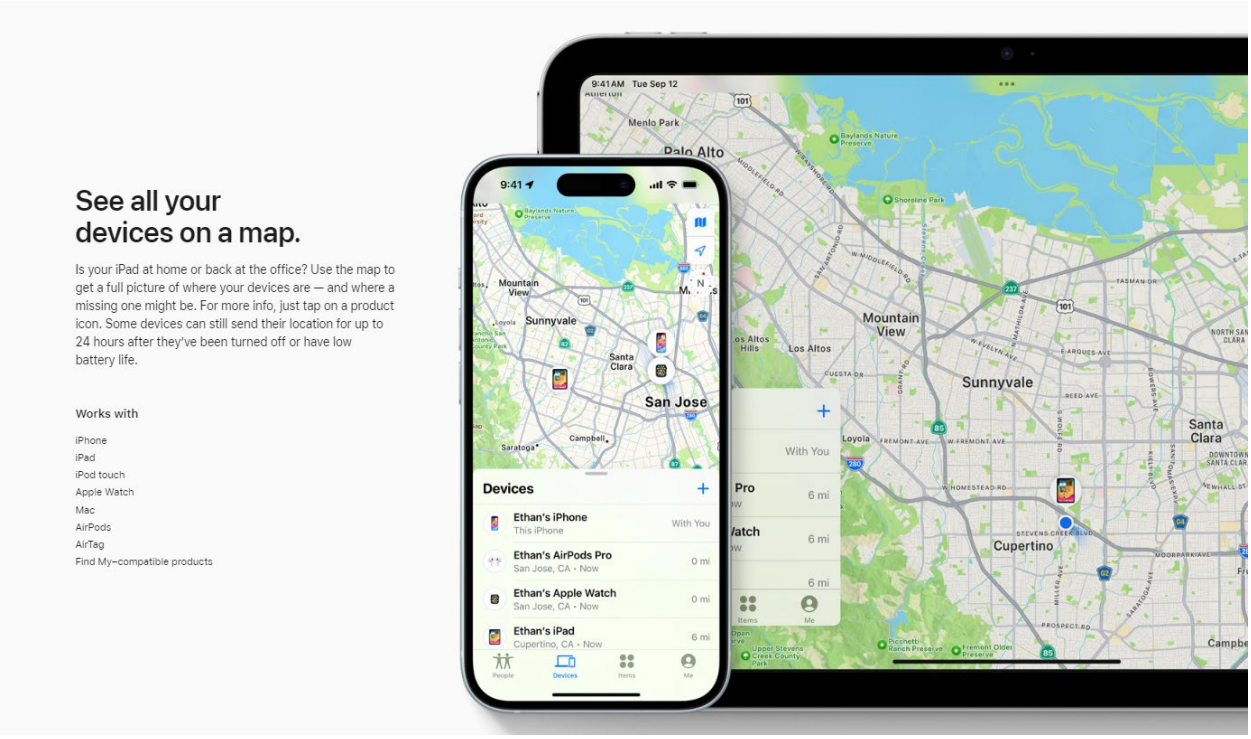


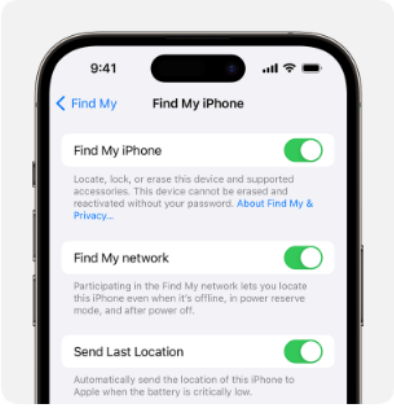
Exhibit 8, https://www.apple.com/icloud/find-my/

Set up Find My on your iPhone, iPad, or Mac

Set up Find My so that you can locate a lost device or item — such as your paired AirPods, Apple Watch, or a personal item with an AirTag attached.

How to turn on Find My for your iPhone or iPad

1. Open the Settings app.
2. Tap your name, then tap Find My.
3. If you want friends and family to know where you are, turn on Share My Location.
4. Tap Find My [device], then turn on Find My [device].



5. To see your device even when it's offline, turn on Find My network.*
   - To have the location of your device sent to Apple when the battery is low, turn on Send Last Location.

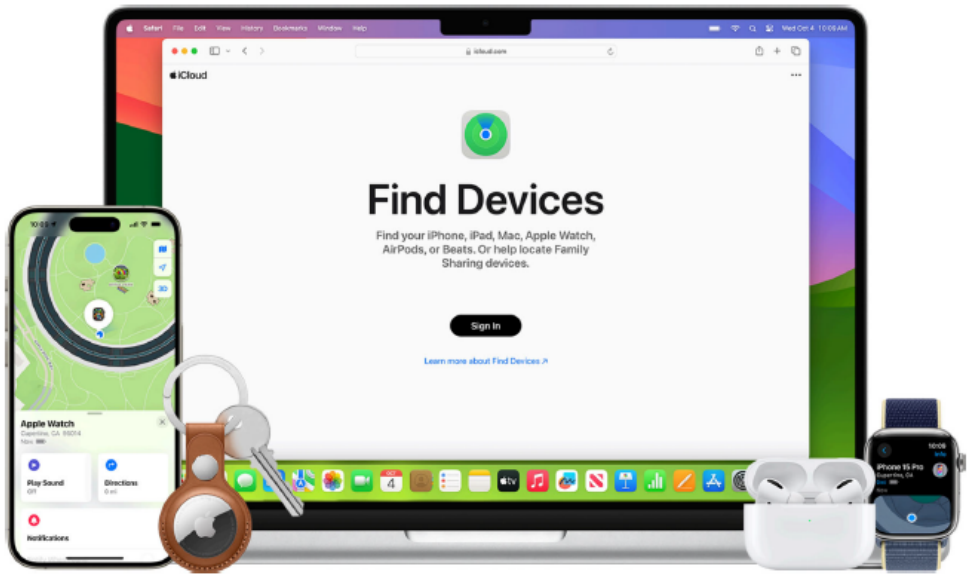
If you want to be able to find your lost device on a map, make sure that Location Services is turned on. To do this, go to Settings > Privacy & Security > Location Services, and turn on Location Services.

* The Find My network is an encrypted, anonymous network of hundreds of millions of Apple devices that can help you locate your device.

Exhibit 14, https://support.apple.com/en-us/102648

Find your lost Apple device or AirTag with Find My

If you lose your Apple device, personal item connected to an AirTag, or other Find My network accessory, use Find My to find it or mark it as lost to protect your device and personal information.



Find your stuff with Find My

If you've lost or misplaced an Apple device or personal item with an AirTag attached, use Find My to find your device or item on a map. You can get directions to its location and, when you're nearby, play a sound or even get help finding its exact location.

Exhibit 15, https://support.apple.com/en-us/104978

100. For example, the result of the BLE advertisement scan by the mobile station that parses a "public key" from the advertisement allows the mobile station to determine that a received advertisement signal is distinctive through its unique key. The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **Finder devices.** Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Exhibit 13, at 3, § 3.

101. For example, the mobile station scans over BLE and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal based on receiving a packet in the OF advertisement format), the mobile station must necessarily store data related to the OF advertisement (*i.e.*, store previous obtained checking data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **6.3 Finding**
>
> All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.
>
> **Generating Reports.** The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

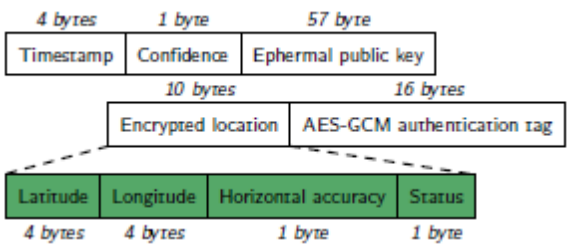


Fig. 2. Binary format of a location report.

ing the algorithm described in § 6.1. Finally, the finder creates a complete location report, including the current timestamp (in seconds since January 1, 2001), the ephemeral public key d', the encrypted message, and the AES-GCM authentication tag as shown in Fig. 2.

Exhibit 13, at 6-7, § 6.3.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0FBAE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Id., at 7, § 6.3.

102. For example, the mobile station scans over BLE and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a received signal is a distinctive defining signal) the mobile station must necessarily store data related to the public key (*i.e.*, store previous obtained first/second data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station sends via a mobile telephone network to the Apple iCloud servers (Apple is a provider of presence related services), a signal that identifies that the mobile station is nearby the first and/or the second lost radio communication defining device that is part of the Find My network (*i.e.*, it is present in the special area). More in detail, when nearby the first and/or second lost radio communication defining device, the mobile station receives the first/second distinctive defining signal. The mobile station is able to identify that the received first/second signal is distinctive and to determine that it is present within the special area, as detailed above. The first/second BLE distinctive signals must include a device identifier such that the Find My services related to the first/second found device can be later provided in connection to that device, as elaborated below.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

103. The Accused Products include the processor further adapted to send from the mobile station via a mobile telephone network an updating signal to one or more servers of a provider of presence related services about the mobile station's presence in the special area, the sending of the updating signal being uncorrelated to any mobile station phone call establishment, the updating signal being sent at least one of (i) periodically, (ii) at times recent to when the mobile station enters into or exists from the special area, and (iii) when the mobile station remains in the special area. For example, the mobile station sends a signal about the mobile station's presence in the special area via a mobile telephone network to the Apple iCloud servers (Apple is the provider of Find My "offline finding" presence related services), the signal including the mobile station's location. When sending the presence updating signal, the mobile station is not necessarily within

Wi-Fi coverage. In that case, the mobile station must send its updating signal via a mobile telephone network. The presence signal must also include the device identifier of the first and/or second found device, because the Find My network needs this to subsequently provide related presence related services (*e.g.*, the notification to the device owner about the device location). The images below indicate that once a mobile station has identified that it is nearby a lost device that is in an offline status, the location of the mobile station and the device identifier of the lost device are collected to provide the Find My service (this information is sent to the Apple servers within the updating signal, as it is required to allow the device owner to locate the device, once found by the mobile station).

> **Advertising Interval.** The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

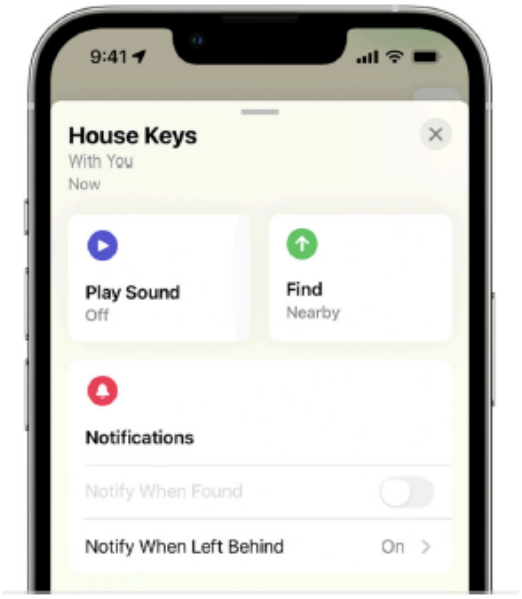
Exhibit 13, at 6, § 6.2.

> **Set up and use Notify When Left Behind in the Find My app**
>
> With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

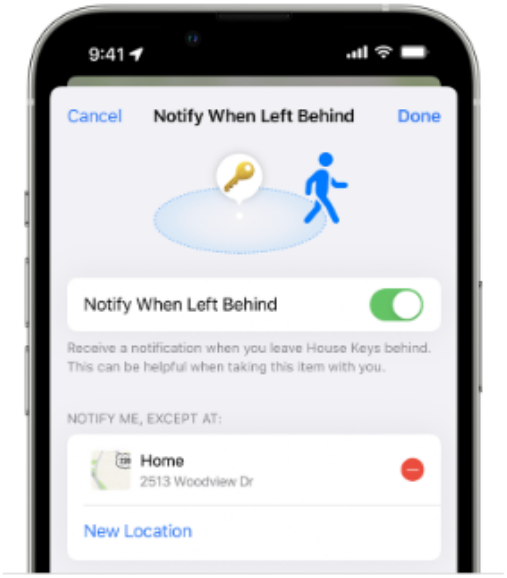
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Id.

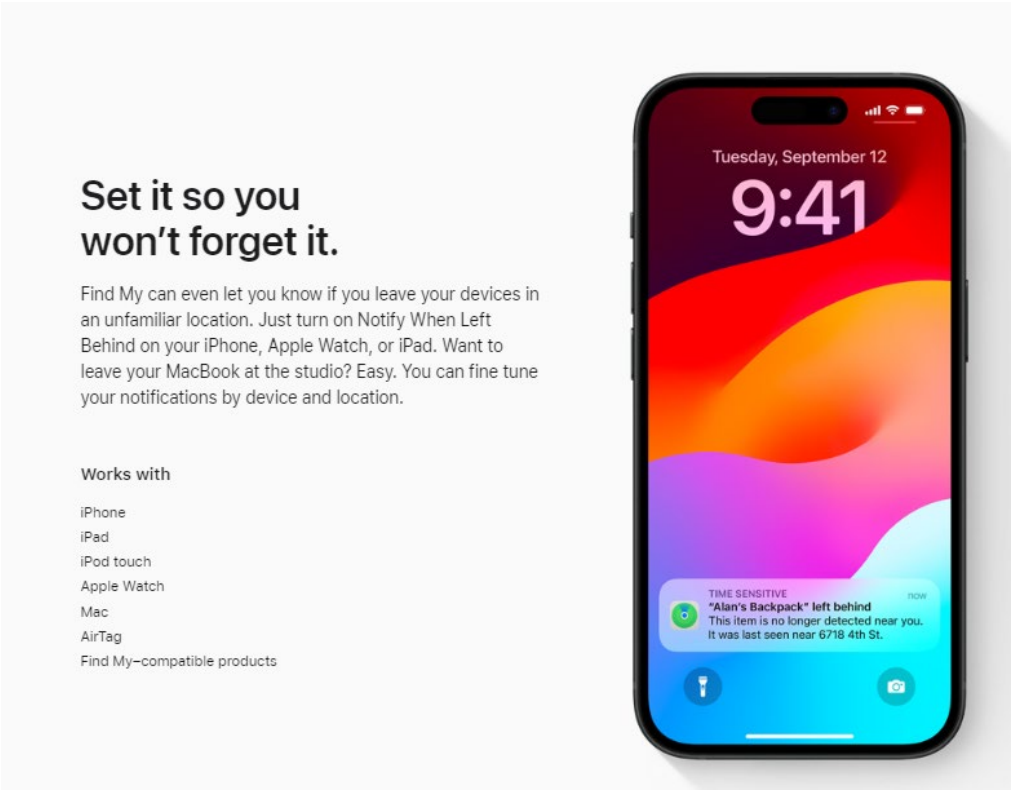


Exhibit 8, https://www.apple.com/icloud/find-my/

104. For example, the Apple iCloud servers (Apple is the provider of presence related services) receives the presence updating signal and uses it to provide presence related services, *e.g.*, displaying the device location on a map or, *e.g.*, sending a notification to the owner that a device has been left behind (Notify When Left Behind).

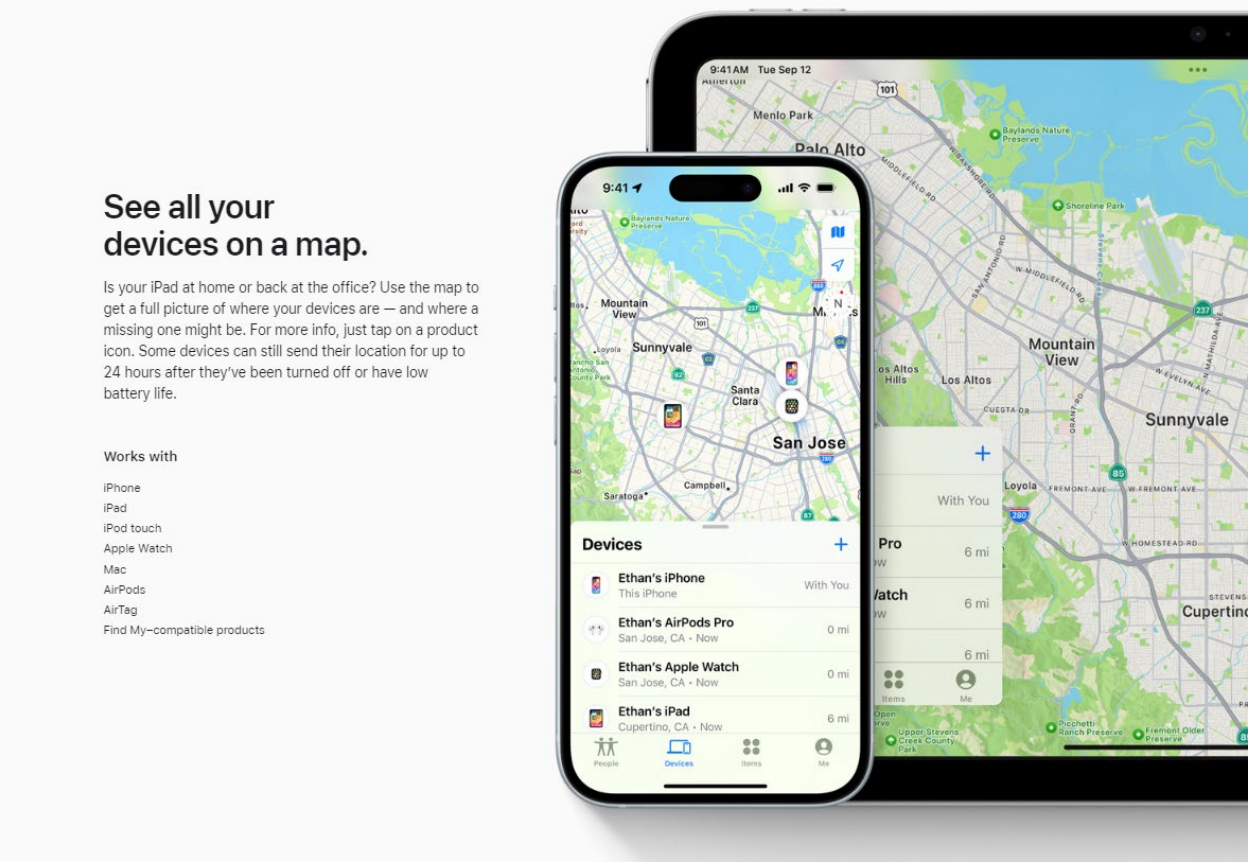
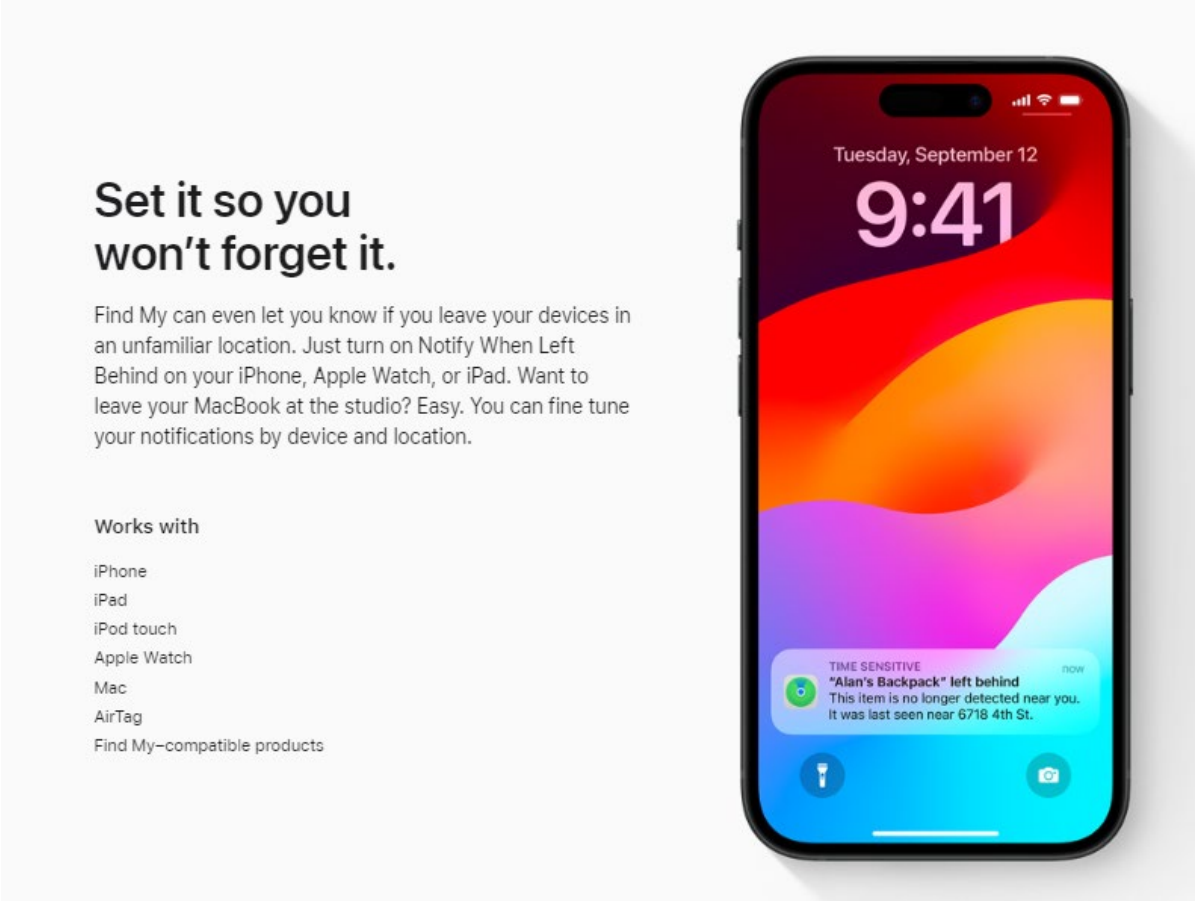


Exhibit 8, https://www.apple.com/icloud/find-my/



Id.

