CONNECT & SECURE YOUR IPHONE & IPAD

Covers iOS 13.1 & iPadOS 13.1

BY GLENN FLEISHMAN

Welcome

Welcome to *Connect and Secure Your iPhone and iPad*, version 1.0.3, written by Glenn Fleishman, published September 26, 2019, by Aperiodical LLC.

This book describes how to use your iPhone and iPod touch with iOS 13.1 and iPad with iPadOS 13.1 on Wi-Fi and cellular/mobile networks securely, making connections with ease while protecting your data and your privacy. It also covers Bluetooth, tracking an Apple mobile device, the Apple Watch, managing passwords, Safari's cookie protections, Personal Hotspot and Instant Hotspot, two-factor authentication with an Apple ID, Sign in with Apple, using AirDrop and AirPlay, and solving connection problems.

Visit **the updates page** to check for new versions and re-download any of the ebook files. Use the password `horsefly`. **Sign up for the announcement email list**, and you'll be notified about free updates to this edition of the book, as well as receive a note and a discount coupon when I release future editions covering newer versions of iOS and iPadOS. I will not sell, rent, or share your information.

Find me on the web at **http://glennf.com/guides**.

Introduction

The book is divided into three major sections:

Networking should be simple, and security should be automatic. And money should grow on trees. Despite how intuitive it is to pick up and use an iPhone or iPad, requiring little thought as to how it connects to a cellular or Wi-Fi network, it becomes complex as soon as you drill down to any details. This is especially true when connectivity fails, and you try to troubleshoot.

Privacy deserves the attention it's now getting. Your information is your own to choose how it's shared, whether it's your location, your food preference, or your address and phone number. iOS and iPadOS provide tools that enhance your ability to control that.

Security is an even denser area. Apple makes its default choices reasonably secure, but to ensure real protection for your data—when you select and use passwords, while your bits are traveling through the æther, or in the event that your device is stolen—you need to know how it all works.

Note: Apple split iOS into two parts in its latest release. iOS is now the name of the operating system that runs an iPhone or iPod touch, while iPadOS naturally powers the iPad. Because nearly everything covered in this book remains identical across both systems, I will frequently refer to them collectively as "the OS" to avoid repetition.

TABLE OF CONTENTS

NETWORKING

Connect to a Wi-Fi Network 8
Join a Network 8
Manage Wi-Fi Connections 10
Drill Down to Network Details 12
Turn Wi-Fi Off 16
Capture the Page 16
Knock, Knock, Apple's There! 16
Auto-Join and Auto-Login the Next Time 18

Wi-Fi Troubleshooting 20
Can't See Wi-Fi Networks or a Network You Need 20
No Wi-Fi Signal Strength in the Indicator 20
Too Many Wi-Fi Networks 21
Correct Password Not Accepted 22
No Internet Service after Connecting 22
Check a Web Page with Safari 23
Check or Ask about the Base Station 23
Check IP Address Settings 23

Make a Mobile Hotspot 25
Work with Personal Hotspot Settings 25
Access via iCloud Devices 27
Let Your Family Share It 28
Allow Others To Join 28
Set a Wi-Fi Password 28
Use Cell Data while Talking 29
Name Your Wi-Fi Network 30
Other Ways To Connect 31
Access via Wi-Fi 32
Tether with USB in macOS 35
Consider Turning Off Certain Radios 39

Choose to Use Cellular Data or Wi-Fi 41
Which Network Are You On? 41
Select Which Service to Use 42

Manage Cell Data Usage 44
Carriers Shift to Throttling 44
Keep Usage Restrained 45
Enable Low Data Mode in Cellular Settings 45
Tracking Cellular Usage on an iPhone 45

Check Cellular Usage on an iPad . . . 47
Turn Cellular Data On Only When You Need It . . . 47
Limit Your Activities on the Cell Network . . . 48

Place Calls via Wi-Fi . . . 51
Turn On Wi-Fi Calling . . . 51
Enable Wi-Fi Calling on Your Main Device . . . 52
Enable Wi-Fi Calling on Other Devices . . . 53

Airplane Mode . . . 56
What's Airplane Mode? . . . 56
When Radios Turn Off and When They Don't . . . 58

Set Up Bluetooth . . . 59
Bluetooth Basics . . . 59
Pairing Any Device . . . 60
Hands-Free Profile . . . 63
Audio Devices . . . 63