105. For example, a mobile station (a *finder* device) identifies that it is present within the area of coverage of a device that is lost (*e.g.*, the first and/or second radio communication defining device) and is part of the Find My finding network and sends to a vendor controller server (*i.e.*, to the Apple iCloud servers in the case of Apple devices and Apple offline finding ecosystem) an updating signal indicating the presence status (the signal including unique beacon data received from the lost first/second device via BLE, together with the location of the device).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Id., at 3, § 3.

106. For example, the sending of the updating signal is uncorrelated to any mobile station phone call establishment. The updating signal is sent when the mobile station enters into the offline finding special area and starts receiving the first and/or second distinctive defining

signals from the first/second lost radio communication defining device. Also, if the mobile station remains nearby the first and/or second lost device (*i.e.*, remains in the special area), it periodically sends a presence updating signal via mobile telephone network to the Apple iCloud servers, as further elaborated below. The mobile station stores in a local database the determination performed by the mobile station about its presence in the special area, in relation to each found device public key identifier (*i.e.*, in connection to at least the first and/or second radio communication defining devices). After storage, the mobile station sends a presence updating signal containing the (each) lost device public key and the location to the Apple iCloud servers. If it is the first (recent) reporting by the mobile station about its presence in the special area, the presence updating signal is then related to the mobile station entering into the special area.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

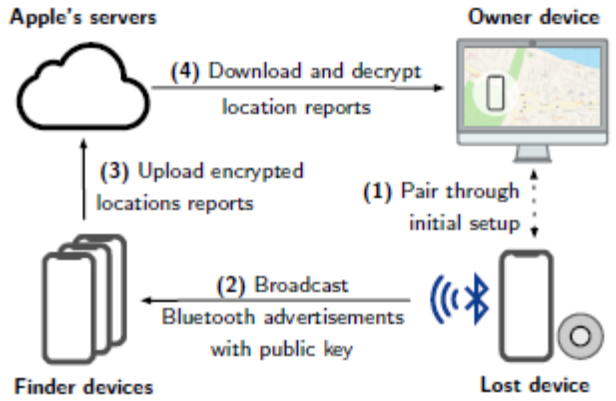


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

107. For example, the mobile station receives an acknowledgment about the presence updating signal having been received in the Apple iCloud servers (via a mobile telephone network), as indicated in the image below. As also indicated in the image below, the presence determination process (*i.e.*, the scanning and filtering of OF advertisements in a certain format) is then reinitiated. If the mobile station remains in the special area in connection to a lost device, it has already reported (*i.e.*, the first and/or second radio communication defining devices), then it may send (after 15 minutes) a new updating signal related to the mobile station presence in the special area (in connection to that lost device): *i.e.*, the presence updating signal is then related to the mobile station remaining in the special area.

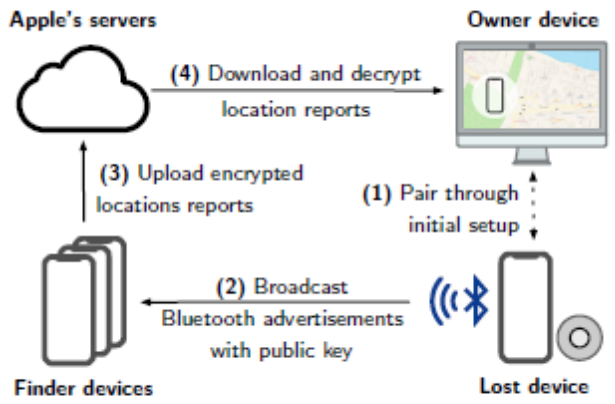


Fig. 1. Simplified offline finding (OF) workflow.

Exhibit 13, at 3, FIG. 1.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

108. For example, the mobile station stores in a local database the determination performed by mobile station about its presence in the special area, in connection to the (each) found device private key (*e.g.*, in connection to at least the first and/or second radio communication defining devices). After the storage, the mobile station sends a presence updating signal containing the device(s) public key(s) and the location to the Apple iCloud servers). If it is the first (recent) reporting by the mobile station about the mobile station presence in the special area, the presence updating signal is then related to the mobile station entering into the special area.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0F8AE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Exhibit 13, at 7, § 6.3.

109. Defendant has and continues to indirectly infringe one or more claims of the '910 Patent by inducing infringement by others, such as Defendant's customers and end-users, in this District and elsewhere in the United States. For example, Defendant's customers and end-users directly infringe, either literally or under the doctrine of equivalents, through their use of the inventions claimed in the '910 Patent. Defendant induces this direct infringement through its

affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products, and providing instructions, documentation, and other information to customers and end-users suggesting that they use the Accused Products in an infringing manner, including technical support, marketing, product manuals, advertisements, and online documentation. *See, e.g.*, Exhibit 8, https://www.apple.com/icloud/find-my/ ("Find My"); *see also, e.g.,* Exhibit 15, available at https://support.apple.com/en-us/104978 ("Find your lost Apple device or AirTag with FindMy"); Exhibit 14, https://support.apple.com/en-us/102648 ("Set up Find My on your iPhone, iPad, or Mac"); Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind. ("Set up and use Notify When Left Behind in the Find My App").

110. Because of Defendant's inducement, Defendant's customers and end-users use the Accused Products in a way Defendant intends and they directly infringe the '910 Patent. Defendant performs these affirmative acts with knowledge of the '910 Patent and with the intent, or willful blindness, that the induced acts directly infringe the '910 Patent.

111. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the '910 Patent, as provided by 35 U.S.C. § 271(c), by contributing to direct infringement by others, such as customers and end-users, in this District and elsewhere in the United States. Defendant's affirmative acts of selling and offering to sell the '910 Accused Products in this District and elsewhere in the United States and causing the '910 Accused Products to be manufactured, used, sold, and offered for sale contribute to others' use and manufacture of the Accused Products, such that the '910 Patent is directly infringed by others. The accused components within the Accused Products including, but not limited to, software manufactured by Defendant, are material to the invention of the '910 Patent, are not staple articles or commodities

of commerce, have no substantial non-infringing uses, and are known by Defendant to be especially made or adapted for use in the infringement of the ’910 Patent. Defendant performs these affirmative acts with knowledge of the ’910 Patent and with intent, or willful blindness, that they cause the direct infringement of the ’910 Patent.

112. Because of Defendant’s direct and indirect infringement of the ’910 Patent, ALT has suffered damages in an amount to be proved at trial.

COUNT IV
(Infringement of the ’922 Patent)

113. Paragraphs 1 through 31 are incorporated by reference as if fully set forth herein.

114. ALT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’922 Patent.

115. Defendant has and continues to directly infringe the claims of the ’922 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, at least by performing each and every limitation of one or more method claims of the ’922 Patent by using the Accused Products.

116. The Accused Products practice the method of at least claim 1 of the ’922 Patent: A method associated with one or more providers of presence related services in connection with the use of a mobile station and electronically storing in one or more memories data capable of linking the mobile station to the first and second special areas, the data including a first checking data of the first radio communication defining device, a second checking data of the second radio communication defining device, and a first identifier related to the mobile station, transmitting via a mobile telephone network to the mobile station at least a portion of the first checking data, and transmitting via the mobile telephone network to the mobile station at least a portion of the second checking data, receiving from the mobile station via the mobile telephone network a first updating

signal uncorrelated to any mobile station phone call establishment that identifies the mobile station's presence in at least the first special area, and receiving from the mobile station via the mobile telephone network, a second updating signal uncorrelated to any mobile station phone call establishment that identifies the mobile station's presence in at least the second special area, the first updating signal including a second identifier related to the mobile station, the second updating signal including a third identifier related to the mobile station, deriving from the first updating signal by one or more processing devices having access to at least a portion of the data whether or not the mobile station is present in the first special area, and deriving from the second updating signal by the one or more processing devices whether or not the mobile station is present in the second special area; and enabling or disabling by use of the one or more processing devices a presence related service based upon the mobile station's presence or non-presence in the first special area, and enabling or disabling by use of the one or more processing devices a presence related service based upon the mobile station's presence or non-presence in the second special area.

117. The Accused Products perform a method associated with one or more providers of presence related services in connection with the use of a mobile station and at least a first radio communication defining device that transmits a first distinctive defining signal and a second radio communication defining device that transmits a second distinctive defining signal, the first distinctive defining signal at least partly defines a first special area by its coverage, the second distinctive defining signal at least partly defining a second special area by its coverage. For example, Apple's Find My implements a method associated with the use of a mobile station and a missing Bluetooth device that is part of the Find My network for offline finding and that transmits a distinctive defining signal indicative that it is in an offline status (*i.e.*, it is lost).

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, available at https://www.apple.com/icloud/find-my/

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

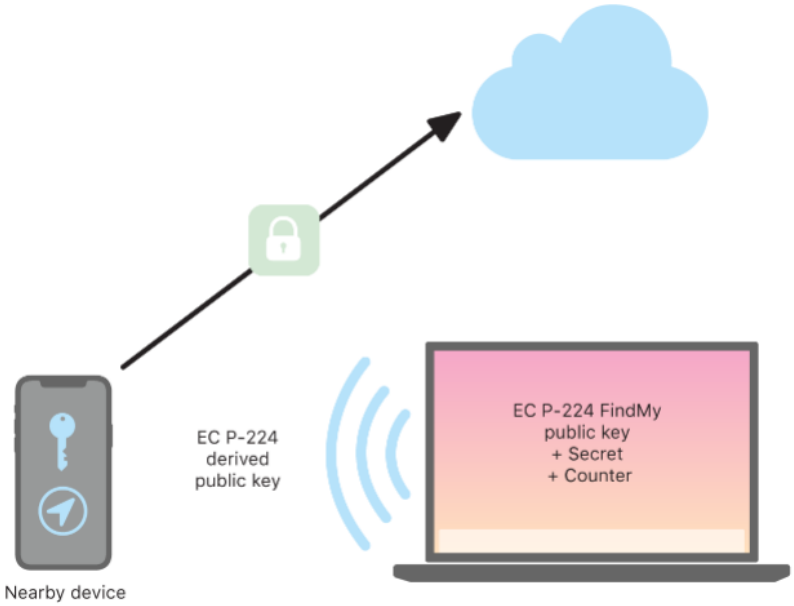


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

When a device goes missing and can't connect to Wi-Fi or cellular — for example, a MacBook Pro is left on a park bench — it begins periodically broadcasting the derived public key P_i for a limited period of time in a Bluetooth payload. By using P-224, the public key representation can fit into a single Bluetooth payload. The surrounding devices can then help in the finding of the offline device by encrypting their location to the public key. Approximately every 15 minutes, the public key is replaced by a new one using an incremented value of the counter and the process above so that the user can't be tracked by a persistent identifier. The derivation mechanism is designed to prevent the various public keys P_i from being linked to the same device.

Exhibit 12, https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

118. For example, within Find My a user may register their Apple devices such that they

may keep them located when they are nearby, by using the Find My App. As illustrated below, Find My also provides an "offline finding" mode wherein user's lost Apple devices (iPhones, iPads, Macs, Apple Watches, AirPods, Apple Pencil, and Apple Vision Pro) that are registered within the Find My network for offline finding can be found with the help of other devices (*e.g.*, iPhones, iPads, Macs).

119. For a further example, the mobile station is an iPhone registered within Find My "offline finding" and helping to find a missing Apple device that is offline and is part of the Find My network. The missing Apple device that is offline and is part of the Find My network for offline finding is a radio communication defining device.

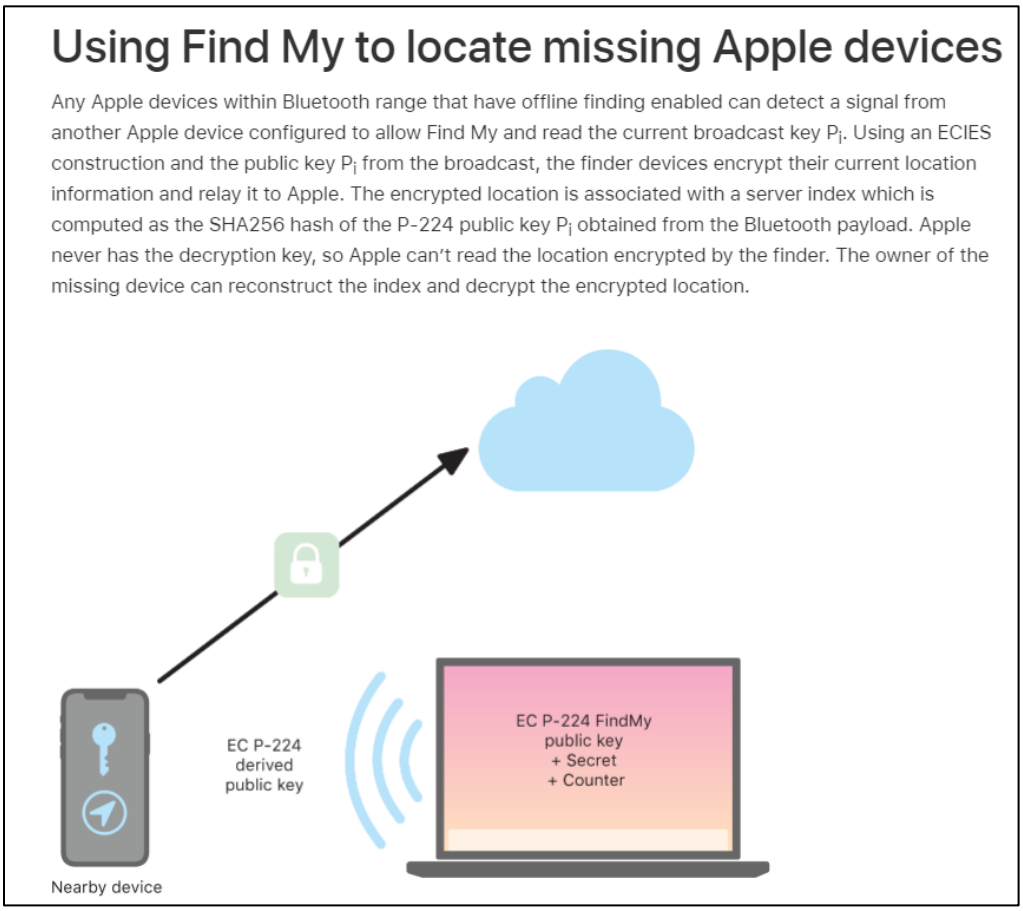


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

120. For example, if an Apple device that is part of the Find My network for offline finding (*i.e.*, a radio communication defining device) has gone offline, it starts emitting a Bluetooth Low Energy signal (*i.e.*, a distinctive defining signal) that can then be picked up by any Apple device that is part of the Find My network for offline finding.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF

Exhibit 13, at 1, Introduction.

6 Apple Offline Finding in Detail

This section describes and discusses the technical details of Apple's OF system. In reference to Fig. 1, we (1) explain the involved cryptography and the key exchange during initial device pairing, and then explain the protocols implementing (2) *losing*, (3) *finding*, (4) *searching* for devices.

In short, devices and accessories in lost mode send out BLE advertisements containing a public key. Finder devices receive them, encrypt their location by using the public key, and upload a report to Apple's servers. This results in an end-to-end encrypted location report that cannot be read by Apple or any other third-party that does not have access to the owner's private keys.

Id., at 5, § 6.

121. For example, Find My finding service involves the use of a mobile station (a *finder* device) and a BLE radio communication defining device (a *lost* device) that transmits a BLE distinctive defining signal (a unique beacon).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Id., at 3, § 3.

6.3 Finding

All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.

Generating Reports. The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

Id., at 6, § 6.3.

122. The Accused Products perform electronically storing in one or more memories, data capable of linking the mobile station to the first and second special areas, the data including a first checking data of the first radio communication defining device, a second checking data of the second radio communication defining device, and a first identifier related to the mobile station, transmitting via a mobile telephone network to the mobile station at least a portion of the first checking data, and transmitting via the mobile telephone network to the mobile station at least a portion of the second checking data. For example, the mobile station observes a channel corresponding to the offline finding service BLE signals transmission and process any received signal to determine whether or not it is receiving an offline finding service defining signal that comprises an offline finding service identifier. If the signal comprises an offline finding service identifier, at that point it is a defining signal for the mobile station. A processor within the mobile station processes any received defining signal and uses data previously stored in the mobile station (*i.e.*, checking data), to determine whether or not the BLE defining signal received is a distinctive defining signal that at least partially defines the offline finding service special area. If the mobile station determines that it is receiving a distinctive defining signal, it consequently identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines

it, as detailed below). Within Find My, every Apple device enabled for "offline finding" is converted into a receiver and locator, which effectively crowdsources the search of a missing device. Any device registered within Find My for "offline finding" becomes a Find Node of the Find My network and may receive and process the offline finding BLE defining signals from lost Apple devices.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1.

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, https://www.apple.com/icloud/find-my/

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

123. For example, the special area can be defined by the area covered by the Bluetooth distinctive defining signals of all the radio communication defining devices that are part of the Find My network for offline finding and are in an offline status at a given time. So, the special area is a dynamic-crowdsourced special area. The area covered by a given Bluetooth distinctive defining signal from a lost radio communication defining device that is in an offline status at least partly defines the special area. A user can make their Apple devices join the Find My network by using the Find My App. As shown below, a user can register various Apple devices for offline finding. The user can locate the devices by using the Find My map.