Pass Files with AirDrop . . . 66
Configure AirDrop . . . 66
Share with AirDrop . . . 67
Share via iOS or iPadOS . . . 68
Receive an Item in iOS or iPadOS . . . 69

Stream via AirPlay . . . 72
Select AirPlay Devices . . . 72
Ways to Use AirPlay . . . 74
Configure an Apple TV for Audio and Video . . . 74
Send Audio with Airfoil . . . 75
Mirror an iPhone or iPad Screen . . . 76

PRIVACY

Privacy Leaks . . . 78
Where Data Lives . . . 78
What Kinds of Data . . . 79
Behavior . . . 79
Differential Privacy . . . 79
Apps . . . 80
The Web and Web Searching . . . 81
Metadata . . . 82
Sensors and Receivers . . . 82
What Can Be Extracted and Learned . . . 83

Apple Blocks Tracking . . . 85
Safari Blocks Cookies . . . 85
Apple Breaks One-to-One Ad Tracking . . . 87
Block Content in Safari with Apps . . . 89

Privacy Settings 92
Setup without Much Sharing 92
Control System Privacy 94
Siri 95
What Siri Knows about You 96
Siri and On-device Searching 97
Safari 99
Apple's Suggestions 100
Sharing and Commenting 100
Passwords and AutoFill 101
Watching the Watchmen 101
Location 104
The How and Why of Location 104
Opting In and Opting Out 106
Photos 109
Bluetooth in Apps 110
Share My Location 110
Privacy Settings and Allowing Access 112

Keeping Creeps Away 113
Block Numbers and Email Addresses 113
Call-Blocking Apps 115
Filter iMessages and SMS 117
Filter SMS with Third-Party Apps 118

SECURITY

Create, Manage, and Use Strong Passwords 120
What Makes for a Good Password 120
Work with iOS and iPadOS's Built-in Manager 122
Passwords & Accounts 122
iOS and iPadOS Help with SMS Login Codes 125
Use Passwords in Web Sites and Apps and Devices 127
Safari 127
Other Apps 128
Fill in on Apple TV 129
Use Third-Party Password Managers 129

Connect to a Secure Wi-Fi Network 131
Connect to a Small Network 131
Share a Wi-Fi Password 132
What's Behind Simple Wireless Security 134
Connect to a Corporate or Academic Network 134

Use Two-Factor Authentication 136
What Have You Got in Your Pocket? 136
The Risk of SMS 2FA Factors 137
Turn On Apple's Two-Factor Authentication 139
Enable Two-Factor 139

Disable Two-Factor 140
Log In with 2FA to Apple Sites and Services 140
Log in to 2FA on a Trusted Device 141
Log in to 2FA using a Trusted Phone Number 142
Log in with 2FA in a Browser 143
Log In to Services with App-Specific Passwords 144
Manage 2FA Devices, Contacts, and Email 145
Add or Remove a Trusted Phone Number 146
Remove a Trusted Device 146
Manage Your Notification Email 147
Recover Account and Access 148
Reset Your Password with a Trusted Device 148
Lost All Trusted Devices 149
Use a Recovery Key when Automatically Upgraded 150

Connect with a VPN 151
Umbrella Protection 151
Get VPN Service via an App 152
Configure a VPN Manually 156
Make a VPN Connection 157

Protect Your Device 159
Use a Passcode 159
Set up a Passcode 160
When a Passcode Is Required 161
Reverting to a Passcode for Safety 162
Use a Biometric Login 162
Use Touch ID 163
Use Face ID 163
Block Unwanted USB Connections 165

When Your Device Goes Missing 166
How Find My Works 166
How Find My Sends Its Location over Wi-Fi or Cellular 167
How Find My Discovers Disconnected Devices 168
Use Find My for Tracking 169
View Your Device's Location 169
Take Remote Action 173
Notification and Driving Directions 173
Play Sound 174
Mark as Lost 174
Erase This Device 178

NETWORKING

It's true that an iPhone or iPad can be used without a live network connection, but their natural states are always hooked up. In the first part of the book, you'll learn how to work with the three types of mobile wireless communication—Wi-Fi, cellular, and Bluetooth—for general connectivity, with personal hotspots, for audio/video streaming, and for file transfer.

Connect to a Wi-Fi Network

Wi-Fi works quite simply in iOS and iPadOS, but there's a lot detail hidden beneath the surface. In this chapter, learn the many ways to connect to Wi-Fi, manipulate network settings, and work with public hotspots.

Join a Network

Open the Settings app and tap Wi-Fi to view nearby networks. You see a single name for all Wi-Fi routers that broadcast a network with that name. Tap a network name to attempt to join it.

You can also use a quicker method added in the latest OS:

1. Swipe to reveal the Control Center.
2. Hold down on the network area.
3. Hold down on the Wi-Fi icon.
4. Select a network from the list that appears (**Figure 1**).

> **Tip:** Tap Wi-Fi Settings to bring up Settings > Wi-Fi, which is discussed next.

The first time you tap a network name to connect, your device joins the network immediately unless encryption is enabled on the network. In that case, you are prompted for a password; once you've entered the password and tapped the Join button, you join the network.

> **Note:** For more on connecting with a password or other methods, see **Connect to a Secure Wi-Fi Network** in the Security section of the book.

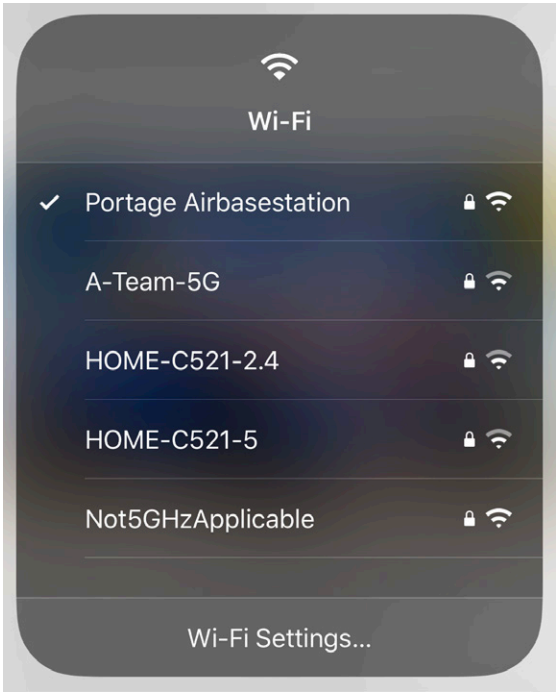

Figure 1: *Hold down the Wi-Fi icon in the Control Center's expanded network area to bring up a list of Wi-Fi networks to join.*

If you don't have a network's password and you're with a friend who has previously logged in, place your device near theirs and tap the network that you want to join. If you're in that person's contacts, their device will prompt them to approve sending your device the password (**Figure 2**)!

Figure 2: *When my younger kid places his iPad near my iPhone and tries to join Portage Airbasestation, I see the message at left. I tap Share Password, and the password is silently shared to his iPad. Then iOS lets me know it succeeded.*

Once your device joins a network, the network name and any associated login information is added to an internal network list. Unlike in macOS and Windows, you can't examine this list, view passwords, or remove entries. The device uses this list to re-join a network when it is in range.

> **Tip:** If you have iCloud Keychain enabled, you can extract a network password on a Mac with Keychain Access in the Utilities folder. Search for the network's name, double-click the entry, click Show Password, and enter your Mac's account password.

Manage Wi-Fi Connections

iOS and iPad OS centralize Wi-Fi management in the Wi-Fi settings view (**Figure 3**). To reach it, open the Settings app and tap Wi-Fi.