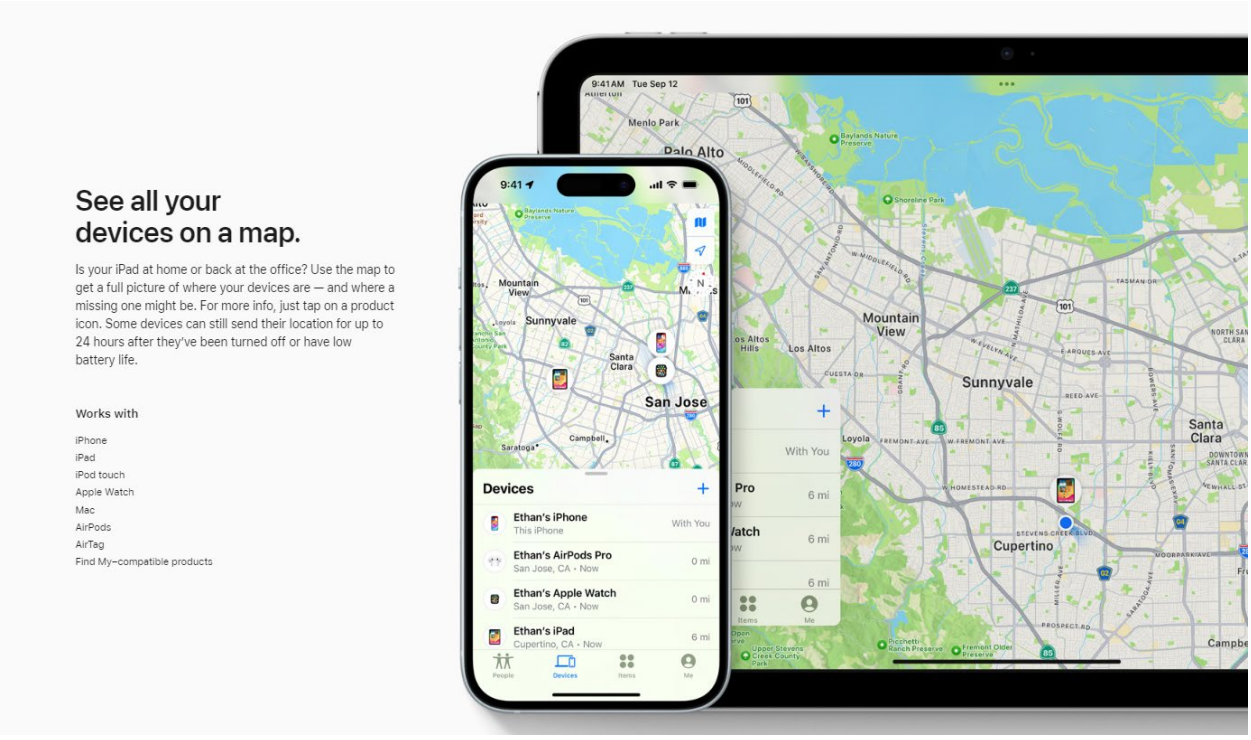


Exhibit 8, https://www.apple.com/icloud/find-my/

124. For example, a processor within the mobile station helps in determining whether or not a received defining signal is a distinctive defining signal that at least partly defines a special area and whether or not the mobile station is present in the offline finding service special area. The mobile station further identifies that it is present within the special area (as the coverage of the

distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **Finder devices.** Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Exhibit 13, at 3, § 3.

125. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal based on receiving a packet in the OF advertisement format), the mobile station must necessarily store data related to the public key (*i.e.*, store previous obtained checking data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **6.3 Finding**
>
> All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.
>
> **Generating Reports.** The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

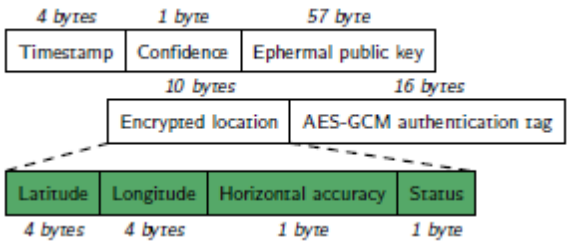


Fig. 2. Binary format of a location report.

ing the algorithm described in § 6.1. Finally, the finder creates a complete location report, including the current timestamp (in seconds since January 1, 2001), the ephemeral public key d', the encrypted message, and the AES-GCM authentication tag as shown in Fig. 2.

Exhibit 13, at 6-7, § 6.3.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0FBAE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Id., at 7, § 6.3.

126. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal with the OF advertisement), the mobile station must necessarily store data related to the location report (*i.e.*, store previous obtained checking data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station sends to a mobile telephone network, and the network routes to the Apple servers (Apple is a provider of presence related services), a signal that identifies that the mobile station is nearby the missing device that is part of the Find My network (*i.e.*, it is present in the special area). Further, when nearby the lost radio communication defining device, the mobile station receives the distinctive defining signal. The mobile station is able to identify that the received defining signal is distinctive and to determine that it is present within the crowdsourced offline finding special area, as detailed above. The BLE distinctive signal must include a device identifier, such that the Find My services related to the found device can be later provided in connection to that device, as elaborated below.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

127. The Accused Products perform receiving from the mobile station via the mobile telephone network a first updating signal uncorrelated to any mobile station phone call establishment that identifies the mobile station's presence in at least the first special area, and receiving from the mobile station via the mobile telephone network a second updating signal uncorrelated to any mobile station phone call establishment that identifies the mobile station's presence in at least the second special area, the first updating signal including a second identifier related to the mobile station, the second updating signal including a third identifier related to the mobile station. For example, the mobile station sends a signal about the mobile station's presence in the special area via a mobile telephone network to the Apple iCloud servers (Apple is the provider of Find My "offline finding" presence related services), the signal including the mobile

station's location. When sending the presence updating signal, the mobile station is not necessarily within Wi-Fi coverage. In that case, the mobile station must send its updating signal via a mobile telephone network. The presence signal must also include the device identifier of the first and/or second found device, because the Find My network needs this to subsequently provide related presence related services (*e.g.*, the notification to the device owner about the found device location).

> **Advertising Interval.** The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

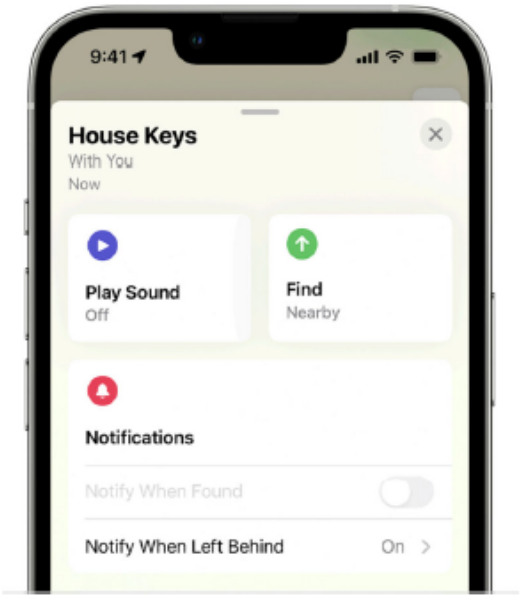
Exhibit 13, at 6, § 6.2.

> **Set up and use Notify When Left Behind in the Find My app**
>
> With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

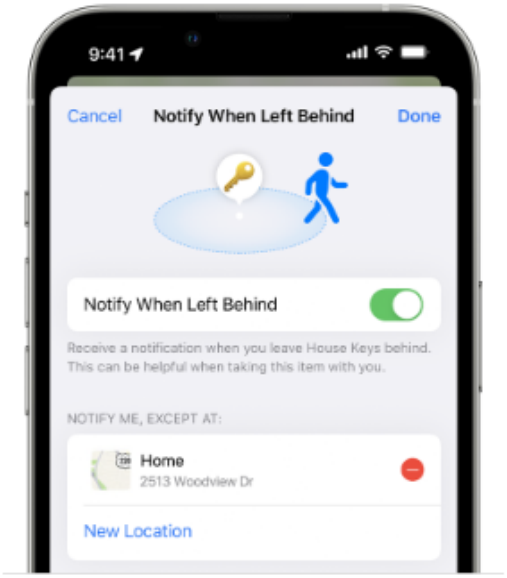
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Id.

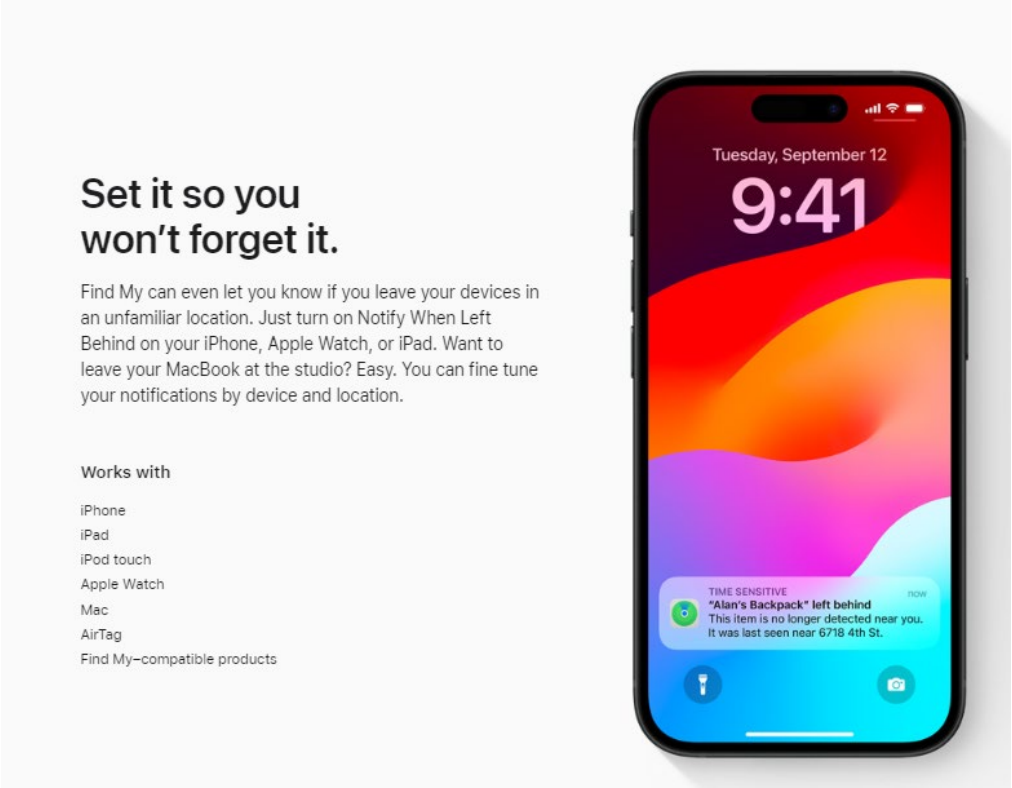


Exhibit 8, https://www.apple.com/icloud/find-my/

128. The Accused Products perform enabling or disabling by use of the one or more processing devices, a presence related service based upon the mobile station's presence or non-presence in the first special area, and enabling or disabling by use of the one or more processing devices, a presence related service based upon the mobile station's presence or non-presence in the second special area. For example, the Apple iCloud servers (Apple is the provider of presence related services) receives the presence updating signal and uses it to provide presence related services (*e.g.*, displaying to the first "found" device's owner, the device's location on a map, as illustrated below, in connection to a found device (and similarly for the second found device); or sending a notification to a device of the owner of the first or second lost device indicating that it has been found).

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Exhibit 13, at 6, § 6.2.

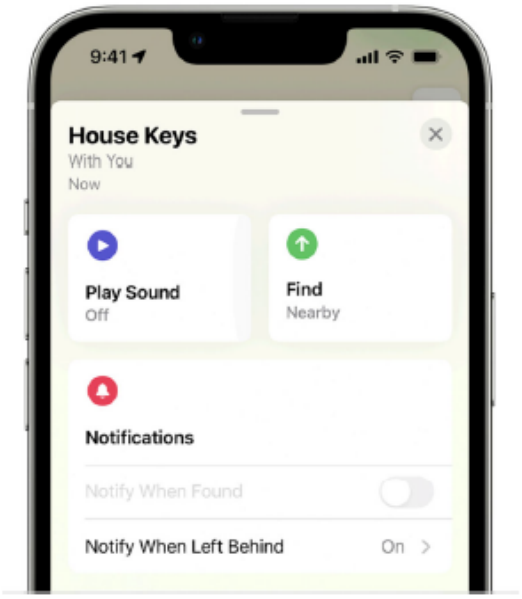
Set up and use Notify When Left Behind in the Find My app

With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

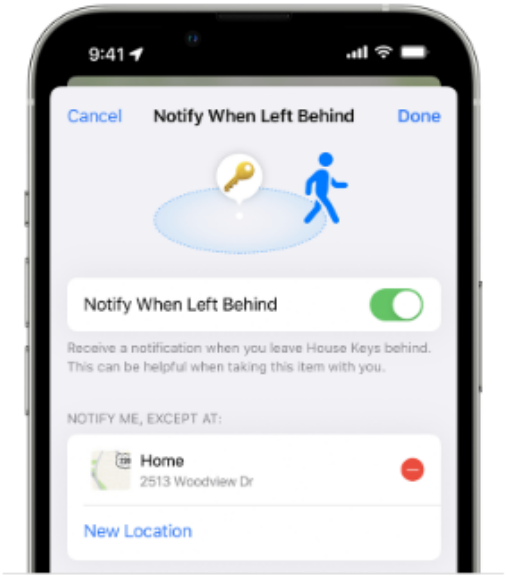
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Id.

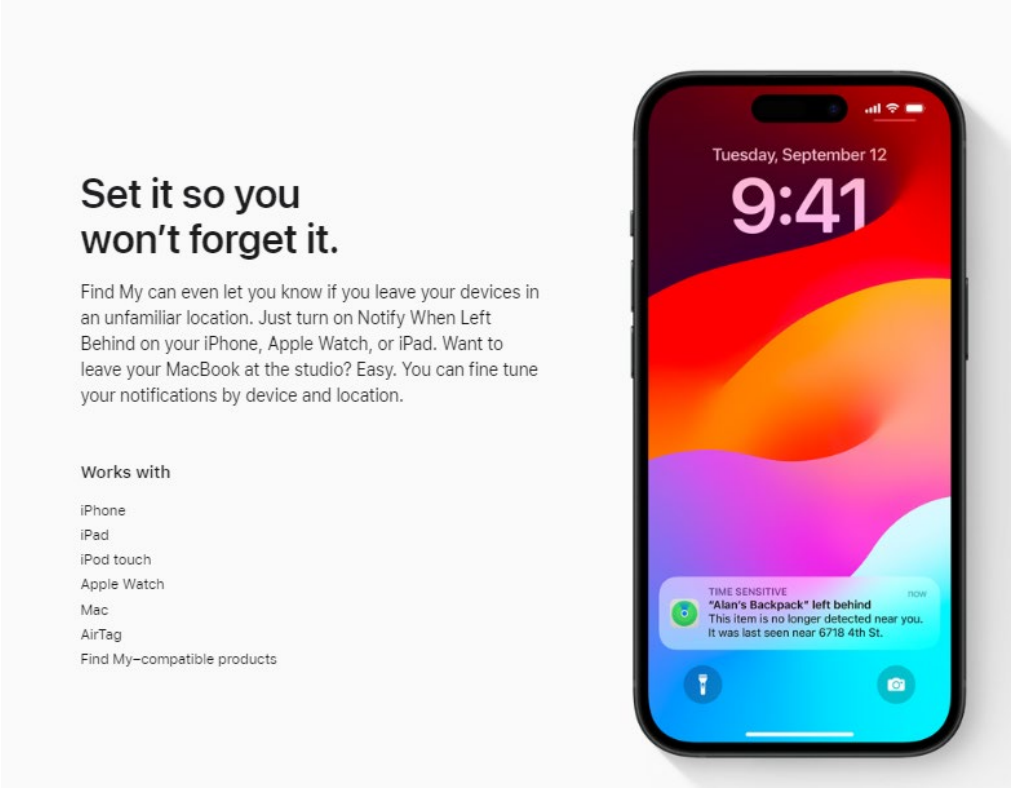


Exhibit 8, https://www.apple.com/icloud/find-my/

129. The Accused Products perform deriving from the first updating signal by one or more processing devices having access to at least a portion of the data whether or not the mobile station is present in the first special area, and deriving from the second updating signal by the one or more processing devices whether or not the mobile station is present in the second special area. For example, a mobile station (a *finder* device) identifies that it is present within the area of coverage of a device that is lost (*e.g.*, the first and/or second radio communication defining device) and is part of the Find My finding network and sends to a vendor controller server (*i.e.*, to the Apple iCloud servers in the case of Apple devices and Apple Find My offline finding ecosystem) an updating signal indicating the presence status (the signal including unique beacon data received from the lost first/second device via BLE, together with the location of the device).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Id., at 3, § 3.

130. The mobile station identifier of the mobile station is included within the updating signal sent to the Apple iCloud.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

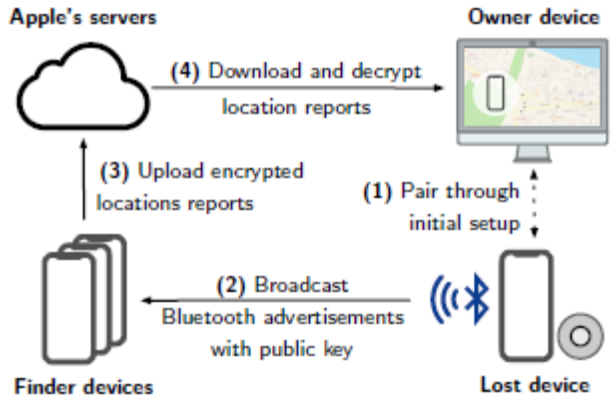


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

131. For example, the sending of the updating signal is uncorrelated to any mobile station phone call establishment. The updating signal is sent when the mobile station enters into the offline finding special area and starts receiving the first and/or second distinctive defining signals from the first/second lost radio communication defining device. Also, if the mobile station remains nearby the first and/or second lost device (*i.e.*, remains in the special area), it periodically sends a presence updating signal via mobile telephone network to the Apple iCloud servers, as further elaborated below. The mobile station stores in a local database the determination performed by the mobile station about its presence in the special area, in relation to each found device public key identifier (*i.e.*, in connection to at least the first and/or second radio communication defining devices). After storage, the mobile station sends a presence updating signal containing the (each) lost device public key and the location to the Apple iCloud servers. If it is the first (recent) reporting by the mobile station about its presence in the special area, the presence updating signal

is then related to the mobile station entering into the special area.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

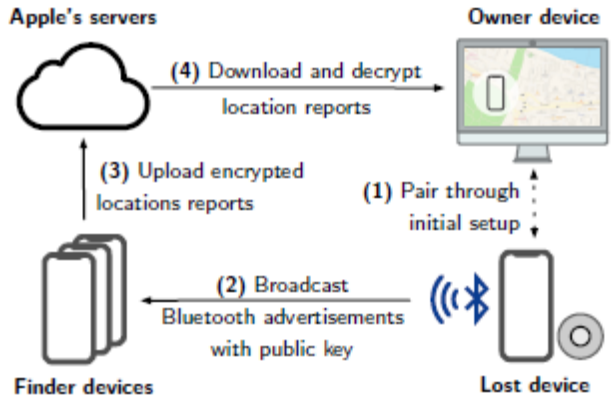


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

132. For example, the mobile station receives an acknowledgment about the presence updating signal having been received in the Apple iCloud servers (via a mobile telephone network), as indicated in the image below. As also indicated in the image below, the presence determination process (*i.e.*, the scanning and filtering of OF advertisements in a certain format) is then reinitiated. If the mobile station remains in the special area in connection to a lost device it has already reported (*i.e.*, the first and/or second radio communication defining devices), then it may send (after 15 minutes) a new updating signal (*i.e.*, a second updating signal) related to the mobile station presence in the special area (in connection to that lost device): *i.e.*, the presence updating signal is then related to the mobile station remaining in the special area.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

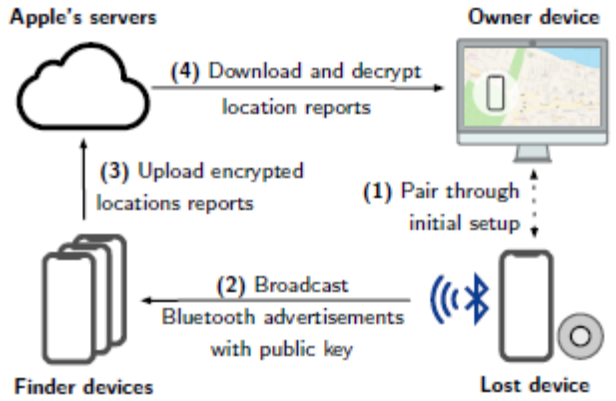


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

133. For example, the mobile station stores in a local database the determination performed by the mobile station about its presence in the special area, in connection to the (each) found device public key (*e.g.*, in connection to at least the first and/or second radio communication defining devices). After the storage, the mobile station sends a presence updating signal containing the recently found device(s), public key(s), and the location to the Apple iCloud servers). If it is the first (recent) reporting by the mobile station about the mobile station presence in the special area, the presence updating signal is then related to the mobile station entering into the special area.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0F8AE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Exhibit 13, at 7, § 6.3.

134. Defendant has and continues to indirectly infringe one or more claims of the '922 Patent by inducing infringement by others, such as Defendant's customers and end-users, in this District and elsewhere in the United States. For example, Defendant's customers and end-users directly infringe, either literally or under the doctrine of equivalents, through their use of the inventions claimed in the '922 Patent. Defendant induces this direct infringement through its

affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products, and providing instructions, documentation, and other information to customers and end-users suggesting that they use the Accused Products in an infringing manner, including technical support, marketing, product manuals, advertisements, and online documentation. *See, e.g.*, Exhibit 8, https://www.apple.com/icloud/find-my/ ("Find My"); *see also, e.g.,* Exhibit 14, available at https://support.apple.com/en-us/104978 ("Find your lost Apple device or AirTag with FindMy"); Exhibit 14, https://support.apple.com/en-us/102648 ("Set up Find My on your iPhone, iPad, or Mac"); Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind. ("Set up and use Notify When Left Behind in the Find My App").

135. Because of Defendant's inducement, Defendant's customers and end-users use the Accused Products in a way Defendant intends and they directly infringe the '922 Patent. Defendant performs these affirmative acts with knowledge of the '922 Patent and with the intent, or willful blindness, that the induced acts directly infringe the '922 Patent.

136. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the '922 Patent, as provided by 35 U.S.C. § 271(c), by contributing to direct infringement by others, such as customers and end-users, in this District and elsewhere in the United States. Defendant's affirmative acts of selling and offering to sell the '922 Accused Products in this District and elsewhere in the United States and causing the '922 Accused Products to be manufactured, used, sold, and offered for sale contribute to others' use and manufacture of the Accused Products, such that the '922 Patent is directly infringed by others. The accused components within the Accused Products including, but not limited to, software manufactured by Defendant, are material to the invention of the '922 Patent, are not staple articles or commodities

of commerce, have no substantial non-infringing uses, and are known by Defendant to be especially made or adapted for use in the infringement of the ’922 Patent. Defendant performs these affirmative acts with knowledge of the ’922 Patent and with intent, or willful blindness, that they cause the direct infringement of the ’922 Patent.

137. Because of Defendant’s direct and indirect infringement of the ’922 Patent, ALT has suffered damages in an amount to be proved at trial.

COUNT V
(Infringement of the ’030 Patent)

138. Paragraphs 1 through 31 are incorporated by reference as if fully set forth herein.

139. ALT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’030 Patent.

140. Defendant has and continues to directly infringe the claims of the ’030 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, at least by performing each and every limitation of one or more method claims of the ’030 Patent by using the Accused Products.

141. The Accused Products practice the method of at least claim 1 of the ’030 Patent: A method associated with a provider of presence related services in connection with the use of a mobile station and at least a first radio communication defining device that transmits a first distinctive defining signal, the first distinctive defining signal at least partly defines a first special area by its coverage, the method comprising: electronically storing in one or more memories data capable of linking the mobile station to the first special area, the data including a checking data of the first radio communication defining device and a first identifier related to the mobile station, transmitting via a mobile telephone network to the mobile station at least a portion of the checking data, receiving from the mobile station via the mobile telephone network an updating signal

uncorrelated to any mobile station phone call establishment that identifies the mobile station's presence in at least the first special area, the updating signal including a second identifier related to the mobile station, deriving from the updating signal by one or more processing devices having access to at least a portion of the data whether or not the mobile station is present in the first special area; and enabling or disabling by use of the one or more processing devices a presence related service based upon the mobile station's presence or non-presence in the first special area.

142. The Accused Products perform a method associated with a provider of presence related services in connection with the use of a mobile station and at least a first radio communication defining device that transmits a first distinctive defining signal, the first distinctive defining signal at least partly defines a first special area by its coverage, the method comprising electronically storing in one or more memories data capable of linking the mobile station to the first special area, the data including a checking data of the first radio communication defining device and a first identifier related to the mobile station, transmitting via a mobile telephone network to the mobile station at least a portion of the checking data. For example, the mobile station observes a channel corresponding to the offline finding service BLE signals transmission and processes any received signal to determine whether or not it is receiving an offline finding service defining signal that comprises an offline finding service identifier. If the signal comprises an offline finding service identifier, at that point it is a defining signal for the mobile station. The mobile station processes any received defining signal and uses data previously stored in the mobile station (*i.e.*, checking data), to determine whether or not the BLE defining signal received is a distinctive defining signal that at least partially defines the offline finding service special area. If the mobile station determines that it is receiving a distinctive defining signal, it consequently identifies that it is present within the special area (as the coverage of the distinctive defining signal

party defines it, as detailed below). Within Find My, every Apple device enabled for "offline finding" is converted into a receiver and locator, which effectively crowdsources the search of a missing device. Any device registered within Find My for "offline finding" becomes a Find Node of the Find My network and may receive and process the offline finding BLE defining signals from lost Apple devices.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1.

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, https://www.apple.com/icloud/find-my/

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

143. For example, the special area can be defined by the area covered by the Bluetooth distinctive defining signals of all the radio communication defining devices that are part of the Find My network for offline finding and are in an offline status at a given time. So, the special area is a dynamic-crowdsourced special area. The area covered by a given Bluetooth distinctive defining signal from a lost radio communication defining device that is in an offline status at least partly defines the special area. A user can make their Apple devices join the Find My network by using the Find My App. As shown below, a user can register various Apple devices for offline finding. The user can locate the devices by using the Find My map.

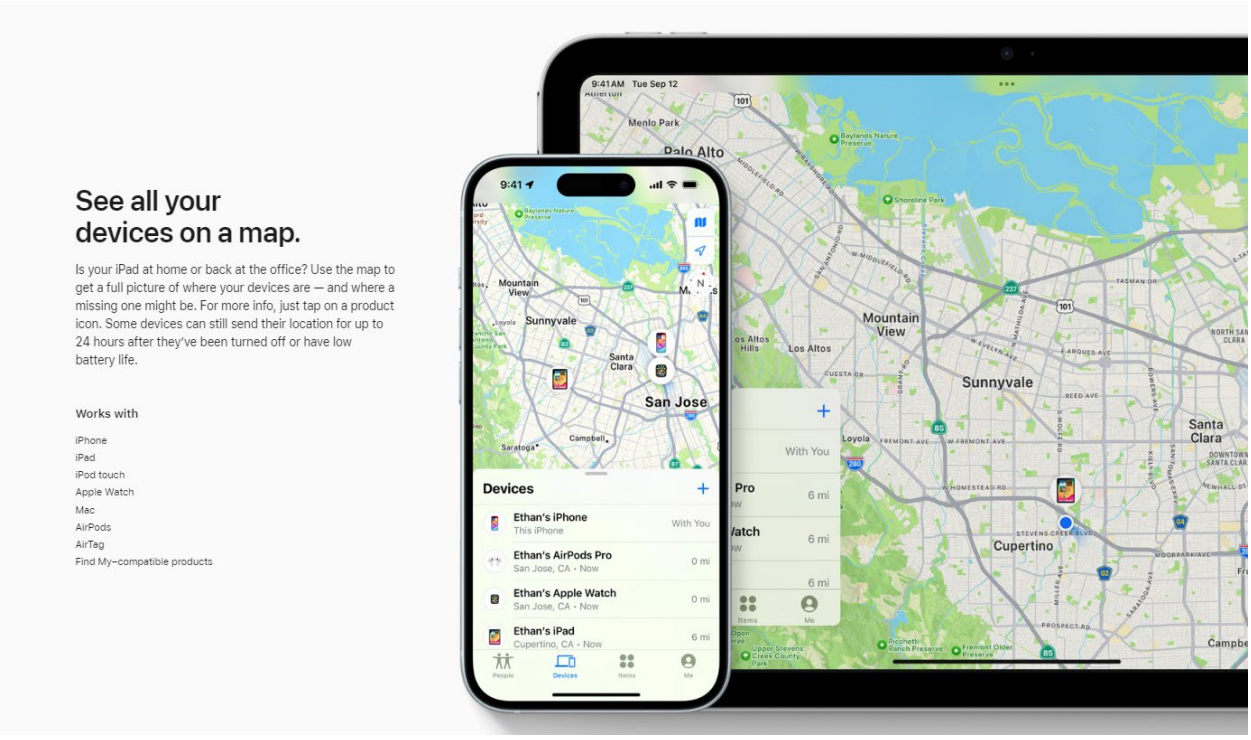


Exhibit 8, https://www.apple.com/icloud/find-my/

144. For example, a mobile device can help the mobile station in determining whether or not a received defining signal is a distinctive defining signal that at least partly defines a special area and whether or not the mobile station is present in the offline finding service special area. The mobile station further identifies that it is present within the special area (as the coverage of the

distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **Finder devices.** Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Exhibit 13, at 3, § 3.

145. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal based on receiving a packet in the OF advertisement format), the mobile station must necessarily store data related to the OF advertisement (*i.e.*, store previous obtained checking data) and use the data to perform the filtering. The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **6.3 Finding**
>
> All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.
>
> **Generating Reports.** The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

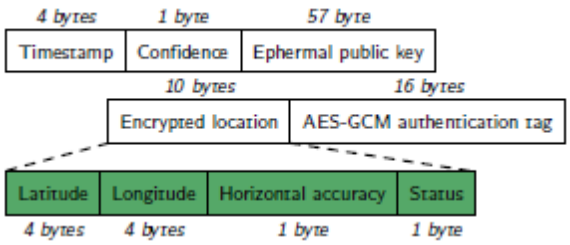


Fig. 2. Binary format of a location report.

ing the algorithm described in § 6.1. Finally, the finder creates a complete location report, including the current timestamp (in seconds since January 1, 2001), the ephemeral public key d', the encrypted message, and the AES-GCM authentication tag as shown in Fig. 2.

Exhibit 13, at 6-7, § 6.3.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0FBAE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Id., at 7, § 6.3.

146. For example, the mobile station scans a BLE channel and is able to filter advertisements in an OF advertisement. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal with the OF advertisement), the mobile station must necessarily store data related to the location report (*i.e.*, store previous obtained checking data) and use the data to perform the filtering. The mobile station sends to a mobile telephone network, and the mobile telephone network routes to the Apple iCloud servers (Apple is a provider of presence related services), a signal that identifies that the mobile station is nearby the missing device that is part of the Find My network (*i.e.*, it is present in the special area). Further, when nearby the lost radio communication defining device, the mobile station receives the distinctive defining signal. The mobile station is able to identify that the received defining signal is distinctive and to determine that it is present within the crowdsourced offline finding special area, as detailed above. The BLE distinctive signal must include a device identifier such that the Find My services related to the found device can be later provided in connection to that device, as elaborated below.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

147. The Accused Products perform receiving from the mobile station via the mobile telephone network an updating signal uncorrelated to any mobile station phone call establishment that identifies the mobile station's presence in at least the first special area, the updating signal including a second identifier related to the mobile station, deriving from the updating signal by one or more processing devices having access to at least a portion of the data whether or not the mobile station is present in the first special area; and enabling or disabling by use of the one or more processing devices a presence related service based upon the mobile station's presence or non-presence in the first special area. For example, the mobile station sends a signal about the mobile station's presence in the special area via a mobile telephone network to the Apple iCloud servers (Apple is the provider of Find My "offline finding" presence related services), the signal

including the mobile station's location. When sending the presence updating signal, the mobile station is not necessarily within Wi-Fi coverage. In that case, the mobile station must send its updating signal via a mobile telephone network. The presence signal must also include the device identifier of the first and/or second found device, because the Find My network needs this to subsequently provide related presence related services (*e.g.*, the notification to the device owner about the found device location). The images below indicate that once a mobile station has identified that it is nearby, a lost device that is in an offline status, the location of the mobile station and the device identifier of the lost device are collected to provide the Find My service (this information is sent to the Apple servers within the updating signal, as it is required to allow the device owner to locate the device, once found by the mobile station).

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Exhibit 13, at 6, § 6.2.

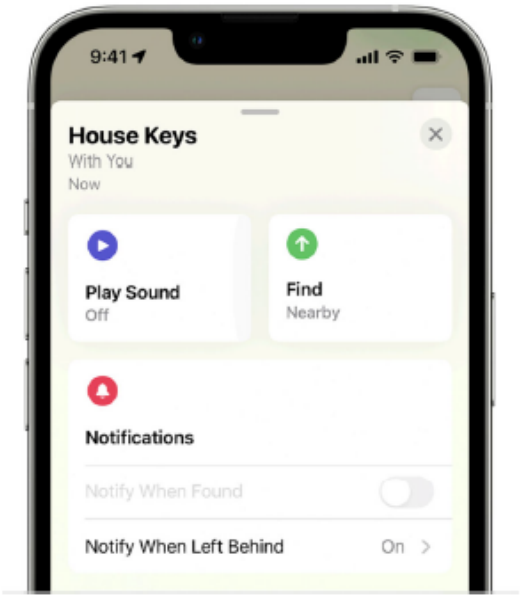
Set up and use Notify When Left Behind in the Find My app

With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

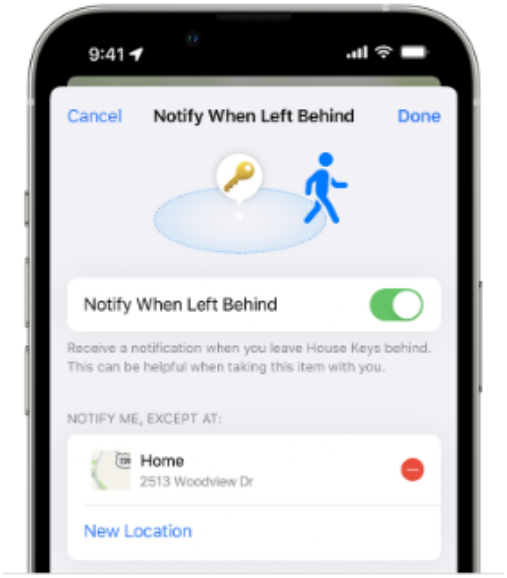
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Id.

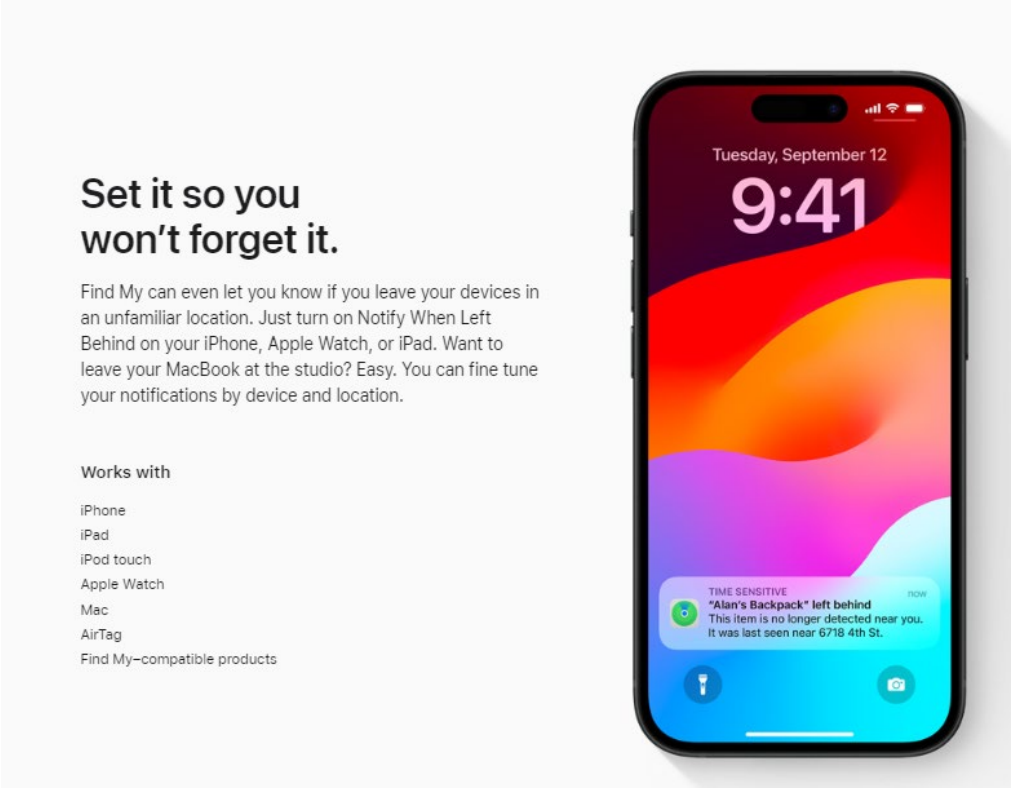


Exhibit 8, https://www.apple.com/icloud/find-my/

148. For example, the Apple iCloud servers (Apple is the provider of presence related services), receives the presence updating signal, and uses it to provide presence related services (*e.g.*, displaying to the first "found" device's owner, the device's location on a map, as illustrated below in connection to a found Apple device (and similarly for the second found device); or sending a notification to a device of the owner of the first or second lost device indicating that it has been found) (*i.e.*, enabling or disabling…a presence related service based upon the mobile station's presence or non-presence in the first special area).

> **Advertising Interval.** The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Exhibit 13, at 6, § 6.2.

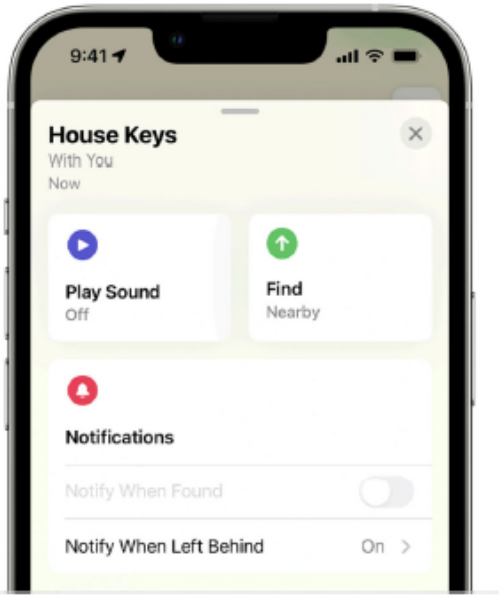
Set up and use Notify When Left Behind in the Find My app

With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

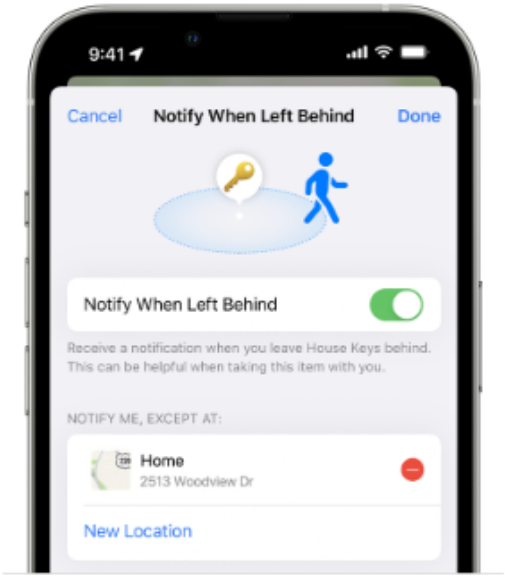
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Id.