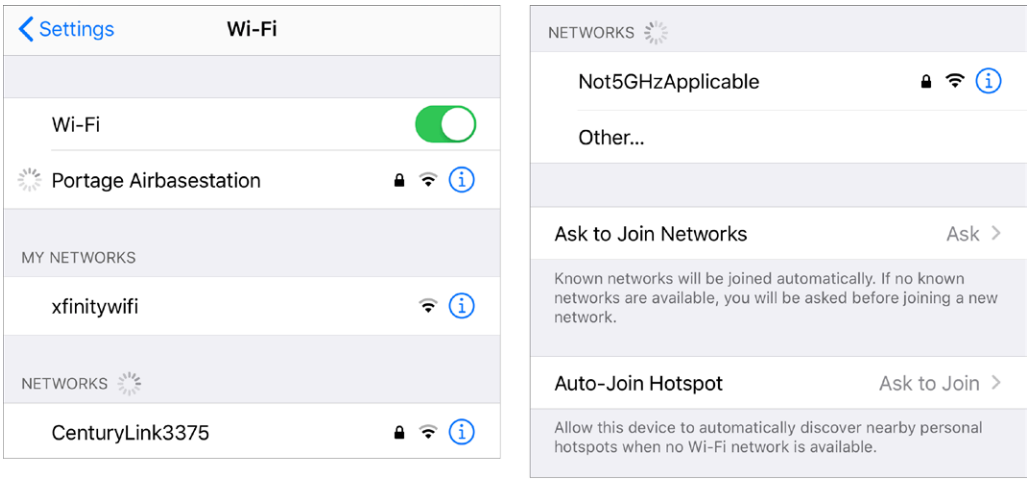

Figure 3: *The Wi-Fi connection view shown in two overlapping parts.*

The Wi-Fi view shows several elements, although not all appear in all cases, depending on what's around you:

- **Wi-Fi (always):** Tap this switch to disable and enable the Wi-Fi radio.
- **Currently connected network:** If you're connected to a network, it appears just below the Wi-Fi switch.
- **My Networks:** This area lists any network in the vicinity to which you've previously connected but aren't currently connected.

- **Personal Hotspots:** If your iPhone or cellular iPad is nearby and logged into the same iCloud account, it appears as a Personal Hotspot, whether or not that feature is active. (This is the Instant Hotspot feature; see **Turn On via Another Device**.)
- **Networks/Other Networks:** All networks in the vicinity appear in this list.
- **Set Up an AirPort Base Station:** This option appears only if your device detects a nearby unconfigured Apple-branded base station. (Apple has discontinued its Wi-Fi gateway line of products, but you may still be using one or replacing one.)
- **Ask to Join Networks:** With this switch, choose whether to be alerted about nearby networks to which the device hasn't previously connected.

> **Tip:** If Ask to Join Networks is off, you won't be alerted about new networks nearby when a known network isn't available. However, the Choose a Network list always shows all named networks around you.

- **Auto-Join Hotspot:** New in the latest release, you can tell your device to either let you know about or automatically join personal hotspots if it can't find any other Wi-Fi network.

Each Wi-Fi network shown—whether as the network to which you're connected or in Personal Hotspots, My Networks, and Networks/Other Networks—has three or four of the following elements:

- **Network name:** A network uses this name to *advertise* itself to Wi-Fi adapters that are looking to make a connection. The network name is also called the SSID (Service Set Identifier) in some of the geekier base station configuration tools.
- **Lock icon:** A lock may appear, indicating that there's some form of protection on the network.
- **Signal-strength indicator:** One, two, or all three radio waves in the indicator are black (starting at the bottom) to show the strength of the signal being received by the device.
- **Instant Hotspot details:** For any iPhone or iPad that meets the Instant Hotspot parameters, you see icons for the device's cellular signal strength, network connection type, and battery charge 

.

- **Personal Hotspot symbol:** Nearby Personal Hotspots that aren't signed into the same iCloud account as the device you're using appear in the Networks/Other Networks list, but show an icon of two overlapping chain links instead of the signal-strength indicator.
- **Information:** Tapping the info button, or anywhere in the network name's line for the currently selected network, reveals technical details about the network, as well as an option to forget the network. For more about these details, see **Drill Down to Network Details**, a few pages ahead.

Apple Watch Wi-Fi and Cellular

Every Apple Watch can connect to its paired iPhone using Wi-Fi if they're both on the same network. However, for an iPhone and Watch to be on the same Wi-Fi network, the network has to meet some very particular criteria:

- The network must use the 2.4 gigahertz (GHz) band. (See **Wi-Fi Troubleshooting**.)
- For an open or hotspot network, it must not have a portal or login page.
- For password-protected networks, the iPhone associated with the Watch must have previously connected to the network.

With watchOS 4 and later, you can connect without the iPhone nearby to a new Wi-Fi network as long as it has no password and no portal to use iPhone-free features, like maps.

Apple Watch Series 3 and later models can include cellular networking—allowing access to notifications, email, texts, and more—even when the iPhone isn't available. But owners aren't required to activate it and pay for cell data access. When a Watch Series 3 or later has an active data plan, it only works on the carrier's footprint—there's no roaming available.

Drill Down to Network Details

For an unusual Wi-Fi connection, such as one requiring a static network address or a different domain name server than the network's default, you may need to poke beneath the surface. Go to Settings > Wi-Fi and tap the info button or anywhere in the line for the current network.