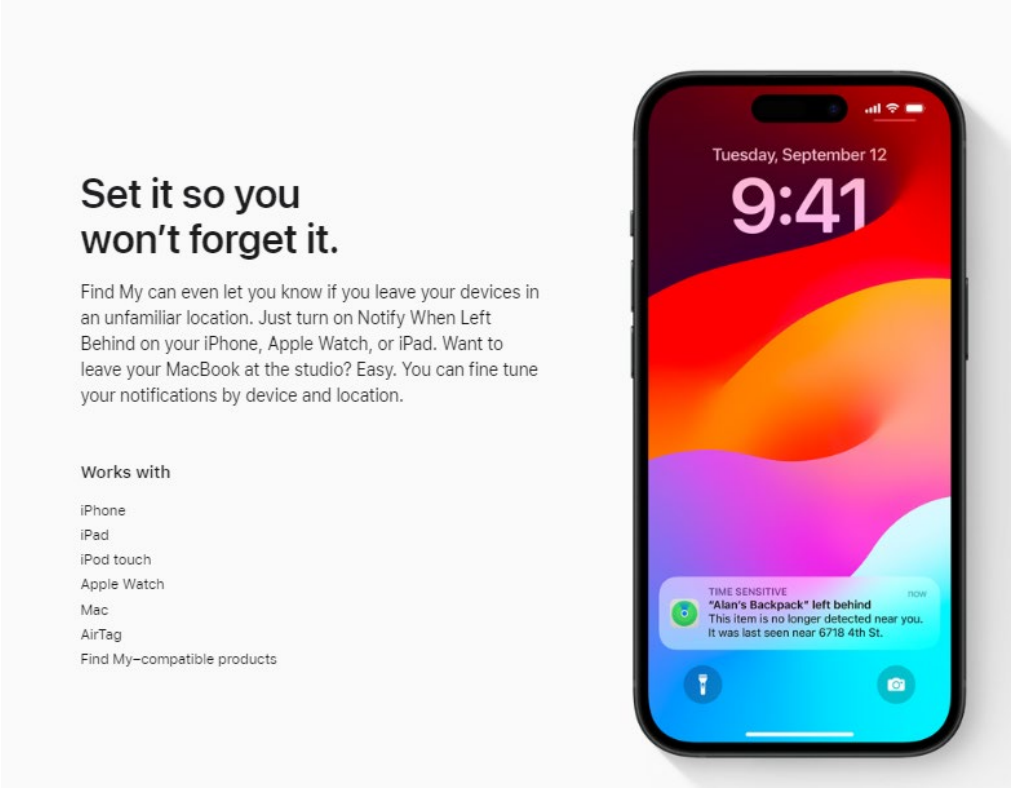


Exhibit 8, https://www.apple.com/icloud/find-my/

149. For example, a mobile station (a *finder* device) identifies that it is present within the area of coverage of a device that is lost (*e.g.*, the first and/or second radio communication defining device) and is part of the Find My finding network and sends to a vendor controller server (*i.e.*, to the Apple iCloud servers in the case of Apple devices and Apple Find My offline finding ecosystem) an updating signal indicating the presence status (the signal including unique beacon data received from the lost first/second device via BLE, together with the location of the device).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Id., at 3, § 3.

150. The mobile station identifier of the mobile station is included within the updating signal sent to the Apple iCloud.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

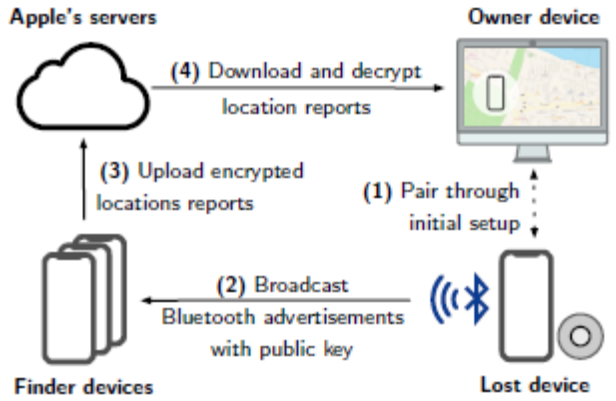


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

> for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].
>
> **Advertising Interval.** The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

151. For example, the sending of the updating signal is uncorrelated to any mobile station phone call establishment. The updating signal is sent when the mobile station enters into the offline finding special area and starts receiving the first and/or second distinctive defining signals from the first/second lost radio communication defining device. Also, if the mobile station remains nearby the first and/or second lost device (*i.e.*, remains in the special area), it periodically sends a presence updating signal via mobile telephone network to the Apple iCloud servers, as further elaborated below. The mobile station stores in a local database the determination performed by the mobile station about its presence in the special area, in relation to each found device public key identifier (*i.e.*, in connection to at least the first and/or second radio communication defining devices). After storage, the mobile station sends a presence updating signal containing the (each) lost device public key and the location to the Apple iCloud servers. If it is the first (recent) reporting by the mobile station about its presence in the special area, the presence updating signal

is then related to the mobile station entering into the special area.

> **Uploading Reports.** Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0F8AE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Exhibit 13, at 7, § 6.3.

152. For example, the mobile station receives an acknowledgment about the presence updating signal having been received in the Apple iCloud servers (via a mobile telephone network), as indicated in the image below. As also indicated in the image below, the presence determination process (*i.e.*, the scanning and filtering of OF advertisements in a certain format) is

then reinitiated. If the mobile station remains in the special area in connection to a lost device it has already reported (*i.e.*, the first and/or second radio communication defining devices), then it may send (after 15 minutes) a new updating signal related to the mobile station presence in the special area (in connection to that lost device): *i.e.*, the presence updating signal is then related to the mobile station remaining in the special area.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

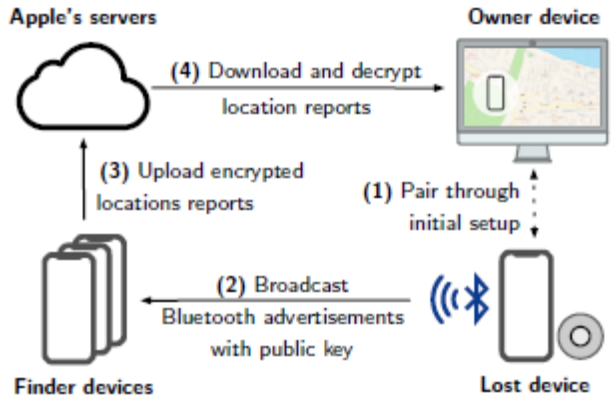


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Id., at 6, § 6.2.

153. For example, the mobile station stores in a local database the determination performed by the mobile station about its presence in the special area, in connection to the (each) found device public key identifier (*e.g.*, in connection to at least the first and/or second radio communication defining devices). After the storage, the mobile station sends a presence updating signal containing the recently found device(s), public key(s), and the location to the Apple iCloud servers). If it is the first (recent) reporting by the mobile station about the mobile station presence in the special area, the presence updating signal is then related to the mobile station entering into the special area.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0F8AE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Exhibit 13, at 7, § 6.3.

154. Defendant has and continues to indirectly infringe one or more claims of the '030 Patent by inducing infringement by others, such as Defendant's customers and end-users, in this District and elsewhere in the United States. For example, Defendant's customers and end-users directly infringe, either literally or under the doctrine of equivalents, through their use of the inventions claimed in the '030 Patent. Defendant induces this direct infringement through its

affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products, and providing instructions, documentation, and other information to customers and end-users suggesting that they use the Accused Products in an infringing manner, including technical support, marketing, product manuals, advertisements, and online documentation. *See, e.g.*, Exhibit 8, https://www.apple.com/icloud/find-my/ ("Find My"); *see also, e.g.,* Exhibit 14, available at https://support.apple.com/en-us/104978 ("Find your lost Apple device or AirTag with FindMy"); Exhibit 14, https://support.apple.com/en-us/102648 ("Set up Find My on your iPhone, iPad, or Mac"); Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind. ("Set up and use Notify When Left Behind in the Find My App").

155. Because of Defendant's inducement, Defendant's customers and end-users use the Accused Products in a way Defendant intends and they directly infringe the '030 Patent. Defendant performs these affirmative acts with knowledge of the '030 Patent and with the intent, or willful blindness, that the induced acts directly infringe the '030 Patent.

156. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the '030 Patent, as provided by 35 U.S.C. § 271(c), by contributing to direct infringement by others, such as customers and end-users, in this District and elsewhere in the United States. Defendant's affirmative acts of selling and offering to sell the '030 Accused Products in this District and elsewhere in the United States and causing the '030 Accused Products to be manufactured, used, sold, and offered for sale contribute to others' use and manufacture of the Accused Products, such that the '030 Patent is directly infringed by others. The accused components within the Accused Products including, but not limited to, software manufactured by Defendant, are material to the invention of the '030 Patent, are not staple articles or commodities

of commerce, have no substantial non-infringing uses, and are known by Defendant to be especially made or adapted for use in the infringement of the ’030 Patent. Defendant performs these affirmative acts with knowledge of the ’030 Patent and with intent, or willful blindness, that they cause the direct infringement of the ’030 Patent.

157. Because of Defendant’s direct and indirect infringement of the ’030 Patent, ALT has suffered damages in an amount to be proved at trial.

COUNT VI
(Infringement of the ’621 Patent)

158. Paragraphs 1 through 31 are incorporated by reference as if fully set forth herein.

159. ALT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’621 Patent.

160. Defendant has and continues to directly infringe the claims of the ’621 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, at least by performing each and every limitation of one or more method claims of the ’621 Patent by using the Accused Products.

161. The Accused Products practice the method of at least claim 1 of the ’621 Patent: A method associated with a provider of presence related services in connection with the use of a mobile station that is operable within a mobile telephone network, and at least a first radio communication defining device that transmits a first distinctive defining signal, the first distinctive defining signal at least partly defines a special area by its coverage, the provider of presence related services having one or more servers, the method comprising: electronically storing in the one or more servers of the provider of presence related services data capable of linking the mobile station to the special area, the data including a checking data of the first radio communication defining device and an identifier related to the mobile station, the provider of presence related services

being different than the mobile telephone network, receiving in the one or more servers of the provider of presence related services from the mobile station via the mobile telephone network an updating signal uncorrelated to any mobile station phone call establishment that identifies the mobile station's presence in the special area, the one or more servers of the provider of presence related services deriving from the updating signal by one or more processing devices having access to at least a portion of the data whether or not the mobile station is present in the special area; and enabling or disabling by use of the one or more processing devices a presence related service based upon the mobile station's presence or non-presence in the special area.

162. The Accused Products perform a method associated with a provider of presence related services in connection with the use of a mobile station that is operable within a mobile telephone network, and at least a first radio communication defining device that transmits a first distinctive defining signal, the first distinctive defining signal at least partly defines a special area by its coverage, the provider of presence related services having one or more servers. For example, Apple Find My implements a method associated with the use of a mobile station and a missing Bluetooth device that is part of the Apple Find My network for offline finding and that transmits a distinctive defining signal indicative that it is in an offline status (*i.e.*, it is lost).

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, available at https://www.apple.com/icloud/find-my/

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

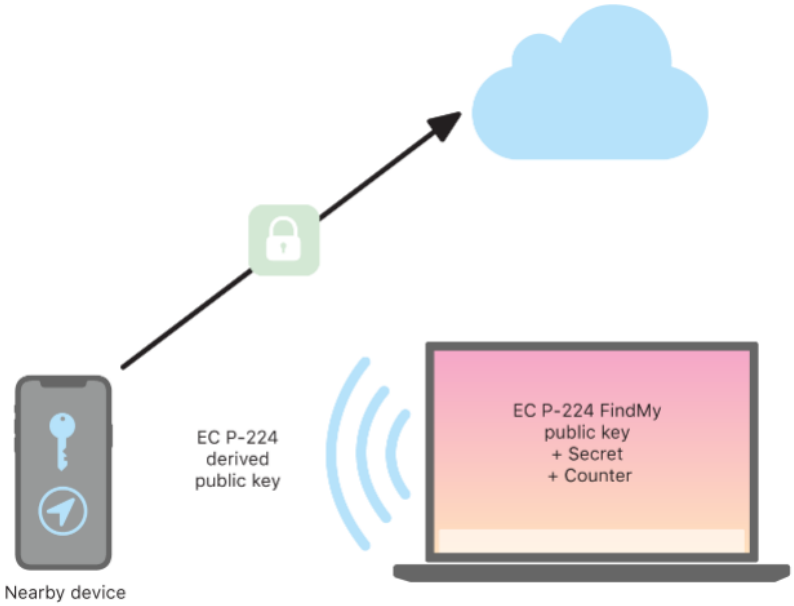


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

When a device goes missing and can't connect to Wi-Fi or cellular — for example, a MacBook Pro is left on a park bench — it begins periodically broadcasting the derived public key P_i for a limited period of time in a Bluetooth payload. By using P-224, the public key representation can fit into a single Bluetooth payload. The surrounding devices can then help in the finding of the offline device by encrypting their location to the public key. Approximately every 15 minutes, the public key is replaced by a new one using an incremented value of the counter and the process above so that the user can't be tracked by a persistent identifier. The derivation mechanism is designed to prevent the various public keys P_i from being linked to the same device.

Exhibit 12, https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

163. For example, within Find My a user may register their Apple devices, such that

they may keep them located when they are nearby, by using the Find My App. As illustrated below, Find My also provides an "offline finding" mode wherein a user's lost Apple devices (iPhones, iPads, Macs, Apple Watches, AirPods, Apple Pencil, and Apple Vision Pro) that are registered within the Find My network for offline finding can be found with the help of other devices (*e.g.*, iPhones, iPads, Macs).

164. For a further example, the mobile station is an iPhone registered within Find My "offline finding" and helps to find a missing Apple device that is offline and is part of the Find My network. The missing Apple device that is offline and is part of the Find My network for offline finding is a radio communication defining device.

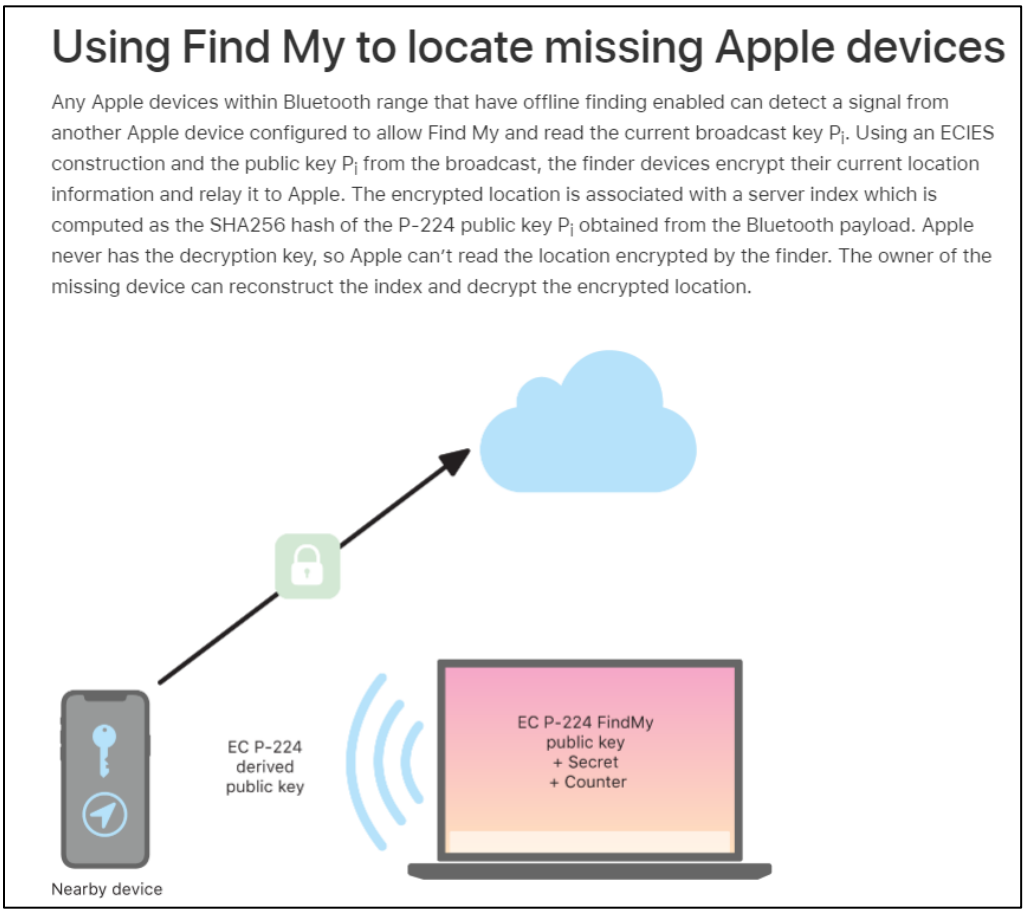


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

165. For example, if an Apple device that is part of the Find My network for offline

finding (*i.e.*, a radio communication defining device) has gone offline, it starts emitting a Bluetooth Low Energy signal (*i.e.*, a distinctive defining signal) that can then be picked up by any Apple device that is part of the Find network for offline finding.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF

Exhibit 13, at 1, Introduction.

6 Apple Offline Finding in Detail

This section describes and discusses the technical details of Apple's OF system. In reference to Fig. 1, we (1) explain the involved cryptography and the key exchange during initial device pairing, and then explain the protocols implementing (2) *losing*, (3) *finding*, (4) *searching* for devices.

In short, devices and accessories in lost mode send out BLE advertisements containing a public key. Finder devices receive them, encrypt their location by using the public key, and upload a report to Apple's servers. This results in an end-to-end encrypted location report that cannot be read by Apple or any other third-party that does not have access to the owner's private keys.

Id., at 5, § 6.

166. For example, Find My finding service involves the use of a mobile station (a *finder* device) and a BLE radio communication defining device (a *lost* device) that transmits a BLE distinctive defining signal (a unique beacon).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Id., at 3, § 3.

6.3 Finding

All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.

Generating Reports. The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

Id., at 6, § 6.3.

167. The Accused Products perform electronically storing in the one or more servers of the provider of presence related services data capable of linking the mobile station to the special area, the data including a checking data of the first radio communication defining device and an identifier related to the mobile station, the provider of presence related services being different than the mobile telephone network. For example, the mobile station observes a channel corresponding to the offline finding service BLE signals transmission and processes any received signal to determine whether or not it is receiving an offline finding service defining signal that comprises an offline finding service identifier. If the signal comprises an offline finding service identifier, at that point it is a defining signal for the mobile station. A processor within the mobile station processes any received defining signal and uses data previously stored in the mobile station (*i.e.*, checking data), to determine whether or not the BLE defining signal received is a distinctive defining signal that at least partially defines the offline finding service special area. If the mobile station determines that it is receiving a distinctive defining signal, it consequently identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it, as detailed below). Within Find My, every iPhone enabled for "offline finding" is converted into a receiver and locator, which effectively crowdsources the search of a missing device. Any

device registered within Find My for "offline finding" becomes a Find Node of the Find My network and may receive and process the offline finding BLE defining signals from lost Apple devices.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1.

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, https://www.apple.com/icloud/find-my/

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

168. For example, the special area can be defined by the area covered by the Bluetooth distinctive defining signals of all the radio communication defining devices that are part of the Find My network for offline finding and are in an offline status at a given time. So, the special area is a dynamic-crowdsourced special area. The area covered by a given Bluetooth distinctive defining signal from a lost radio communication defining device that is in an offline status at least partly defines the special area. A user can make their Apple devices join the Find My network by using the Find My App. As shown below, a user can register various Apple devices for offline finding. The user can locate the devices by using the Find My map.

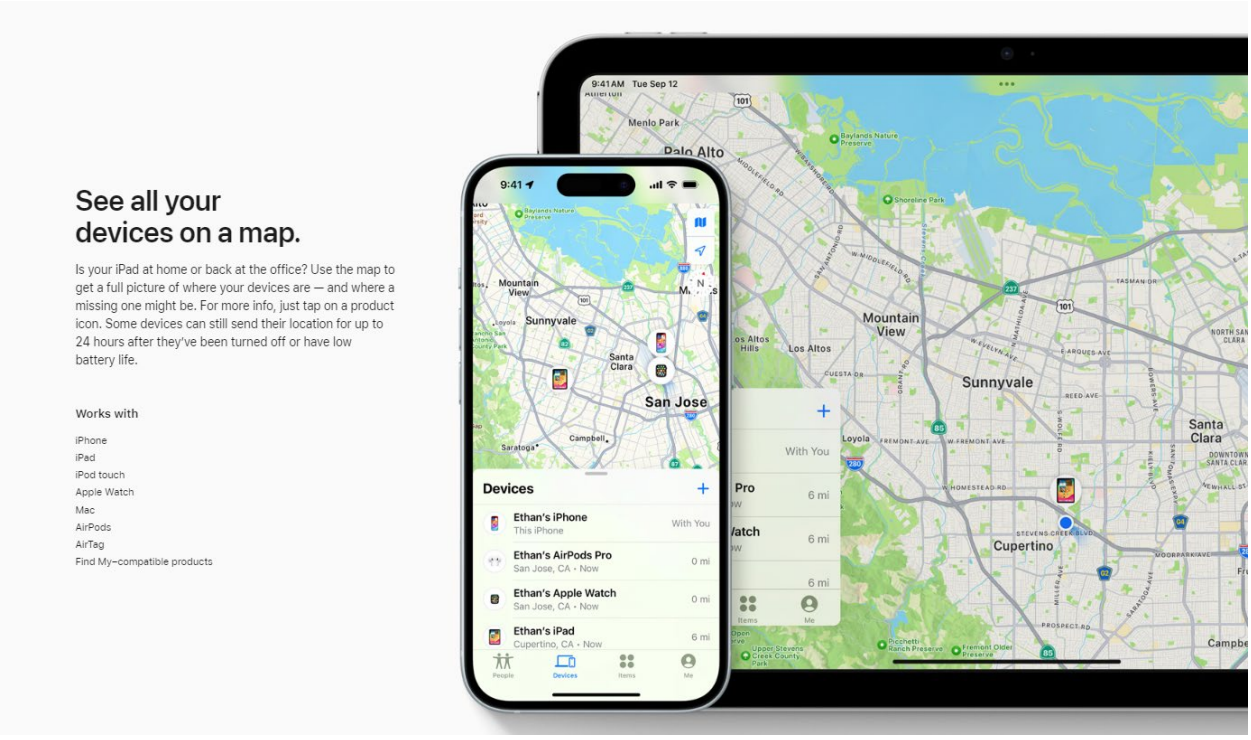


Exhibit 8, https://www.apple.com/icloud/find-my/

169. For example, a processor within a mobile device can help the mobile station in determining whether or not a received defining signal is a distinctive defining signal that at least partly defines a special area and whether or not the mobile station is present in the offline finding service special area. The mobile station further identifies that it is present within the special area

(as the coverage of the distinctive defining signal partly defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **Finder devices.** Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Exhibit 13, at 3, § 3.

170. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal based on receiving a packet in the OF advertisement format), the mobile station must necessarily store data related to the OF advertisement (*i.e.*, store previous obtained checking data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **6.3 Finding**
>
> All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.
>
> **Generating Reports.** The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

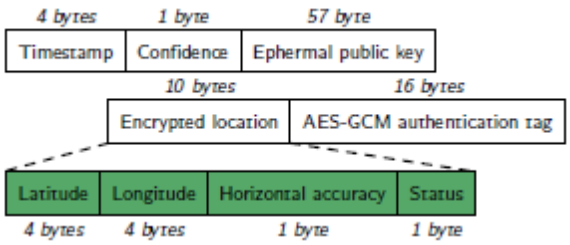


Fig. 2. Binary format of a location report.

ing the algorithm described in § 6.1. Finally, the finder creates a complete location report, including the current timestamp (in seconds since January 1, 2001), the ephemeral public key d', the encrypted message, and the AES-GCM authentication tag as shown in Fig. 2.

Exhibit 13, at 6-7, § 6.3.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0FBAE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Id., at 7, § 6.3.

171. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal based on receiving a packet in the OF advertisement), the mobile station must necessarily store data related to the OF advertisement (*i.e.*, store previous obtained checking data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station sends to a mobile telephone network, and the mobile telephone network routes to the Apple iCloud servers (Apple is a provider of presence related services), a signal that identifies that the mobile station is nearby the missing device that is part of the Find My network (*i.e.*, it is present in the special area). Further, when nearby the lost radio communication defining device, the mobile station receives the distinctive defining signal. The mobile station is able to identify that the received defining signal is distinctive and to determine that it is present within the crowdsourced offline finding special area, as detailed above. The BLE distinctive signal must include a device identifier such that the Find My services related to the found device can be later provided in connection to that device, as elaborated below.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

172. The Accused Products perform receiving in the one or more servers of the provider of presence related services from the mobile station via the mobile telephone network an updating signal uncorrelated to any mobile station phone call establishment that identifies the mobile station's presence in the special area, the one or more servers of the provider of presence related services deriving from the updating signal by one or more processing devices having access to at least a portion of the data whether or not the mobile station is present in the special area; and enabling or disabling by use of the one or more processing devices a presence related service based upon the mobile station's presence or non-presence in the special area. For example, the mobile station sends a signal about the mobile station's presence in the special area via a mobile telephone network to the Apple iCloud servers (Apple is the provider of Find My "offline finding" presence

related services), the signal including the mobile station's location. When sending the presence updating signal, the mobile station is not necessarily within Wi-Fi coverage. In that case, the mobile station must send its updating signal via a mobile telephone network. The presence signal must also include the device identifier of the first and/or second found device, because the Find My network needs this to subsequently provide related presence related services (*e.g.*, the notification to the device owner about the found device location). The images below indicate that once a mobile station has identified that it is nearby a lost device that is in an offline status, the location of the mobile station and the device identifier of the lost device are collected to provide the Find My service (this information is sent to the Apple servers within the updating signal, as it is required to allow the device owner to locate the device, once found by the mobile station).

> **Advertising Interval.** The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

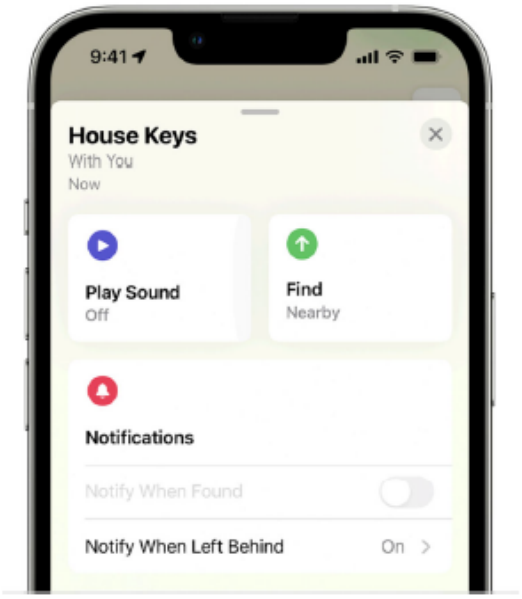
Exhibit 13, at 6, § 6.2.

> **Set up and use Notify When Left Behind in the Find My app**
>
> With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

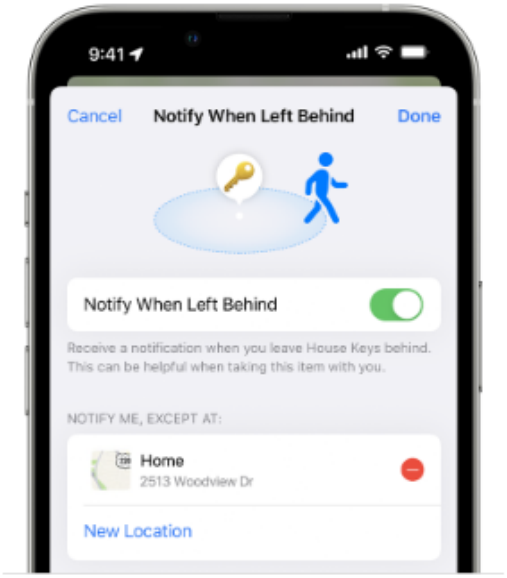
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Id. 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

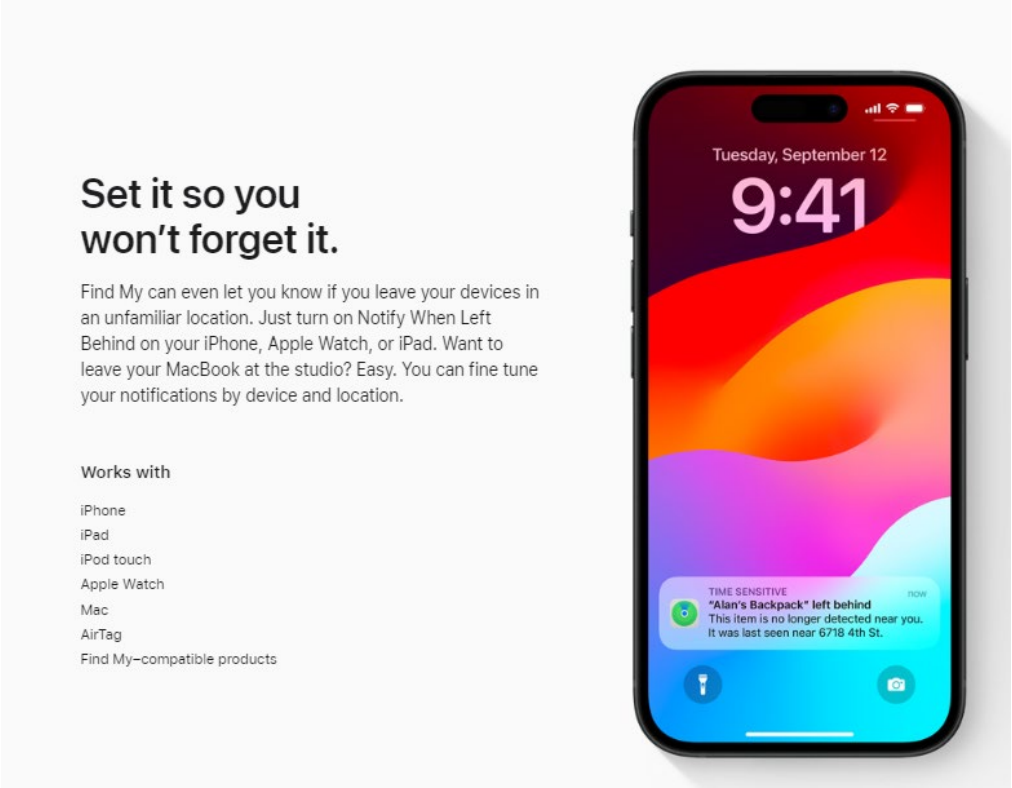


Exhibit 8, https://www.apple.com/icloud/find-my/

173. For example, the Apple iCloud servers (Apple is the provider of presence related services) receives the presence updating signal and uses it to provide presence related services (*e.g.*, displaying to the first "found" device's owner, the device's location on a map, as illustrated below in connection to a found Apple device (and similarly for the second found device); or sending a notification to a device of the owner of the first or second lost device indicating that it has been found).

> **Advertising Interval.** The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Exhibit 13, at 6, § 6.2.

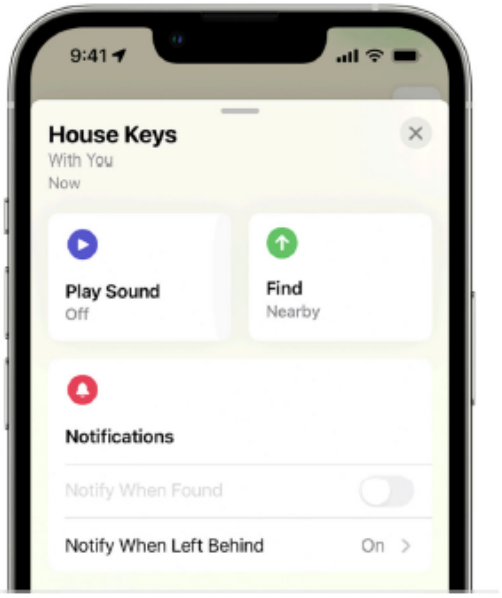
Set up and use Notify When Left Behind in the Find My app

With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

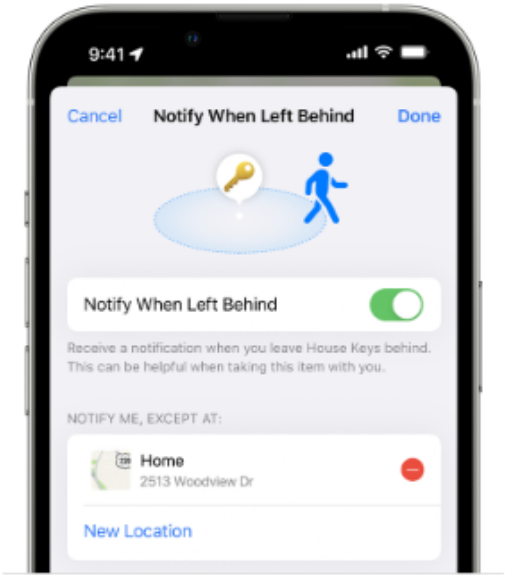
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

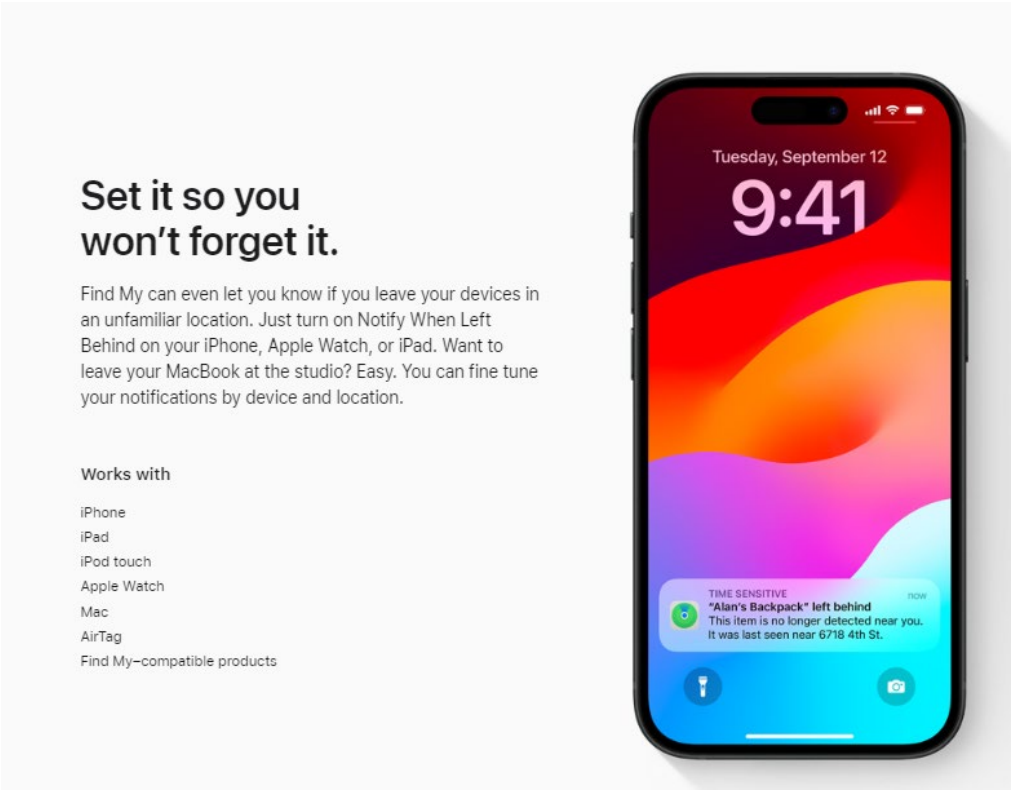


Exhibit 8, https://www.apple.com/icloud/find-my/

174. For example, a mobile station (a *finder* device) identifies that it is present within the area of coverage of a device that is lost (*e.g.*, the first and/or second radio communication defining device) and is part of the Find My finding network and sends to a vendor controller server (*i.e.*, to the Apple iCloud servers in the case of Apple devices and Apple Find My offline finding ecosystem) an updating signal indicating the presence status (the signal including unique beacon data received from the lost first/second device via BLE, together with the location of the device).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

175. The mobile station identifier of the mobile station is included within the updating signal sent to the Apple iCloud.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

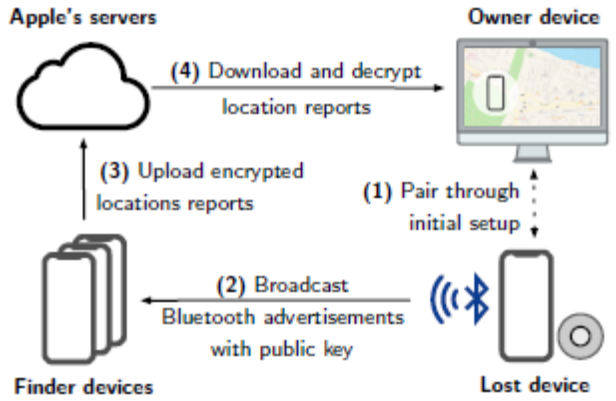


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Exhibit 13, at 6, § 6.2.

176. For example, the sending of the updating signal is uncorrelated to any mobile station phone call establishment. The updating signal is sent when the mobile station enters into the offline finding special area and starts receiving the first and/or second distinctive defining signals from the first/second lost radio communication defining device. Also, if the mobile station remains nearby the first and/or second lost device (*i.e.*, remains in the special area), it periodically sends a presence updating signal via mobile telephone network to the Apple iCloud servers, as further elaborated below. The mobile station stores in a local database the determination performed by the mobile station about its presence in the special area, in relation to each found device public key identifier (*i.e.*, in connection to at least the first and/or second radio communication defining devices). After storage, the mobile station sends a presence updating signal containing the (each) lost device public key and the location to the Apple iCloud servers. If it is the first (recent) reporting by the mobile station about its presence in the special area, the presence updating signal

is then related to the mobile station entering into the special area.

> **Uploading Reports.** Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0F8AE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Exhibit 13, at 7, § 6.3.

177. For example, the mobile station receives an acknowledgment about the presence updating signal having been received in the Apple iCloud servers (via a mobile telephone network), as indicated in the image below. As also indicated in the image below, the presence determination process (*i.e.*, the scanning and filtering of OF advertisements in a certain format) is

then reinitiated. If the mobile station remains in the special area in connection to a lost device it has already reported (*i.e.*, the first and/or second radio communication defining devices), then it may send (after 15 minutes) a new updating signal related to the mobile station presence in the special area (in connection to that lost device): *i.e.*, the presence updating signal is then related to the mobile station remaining in the special area.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

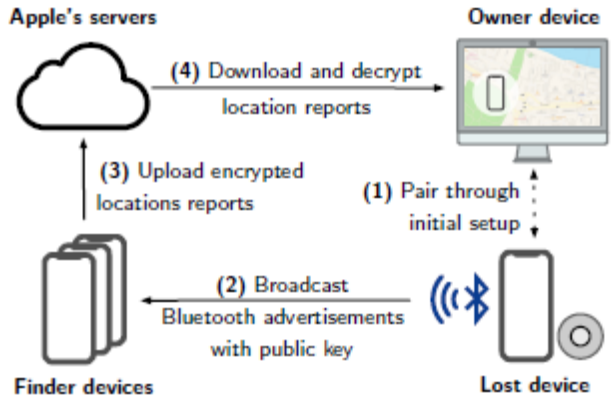


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Exhibit 13, at 6, § 6.2.

178. For example, the mobile station stores in a local database the determination performed by the mobile station about its presence in the special area, in connection to the (each) found device public key identifier (*e.g.*, in connection to at least the first and/or second radio communication defining devices). After the storage, the mobile station sends a presence updating signal containing the recently found device(s), public key(s), and the location to the Apple iCloud servers). If it is the first (recent) reporting by the mobile station about the mobile station presence in the special area, the presence updating signal is then related to the mobile station entering into the special area.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0F8AE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Exhibit 13, at 7, § 6.3.

179. Defendant has and continues to indirectly infringe one or more claims of the '621 Patent by inducing infringement by others, such as Defendant's customers and end-users, in this District and elsewhere in the United States. For example, Defendant's customers and end-users directly infringe, either literally or under the doctrine of equivalents, through their use of the inventions claimed in the '621 Patent. Defendant induces this direct infringement through its

affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products, and providing instructions, documentation, and other information to customers and end-users suggesting that they use the Accused Products in an infringing manner, including technical support, marketing, product manuals, advertisements, and online documentation. *See, e.g.*, Exhibit 8, https://www.apple.com/icloud/find-my/ ("Find My"); *see also, e.g.,* Exhibit 14, available at https://support.apple.com/en-us/104978 ("Find your lost Apple device or AirTag with FindMy"); Exhibit 14, https://support.apple.com/en-us/102648 ("Set up Find My on your iPhone, iPad, or Mac"); Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind. ("Set up and use Notify When Left Behind in the Find My App").

180. Because of Defendant's inducement, Defendant's customers and end-users use the Accused Products in a way Defendant intends and they directly infringe the '621 Patent. Defendant performs these affirmative acts with knowledge of the '621 Patent and with the intent, or willful blindness, that the induced acts directly infringe the '621 Patent.

181. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the '621 Patent, as provided by 35 U.S.C. § 271(c), by contributing to direct infringement by others, such as customers and end-users, in this District and elsewhere in the United States. Defendant's affirmative acts of selling and offering to sell the '621 Accused Products in this District and elsewhere in the United States and causing the '621 Accused Products to be manufactured, used, sold, and offered for sale contribute to others' use and manufacture of the Accused Products, such that the '621 Patent is directly infringed by others. The accused components within the Accused Products including, but not limited to, software manufactured by Defendant, are material to the invention of the '621 Patent, are not staple articles or commodities

of commerce, have no substantial non-infringing uses, and are known by Defendant to be especially made or adapted for use in the infringement of the ’621 Patent. Defendant performs these affirmative acts with knowledge of the ’621 Patent and with intent, or willful blindness, that they cause the direct infringement of the ’621 Patent.