The resulting view has the network name at top and three or four configuration areas, depending on the network (**Figure 4**). Let's look at each.

Unsecured network

Starting in iOS 10, Apple displays a fairly severe warning about using an unencrypted network connection. When you tap a network without encrypted enabled, it displays "Unsecured Network" in the main Wi-Fi view under the network, and then explains further in this details screen that "open networks provide no security and expose all network traffic." And it has a link to follow to get even more information.

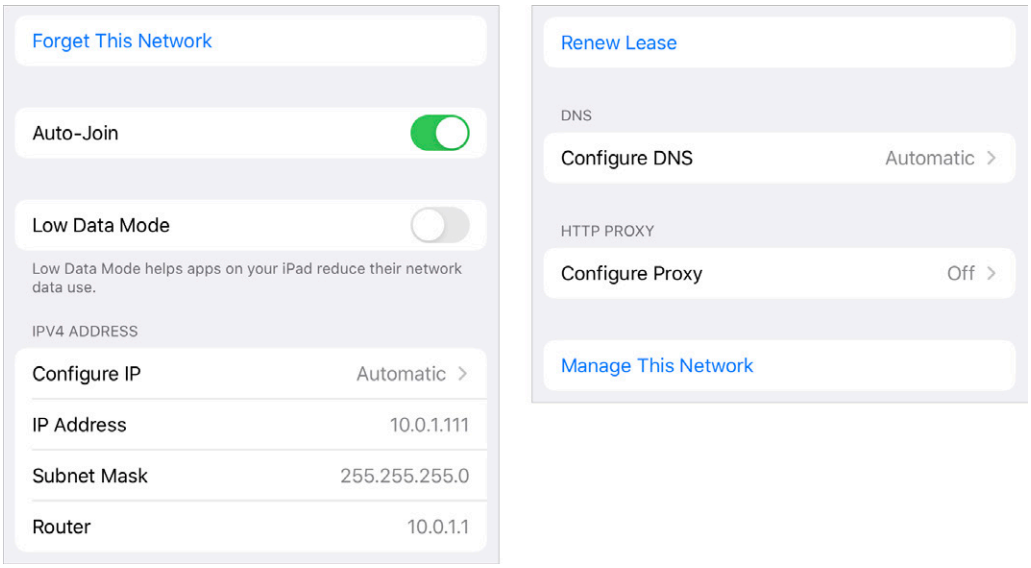

Figure 4: *View and set Wi-Fi connection values.*

What makes the message seem a little silly is that it appears for all public hotspots—including the ones in Apple Stores. It should rather suggest you use a VPN, which I discuss in **Connect with a VPN**.

Forget This Network

Tap Forget This Network to remove the network from the list of previously joined Wi-Fi networks; tap Forget to confirm. This disconnects the device immediately and prevents it from connecting again.

> **Note:** You can remove a stored network's entry only when you're connected to it.

If you have iCloud Keychain enabled, this action also removes the network's details from all of your other iCloud-linked devices.

Forgetting a network can solve network problems by letting the OS dump any corrupted or cached information prior to the next time you connect.

Auto-Join

Auto-Join lets you opt whether to connect the next time the network is nearby. This lets you keep a stored profile that you can tap to use without having it connect automatically. (A separate option, Auto-Login, only appears for hotspot networks where your device has recognized that there's a portal in place. See **Auto-Join and Auto-Login the Next Time**.)

Low Data Mode

New in version 13, Low Data Mode uses data-reduction techniques previously found only in Low Power Mode. The OS disables most background data uses, like synchronization and allowing Mail to pull down new messages. Foreground apps can reduce data usage, too. Music and FaceTime decrease data rates, for instance. When in use, a Low Data Mode label appears in small text below the network name in Wi-Fi settings.

You should use Low Data Mode (also available in Cellular settings) whenever you're in a place with low network throughput, a limited total amount of data you can consume, or when you're paying based on usage.

Renew Lease

The Renew Lease button is specific to DHCP (Dynamic Host Configuration Protocol). A lease is the assignment of an address by DHCP to your device. A lease can have a duration (like 15 minutes or 15 days). Occasionally, when you seem to have a network address but can't connect, tapping Renew Lease will obtain a new address and resume connectivity.

IP Address

The IPv4 Address section covers TCP/IP values used for addressing and routing. You start with a Configure IP menu that lets you pick among Automatic (DHCP), Manual (to tap in a fixed address), and BootP.