182. Because of Defendant’s direct and indirect infringement of the ’621 Patent, ALT has suffered damages in an amount to be proved at trial.

COUNT VII
(Infringement of the ’032 Patent)

183. Paragraphs 1 through 31 are incorporated by reference as if fully set forth herein.

184. ALT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the ’032 Patent.

185. Defendant has and continues to directly infringe the claims of the ’032 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, at least by performing each and every limitation of one or more method claims of the ’032 Patent by using the Accused Products.

186. The Accused Products practice the method of at least claim 1 of the ’032 Patent: A method associated with a provider of presence related services and a mobile station that stores in a memory first checking data and uses the first checking data to determine whether or not a defining signal received from a radio communication defining device is a distinctive defining signal, the distinctive defining signal at least partly defines a special area by its coverage, the method comprising: one or more servers of a provider of presence related services receiving from the mobile station via a mobile telephone network an updating signal that identifies the mobile station’s presence in the special area, the provider of presence related services being different than the mobile telephone network; and storing in the one or more servers a parameters database having

an operating parameter whose value is determined at least in part by the updating signal received from the mobile station; and sending from the one or more servers to the mobile station second checking data different from the first checking data to modify the special area.

187. The Accused Products perform a method associated with a provider of presence related services. For example, Apple Find My implements a method associated with the use of a mobile station and a missing Bluetooth device that is part of the Apple Find My network for offline finding and that transmits a distinctive defining signal indicative that it is in an offline status (*i.e.*, it is lost).

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, available at https://www.apple.com/icloud/find-my/.

Using Find My to locate missing Apple devices

Any Apple devices within Bluetooth range that have offline finding enabled can detect a signal from another Apple device configured to allow Find My and read the current broadcast key P_i. Using an ECIES construction and the public key P_i from the broadcast, the finder devices encrypt their current location information and relay it to Apple. The encrypted location is associated with a server index which is computed as the SHA256 hash of the P-224 public key P_i obtained from the Bluetooth payload. Apple never has the decryption key, so Apple can't read the location encrypted by the finder. The owner of the missing device can reconstruct the index and decrypt the encrypted location.

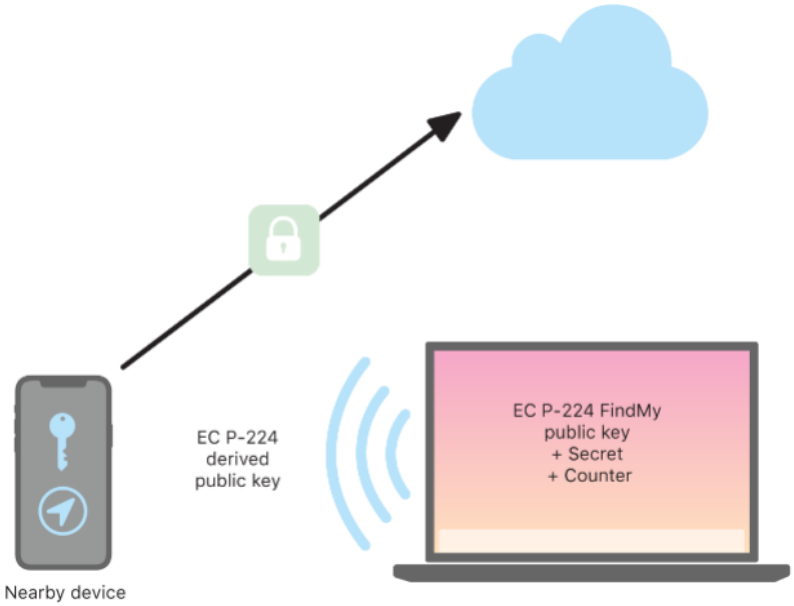


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

When a device goes missing and can't connect to Wi-Fi or cellular — for example, a MacBook Pro is left on a park bench — it begins periodically broadcasting the derived public key P_i for a limited period of time in a Bluetooth payload. By using P-224, the public key representation can fit into a single Bluetooth payload. The surrounding devices can then help in the finding of the offline device by encrypting their location to the public key. Approximately every 15 minutes, the public key is replaced by a new one using an incremented value of the counter and the process above so that the user can't be tracked by a persistent identifier. The derivation mechanism is designed to prevent the various public keys P_i from being linked to the same device.

Exhibit 12, https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

188. For example, within Find My, a user may register their Apple devices such that

they may keep them located when they are nearby, by using the Find My App. As illustrated below, Find My also provides an "offline finding" mode wherein a user's lost Apple devices (iPhones, iPads, Macs, Apple Watches, AirPods, Apple Pencil, and Apple Vision Pro) that are registered within the Find My network for offline finding can be found with the help of other devices (*e.g.*, iPhones, iPads, Macs).

189. For further example, the mobile station is an iPhone registered within Find My "offline finding" and helps to find a missing Apple device that is offline and is part of the Find My network. The missing Apple device that is offline and is part of the Find My network for offline finding is a radio communication defining device.

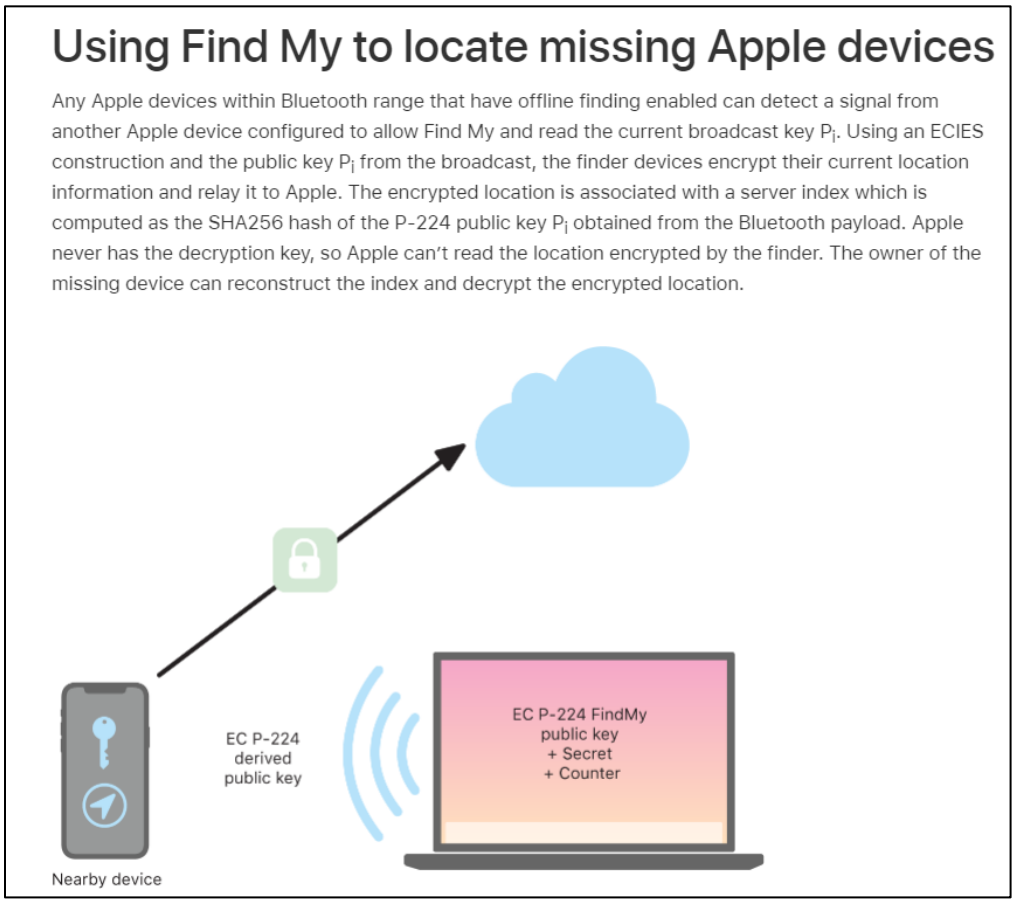


Exhibit 11, available at https://support.apple.com/en-au/guide/security/sece994d0126/web

190. For example, if an Apple device that is part of the Find My network for offline

finding (*i.e.*, a radio communication defining device) has gone offline, it starts emitting a Bluetooth Low Energy signal (*i.e.*, a distinctive defining signal) that can then be picked up by any Apple device that is part of the Find network for offline finding.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF

Exhibit 13, at 1, Introduction.

6 Apple Offline Finding in Detail

This section describes and discusses the technical details of Apple's OF system. In reference to Fig. 1, we (1) explain the involved cryptography and the key exchange during initial device pairing, and then explain the protocols implementing (2) *losing*, (3) *finding*, (4) *searching* for devices.

In short, devices and accessories in lost mode send out BLE advertisements containing a public key. Finder devices receive them, encrypt their location by using the public key, and upload a report to Apple's servers. This results in an end-to-end encrypted location report that cannot be read by Apple or any other third-party that does not have access to the owner's private keys.

Exhibit 13, at 5, § 6.

191. For example, the Find My finding service involves the use of a mobile station (a *finder* device) and a BLE radio communication defining device (a *lost* device) that transmits a BLE distinctive defining signal (a unique beacon).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.3 Finding

All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.

Generating Reports. The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

Exhibit 13, at 6, § 6.3.

192. The Accused Products perform a method where a mobile station that stores in a memory first checking data and uses the first checking data to determine whether or not a defining signal received from a radio communication defining device is a distinctive defining signal, the distinctive defining signal at least partly defines a special area by its coverage. For example, the mobile station observes a channel corresponding to the offline finding service BLE signals transmission and processes any received signal to determine whether or not it is receiving an offline finding service defining signal that comprises an offline finding service identifier. If the signal comprises an offline finding service identifier, at that point it is a defining signal for the mobile station. A processor within the mobile station processes any received defining signal and uses data previously stored in the mobile station (*i.e.*, checking data), to determine whether or not the BLE defining signal received is a distinctive defining signal that at least partially defines the offline finding service special area. If the mobile station determines that it is receiving a distinctive defining signal, it consequently identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it, as detailed below). Within Find My every Apple device enabled for "offline finding" is converted into a receiver and locator, which effectively crowdsources the search of a missing device. Any device registered within Find My for "offline

finding" becomes a Find Node of the Find My network and may receive and process the offline finding BLE defining signals from lost Apple devices.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1.

You can even find devices that are offline or powered off.

If your missing device can't connect to the internet or has little to no battery life, the Find My app can still help you track it down using the Find My network — hundreds of millions of iPhone, iPad, and Mac devices around the world. Nearby devices securely send the location of your missing device to iCloud, then you can see where it is in the Find My app. It's all anonymous and encrypted to protect everyone's privacy.

Exhibit 8, available at https://www.apple.com/icloud/find-my/

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

193. For example, the special area can be defined by the area covered by the Bluetooth distinctive defining signals of all the radio communication defining devices that are part of the Find My network for offline finding and are in an offline status at a given time. So, the special area is a dynamic-crowdsourced special area. The area covered by a given Bluetooth distinctive defining signal from a lost radio communication defining device that is in an offline status at least partly defines the special area. A user can make their Apple devices join the Find My network by using the Find My App. As shown below, a user can register various Apple devices for offline finding. The user can locate the devices by using the Find My map.

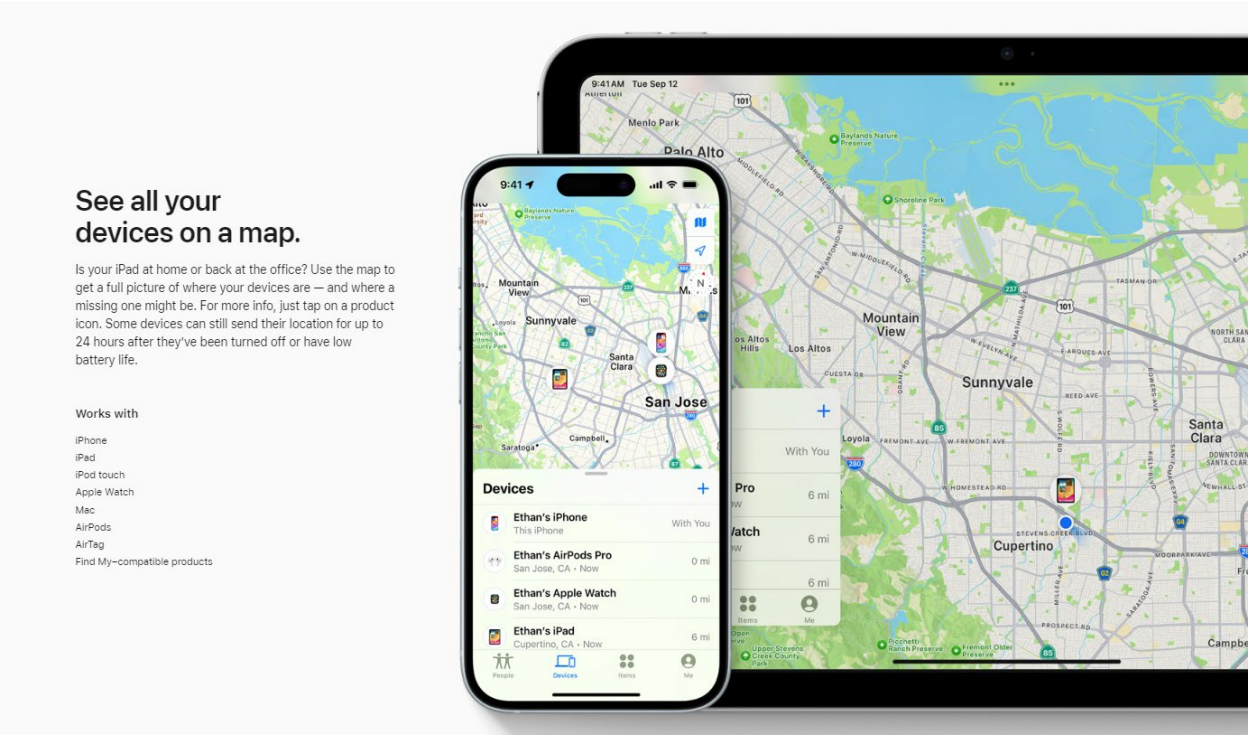


Exhibit 8, https://www.apple.com/icloud/find-my/

194. For example, a processor within a mobile device can help the mobile station in determining whether or not a received defining signal is a distinctive defining signal that at least partly defines a special area and whether or not the mobile station is present in the offline finding service special area. The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

> **Finder devices.** Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Exhibit 13, at 3, § 3.

195. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal based on receiving a packet in the OF advertisement format), the mobile station must necessarily store data related to the OF advertisement (*i.e.*, store previous obtained checking data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station further identifies that it is present within the special area (as the coverage of the distinctive defining signal party defines it). The mobile station obtains the lost device ID (*i.e.*, the public key) by processing the distinctive defining signal.

6.3 Finding

All finder devices regularly scan for OF advertisements. When the finder receives a packet in the OF advertisement format, it generates and uploads an encrypted location report to Apple's servers.

Generating Reports. The finder parses the public key from the advertisement. Then, it determines its current geolocation and creates a message that includes location, accuracy,[3] and status information (cf. green fields in Fig. 2). The message is then encrypted us-

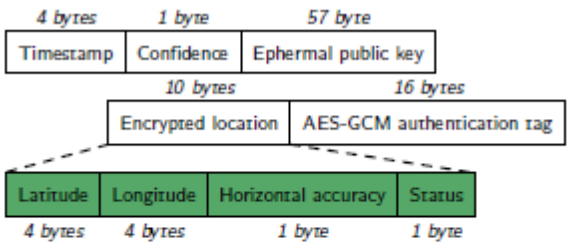


Fig. 2. Binary format of a location report.

ing the algorithm described in § 6.1. Finally, the finder creates a complete location report, including the current timestamp (in seconds since January 1, 2001), the ephemeral public key d', the encrypted message, and the AES-GCM authentication tag as shown in Fig. 2.

Exhibit 13, at 6-7, § 6.3.

Uploading Reports. Finder devices accumulate reports over time and upload them in batches regularly, possibly reducing energy and bandwidth consumption. During the evaluation with our test devices, we discovered that the median time from generating to uploading a location report is 26 min. We include the delay distribution in Appendix B. The delay can increase to several hours if the finder device is in a low power mode [7]. A finder limits the number of uploaded reports for the same advertisement key to four, most likely to prevent excess traffic on Apple's servers. The upload is implemented as an HTTPS POST request to https://gateway.icloud.com/acsnservice/submit. Every request is authenticated to ensure that only genuine Apple devices can upload requests. Table 3 shows the request header containing a device identity certificate, the signing CA's certificate, and an Elliptic Curve Digital Signature Algorithm (ECDSA) signature over the request body. The certificates are stored in the device's keychain. However, the private key used for signing is stored in the Secure Enclave Processor (SEP), Apple's implementation of a trusted execution environment (TEE) [4]. The SEP prohibits the extraction of the signing key but provides an interface for signing requests. We assume that the finder authentication serves as a form of remote attestation. However, we were unable to verify this assumption due to the obfuscated code. The HTTPS request body is prefixed with a fixed header (`0x0FBAE0`) and one byte specifying the number of included reports. This limits the number of reports in a single request to 255. Each report consists the ID (SHA-256(p_i)) followed by the 88-byte location report shown in Fig. 2.

Exhibit 13, at 7, § 6.3.

196. For example, the mobile station scans a BLE channel and is able to filter advertisements when it receives a packet in the OF advertisement format. To perform such filtering (*i.e.*, to determine that a defining signal with an offline finding service identifier is a distinctive defining signal based on receiving a packet in the OF advertisement format), the mobile station must necessarily store data related to the OF advertisement (*i.e.*, store previous obtained checking data) and use the data to perform the filtering (*i.e.*, the determination). The mobile station sends to a mobile telephone network, and the mobile telephone network routes to the Apple iCloud servers

(Apple is a provider of presence related services), a signal that identifies that the mobile station is nearby the missing device that is part of the Find My network (*i.e.*, it is present in the special area). Further, when nearby the lost radio communication defining device, the mobile station receives the distinctive defining signal. The mobile station is able to identify that the received defining signal is distinctive and to determine that it is present within the crowdsourced offline finding special area, as detailed above. The BLE distinctive signal must include a device identifier such that the Find My services related to the found device can be later provided in connection to that device, as elaborated below.

Overview

The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.

Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.

Note: Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

197. The Accused Products perform a method where one or more servers of a provider of presence related services receiving from the mobile station via a mobile telephone network an

updating signal that identifies the mobile station's presence in the special area, the provider of presence related services being different than the mobile telephone network and perform storing in the one or more servers a parameters database having an operating parameter whose value is determined at least in part by the updating signal received from the mobile station. For example, as the Bluetooth Low Energy distinctive defining signal is transmitted by the radio communication defining device when it has gone offline, the signal serves to identify (*e.g.*, using an "offline finding service identifier") that the device is in an offline status for offline finding. The offline status of the radio communication defining device (*e.g.*, an Apple device registered with Find My) implies that it is not located nearby any other Apple device of the device owner with capacity to update the location of the missing device and associated to the same Apple Account (*e.g.*, an iPhone registered within Find My in connection to the same account). If the radio communication defining device is not located nearby those other Apple devices, it means that it is located in an environment that is outside the environment defined as the sum of the volumetric spaces wherein the BLE signal from the missing user's device can be received in each of the other user's Apple devices (associated to the same user's account). Said outside environment is the predetermined environment, and the fact that the distinctive defining signal identifies that the device is offline for offline finding serves to indicate to the mobile station that the device is in the referred predetermined environment. As the predetermined environment depends on the location of the other user's Apple devices, the predetermined environment changes when the location of the other Apple devices changes. As an example: a user has registered within Find My an iPhone 15, Apple AirPods Pro, and AirTags, and he has lost the AirTags. On the basis of the iPhone 15 being switched on and with the Bluetooth enabled, the AirTags being offline implies that the AirTags are located within an environment that is outside the volumetric space wherein the BLE signal from the lost AirTags can be received in

the iPhone 15. Said outside environment is the predetermined environment. The following table summarizes the key features of BLE signals. The referred other user's Apple devices can receive a BLE signal from the Apple device when being in range. Otherwise, the Apple device is lost and it is in the predetermined environment.

Table 2. OF advertisement format (with zero-indexed bytes).

Bytes	Content (details cf. [6, § 5.1])
0–5	BLE address $((p_i[0] \mid (0b11 \ll 6)) \mid\mid p_i[1..5])$
6	Payload length in bytes (30)
7	Advertisement type (0xFF for manufacturer-specific data)
8–9	Company ID (0x004C)
10	OF type (0x12)
11	OF data length in bytes (25)
12	Status (e.g., battery level)
13–34	Public key bytes $p_i[6..27]$
35	Public key bits $p_i[0] \gg 6$
36	Hint (0x00 on iOS reports)

Exhibit 13, available at https://arxiv.org/pdf/2103.02282

198. For example, the mobile station sends via a mobile telephone network to the Apple iCloud servers (Apple is a provider of presence related services) a signal that identifies that the mobile station is nearby the missing device that is part of the Find My network (*i.e.*, it is present in the special area). Further, when nearby the lost radio communication defining device, the mobile station receives the distinctive defining signal. The mobile station is able to identify that the received signal is distinctive in that it relates to the offline finding service (*e.g.*, may comprise an "offline finding service identifier") which means that it is transmitted by a BLE Apple device that is enabled for offline finding and is in an offline status. By determining that it is receiving the BLE offline finding signal the mobile station also identifies that it is present within the crowdsourced offline finding special area (as the device is part of the Find My network for offline finding and its BLE offline finding signal partly defines the special area). The BLE distinctive signal must include a device identifier such that the Find My services related to the found device can be later provided

in connection to that device, as elaborated below.

> **Overview**
>
> The Find My app combines Find My iPhone and Find My Friends into a single app in iOS, iPadOS and macOS. Find My can help users locate a missing device, even an offline Mac. An online device can simply report its location to the user via iCloud. Find My works offline by sending out short range Bluetooth signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app — all while protecting the privacy and security of all the users involved. Find My even works with a Mac that is offline and asleep.
>
> Using Bluetooth and the hundreds of millions of iOS, iPadOS and macOS devices in active use around the world, a user can locate their missing device even if it can't connect to a Wi-Fi or mobile network. Any iOS, iPadOS or macOS device with "offline finding" enabled in Find My settings can act as a "finder device". This means the device can detect the presence of another missing offline device using Bluetooth and then use its network connection to report an approximate location back to the owner. When a device has offline finding enabled, it also means that it can be located by other participants in the same way. This entire interaction is end-to-end encrypted, anonymous and designed to be battery and data efficient. There is minimal impact on battery life and mobile data plan usage, and user privacy is better protected.
>
> *Note:* Find My may not be available in all countries or regions.

Exhibit 12, available at https://help.apple.com/pdf/security/en_AU/apple-platform-security-guide-x.pdf

199. For example, as a result of the mobile station identifying that it is present in the crowdsourced special area, the mobile station sends (encrypted and securely protected) a signal about the mobile station´s presence in the special area to the Apple iCloud servers (Apple is the provider of Find My "offline finding" presence related services), the signal including the mobile station location as detailed in the image above. A mobile station is not typically placed at the user´s home when receiving the distinctive defining signal from a lost device, but in a public environment. So, in those scenarios the mobile station is not connected to the network via Wi-Fi but through mobile telephony communications, *i.e.*, via a mobile telephone network. The presence signal must also include the device identifier, as it is required by the Apple iCloud to subsequently

provide related presence related services (*e.g.*, the above-referred notification about the device location).

200. The images below indicate that once a mobile station has identified that it is nearby a lost device that is in an offline status, the location of the mobile station and the device identifier of the lost device are collected to provide the Find My service (this information is sent to the Apple servers within the updating signal, as it is required to allow the device owner to locate the device, once found by the mobile station).

> **Advertising Interval.** The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

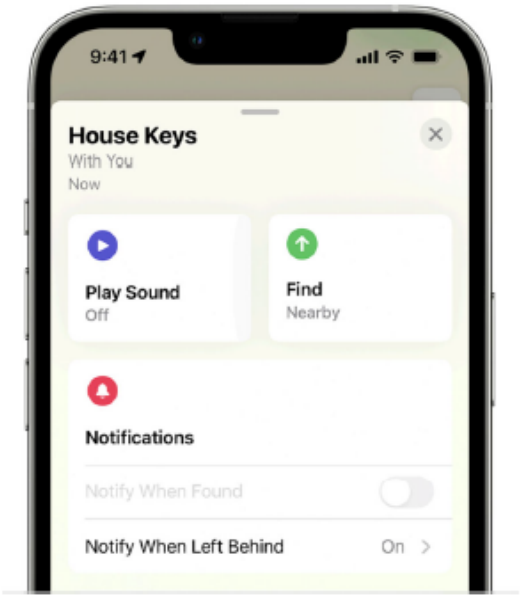
Exhibit 13, at 6, § 6.2.

> **Set up and use Notify When Left Behind in the Find My app**
>
> With Notify When Left Behind, your iPhone will alert you when you leave a supported Apple device, AirTag, or Find My network accessory at an unknown location. Learn how to set up Notify When Left Behind in the Find My app. And add locations where you don't want to be notified if something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

Set up Notify When Left Behind

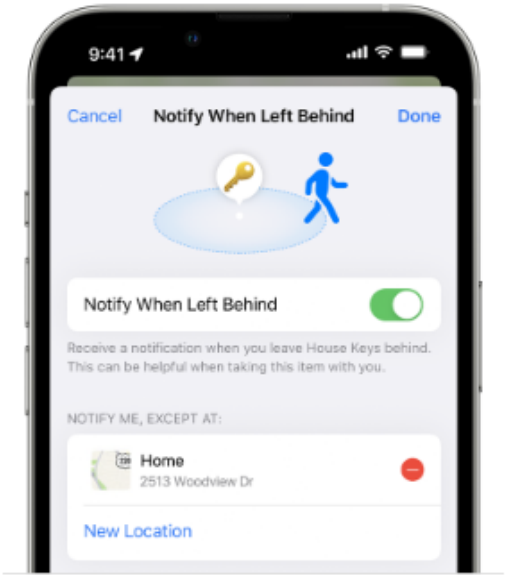
1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.



4. Under Notifications, tap Notify When Left Behind. If you don't see Notify When Left Behind, then that device might not be supported.
5. Turn Notify When Left Behind on or off.

Add locations where you don't want to be notified

1. On your iPhone, open the Find My app.
2. Tap Devices or Items.
3. Tap a device.
4. Under Notifications, tap Notify When Left Behind.



5. From here you can:
   - See your Home as a location where you won't be notified.
   - Tap New Location to add locations where you don't want to be notified when something's left there.
   - Tap the delete button ⊖ next to a location where you want to be notified when something's left there.

Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind

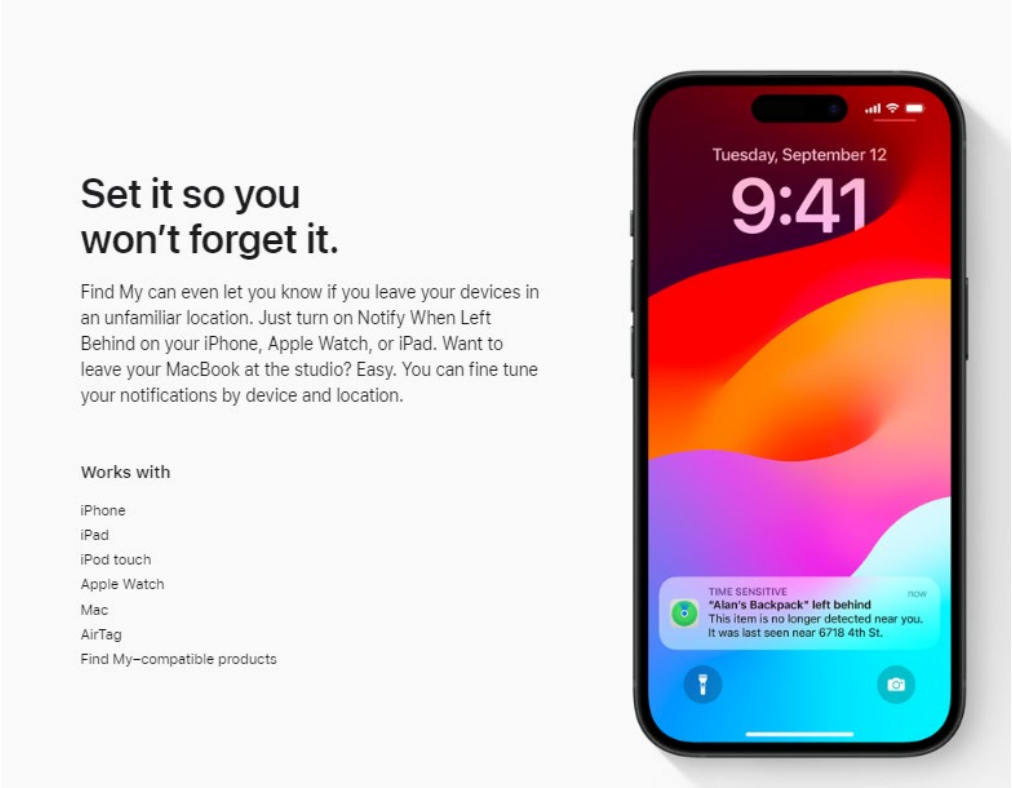


Exhibit 8, available at https://www.apple.com/icloud/find-my/

201. For example, a mobile station (a *finder* device) identifies that it is present within the area of coverage of a device that is lost and is part of the Find My finding network and sends to a vendor controller server (*i.e.*, to the Apple iCloud servers in the case of Apple devices and Apple Find My offline finding ecosystem) an updating signal indicative of the presence status (the signal including the unique beacon data received from the lost device via BLE, together with the location of the device).

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3

202. For example, the mobile station identifier of the mobile station is included within the updating signal sent to the Samsung Cloud.

3 Apple Offline Finding Overview

Apple introduced OF in 2019 for iOS 13, macOS 10.15, and watchOS 6 [10]. OF enables locating Apple devices without an Internet connection and promises to operate in a privacy-preserving manner. In 2020, Apple announced to support third-party BLE-enabled devices to be tracked by the OF network [11] and released a protocol specification for their integration [6]. We found that this public specification is incomplete concerning the overall OF system. Within this paper, we focus on our recovered specification that was partly validated by the accessory specification [6].

In the following, we give a brief overview of how OF works and introduce the different roles of devices. Fig. 1 depicts the interplay of the roles and protocols involved in OF. In particular, OF involves (1) initial pairing of owner devices, (2) broadcasting BLE advertisements that contain a rolling public key, (3) uploading encrypted location reports to Apple's servers, and (4) retrieving the location reports on owner devices. The terminology of the roles below has been derived from the official documentation [6].

Owner devices. Owner devices share a common Apple ID and can use the *Find My* application on macOS and iOS to search for any devices of the same owner.

Lost devices. Devices that determine to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices

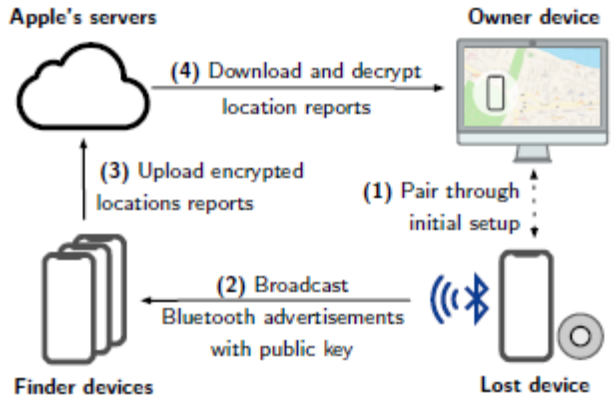


Fig. 1. Simplified offline finding (OF) workflow.

are considered to be lost when they lose Internet connectivity. Third-party accessories [6] are small battery-powered devices that can be attached to a personal item and are set up through an owner device. Accessories determine to be *lost* when they lose their BLE connection to the owner device.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

6.2 Losing

An OF device that loses its Internet connection starts emitting BLE advertisements. This advertisement consists of the 224 bit (28 bytes) public part[2] of the advertisement key (p_i), but required some engineering effort to fit in a single BLE packet.

Advertisement Packet Format. Apple had to engineer its way around the fact that one BLE advertisement packet may contain at most 37 bytes [19, Vol. 6, Part B, § 2.3.1.3], of which 6 bytes are reserved for the advertising MAC address, and up to 31 can be used

for the payload. For standard compliance, the custom OF advertisements needs to add a 4-byte header for specifying *manufacturer-specific data*, which leaves 27 bytes. Within this space, Apple uses a custom encoding for subtypes used by other wireless services such as AirDrop [21]), which leaves 25 bytes for OF data. To fit the 28-byte advertisement key in one packet, Apple repurposes the random address field to encode the key's first 6 bytes. However, there is one caveat: the BLE standard requires that the first two bits of a random address be set to $0b11$. OF stores the first two bits of the advertisement key together with the 24 remaining bytes in the payload to solve the problem. We depict the complete BLE advertisement packet format in Tab. 2. Apple confirmed the reverse-engineered specification later [6].

Advertising Interval. The same key is emitted during a window of 15 minutes, after which the next key p_{i+1} is used. During a window, OF-enabled iOS and macOS devices emit one BLE advertisement every two seconds when they lose Internet connectivity.

Exhibit 13, at 6, § 6.2.

203. For example, the updating signal is usable by the Apple iCloud servers to adjust a [lost/found] service flag operational parameter to "found" and to adjust/activate the presence related services provided to the mobile station, as services requestor (as elaborated herein below). The Apple iCloud servers (Apple is the provider of presence related services) receives the presence updating signal and uses it to provide presence related services. When a Find "offline finding" registered device related to a given Apple Find My user's account is missing, a service flag operational parameter is set to "Mark as Lost" in the Apple iCloud, such that the device is displayed as "Activated" or "Enabled." In that situation the user can wait for a mobile station that is part of the Find My network for offline finding to help in finding it. The image below illustrates how the found device owner benefits from the visualization of an updated location within a Find My map, in connection to the device found by the mobile station (as a result of the activation or enabling referred to above). If the device owner selected the "Notify When Found" feature (see the first

image below), then they will be notified when the missing device is found.

See the location of your device on a map

You can see your device's current or last known location in the Find My app.

Tap Devices at the bottom of the screen, then tap the name of the device you want to locate.

- *If the device can be located:* It appears on the map so you can see where it is.
- *If the device can't be located:* You see "No location found" below the device's name. Below Notifications, turn on Notify When Found. You receive a notification when it's located.

  Important: Make sure you allow notifications for the Find My app. See Change notification settings on iPhone.

For troubleshooting steps, see the Apple Support article If Find My is offline or not working.

Exhibit 17, https://support.apple.com/guide/iphone/locate-a-device-iph09b087eda/ios.

204. As a further example, when the Apple iCloud servers adjust the [lost/found] service flag operational parameter to "found," as detailed above, as a result of receiving the presence updating signal, the adjustment also serves to activate a presence related service related to the sending of an acknowledgment signal to the mobile station. As in the previous examples, the presence related service is provided to the mobile station as it is the entity triggering the updating signal, that is the service request. The acknowledgement presence related service is partly processed by the provider of presence related services, *i.e.*, by the Apple iCloud that generates the ack once the operation to update the device status to Turn off Lost Mode has been successful, and partly processed by the mobile station.

1 Introduction

In 2019, Apple introduced *offline finding (OF)*, a proprietary crowd-sourced location tracking system for offline devices. The basic idea behind OF is that so-called *finder* devices can detect the presence of other *lost* offline devices using Bluetooth Low Energy (BLE) and use their Internet connection to report an approximate location back to the *owner*. Apple's OF network consists of "hundreds of millions" of devices [4], making it the currently largest crowd-sourced location tracking system in existence. We expect the network to grow as OF will officially support the tracking of non-Apple devices in the future [6]. Regardless of its size, the system has sparked considerable interest and discussion within the broader tech and security communities [28, 29] as Apple makes strong security and privacy claims supported by new cryptographic primitives that other commercial systems are lacking [51]. In particular, Apple claims that it cannot access location reports, finder identities are not revealed, and BLE advertisements cannot be used to track devices [35]. Apple has yet to provide ample proof for their claims as, until today, only selected components have been publicized [4, 6, 35].

Exhibit 13, at 1, Introduction.

Finder devices. Finder devices form the core of the OF network. As of 2020, only iPhones and iPads with a GPS module are offering finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an OF advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers.

Apple's servers. Apple's servers store OF location reports submitted by finder devices. Owner devices can fetch those reports and decrypt them locally.

Exhibit 13, at 3, § 3.

205. For example, the beneficiary of the presence related service is the mobile station, that can adapt the reporting process based upon the received acknowledgement. The updating signal is triggered as a result of the mobile station receiving the distinctive defining signal

indicative that the lost device is in an offline status. Thus, the updating signal related to the offline finding service is, by its nature, indicative that the found device is in an offline status.

206. The Accused Products perform sending from the one or more servers to the mobile station, second checking data different from the first checking data to modify the special area. For example, as noted above, first and second checking data may correspond to a first and second mobile device. The special area can be modified by sending second checking data from server(s) that corresponds to the second mobile device instead of the first mobile device.

207. Defendant has and continues to indirectly infringe one or more claims of the '032 Patent by inducing infringement by others, such as Defendant's customers and end-users, in this District and elsewhere in the United States. For example, Defendant's customers and end-users directly infringe, either literally or under the doctrine of equivalents, through their use of the inventions claimed in the '032 Patent. Defendant induces this direct infringement through its affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products, and providing instructions, documentation, and other information to customers and end-users suggesting that they use the Accused Products in an infringing manner, including technical support, marketing, product manuals, advertisements, and online documentation. *See, e.g.*, Exhibit 8, https://www.apple.com/icloud/find-my/ ("Find My"); *see also, e.g.,* Exhibit 14, available at https://support.apple.com/en-us/104978 ("Find your lost Apple device or AirTag with FindMy"); Exhibit 14, https://support.apple.com/en-us/102648 ("Set up Find My on your iPhone, iPad, or Mac"); Exhibit 16, https://support.apple.com/en-us/102414#:~:text=On%20your%20iPhone%2C%20open%20the,tap%20Notify%20When%20Left%20Behind. ("Set up and use Notify When Left Behind in the Find My App").

208. Because of Defendant's inducement, Defendant's customers and end-users use the

Accused Products in a way Defendant intends and they directly infringe the ’032 Patent. Defendant performs these affirmative acts with knowledge of the ’032 Patent and with the intent, or willful blindness, that the induced acts directly infringe the ’032 Patent.

209. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the ’032 Patent, as provided by 35 U.S.C. § 271(c), by contributing to direct infringement by others, such as customers and end-users, in this District and elsewhere in the United States. Defendant’s affirmative acts of selling and offering to sell the ’032 Accused Products in this District and elsewhere in the United States and causing the ’032 Accused Products to be manufactured, used, sold, and offered for sale contribute to others’ use and manufacture of the Accused Products, such that the ’032 Patent is directly infringed by others. The accused components within the Accused Products including, but not limited to, software manufactured by Defendant, are material to the invention of the ’032 Patent, are not staple articles or commodities of commerce, have no substantial non-infringing uses, and are known by Defendant to be especially made or adapted for use in the infringement of the ’032 Patent. Defendant performs these affirmative acts with knowledge of the ’032 Patent and with intent, or willful blindness, that they cause the direct infringement of the ’032 Patent.

210. Because of Defendant’s direct and indirect infringement of the ’032 Patent, ALT has suffered damages in an amount to be proved at trial.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, ALT prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed

one or more claims of each of the Patents-in-Suit;

b. An order awarding damages sufficient to compensate ALT for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with pre-judgment and post-judgment interest and costs;

c. Enhanced damages pursuant to 35 U.S.C. § 284;

d. Entry of judgment declaring that this case is exceptional and awarding ALT its costs and reasonable attorney fees under 35 U.S.C. § 285; and

e. Such other and further relief as the Court deems just and proper.

Dated: September 13, 2024

Respectfully submitted,

/s/ Peter Lambrianakos

Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
FABRICANT LLP
411 Theodore Fremd Avenue
Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

ATTORNEYS FOR PLAINTIFF AVANT LOCATION TECHNOLOGIES LLC