You shouldn't need to change this from Automatic. DHCP, the most common method, lets your gear request a network address from a router on the network, and then use it to interact on the local network and beyond.

In the main Wi-Fi settings, when your device uses DHCP to get an address on the local network, you can't change the IP Address, Subnet Mask, or Router fields; those values are provided by the DHCP server.

Note: Apple shows IPv4 Address or IPv6 Address (or both) depending on the version of addressing used by your network. IPv4 is the original Internet flavor. IPv6 is over 15 years old, and adds a bazillion more unique addresses to cope with the Internet's growth, but it's still only now coming into wider use.

Tip: The Client ID field can be useful with Wi-Fi gateways that assign local network addresses. On the gateway, you typically use a setting called DHCP Reservation and assign the Client ID to an address you pick on the local network.

DNS

DNS (Domain Name System) is used to convert human-readable domain names, like `www.glennf.com`, into machine-readable IP addresses, like `173.255.209.35`.

Tap Configure DNS and then tap Manual to change the defaults set by DHCP, which are listed under DNS Servers. This can be useful if the network to which you're connected has poorly run or slow default DNS servers. Tap the + to add additional DNS servers and the – to remove them.

The Search Domains option is something that only a network administrator should need to tell you to set.

Tip: Unfortunately, you can't set DNS for every connection—you can set it only for individual networks. It's only worth the effort to set it for connections you use frequently, such as your home Wi-Fi connection.

HTTP Proxy

This option is useful only for companies and schools. It redirects web requests you make to the Internet to a local server that handles them indirectly. It also allows the use of caching, in which pages retrieved by anyone in an organization are fed to you from this server instead of from the remote web site. This reduces bandwidth consumption.

Manage This Network

On a network that uses Apple's now-discontinued Wi-Fi gateways, this button will appear. Tap it, and it launches the AirPort Utility app if it's installed or prompts you to download it if it's not.

Turn Wi-Fi Off

Whenever the Wi-Fi radio is active, even if you aren't connected to a network, it's scanning for networks, which can slowly drain the battery. If you're nowhere near a network you can access or if you want to conserve battery life, turn off Wi-Fi by tapping Settings > Wi-Fi and then setting the Wi-Fi switch to Off. (See **Airplane Mode** for more details.)

WARNING! *Control Center also has a Wi-Fi switch, but tapping it only* ***disconnects*** *the current Wi-Fi network. It doesn't turn Wi-Fi off; it temporarily disables networking connections, because Apple uses Wi-Fi (and Bluetooth) for a lot of other purposes. For the full details, see* ***Airplane Mode****.*

Capture the Page

You'll find hotspot networks in public places such as cafés, libraries, and airports. After you connect to a network, which appears as open and unprotected, you're required to launch a browser and view a hotspot connection page (also called a captive portal) before you can use the Internet.

Apple has a trick and a configuration option that helps you interact with these networks whenever you encounter them or re-visit them.

Knock, Knock, Apple's There!

The OS has a clever feature that lets it display a hotspot network login screen and, in some cases, remember the login and other details. However, you can get stuck reconnecting to the same network.

Normally, to reach the captive portal, you must try to visit any web site in a browser, which is redirected by the network to the login page. Instead, iOS and iPadOS (and macOS since 10.7) perform a test that detects such redirections whenever you connect to a Wi-Fi network.

Immediately after your device joins a Wi-Fi network, it tries to connect to Apple's web site. If it doesn't get through, it assumes that it has reached a captive portal. Then, the next time anything happens on the device that requires Internet access (like retrieving email), the OS shows a special screen showing the portal's web page as if it were in Safari.

The hotspot network's captive-portal page will typically ask that you do one of the following (rarely more than one):

- Read a set of terms and conditions for use and tap an Agree button; enter an email address and tap an Agree button; or check a box that says "I agree" and tap a Submit button.
- Require that you register an account to use the network at no cost. With an account, you can log in and use the network.
- Require that you either pay for a connection to the network using a credit card, or enter login information for an active account on the network or an active account of a roaming partner.

After you carry out any of those actions, the OS should close the special screen and Wi-Fi service should be available. These pages are still often absurdly not customized for mobile devices, and the type and buttons are tiny. You'll need to pinch to zoom in almost all of the time.

Connect to a Captive Portal If It's Not Detected

If the special screen doesn't appear, you can reach the captive portal by launching the Safari app. Most of the time, the previously visited page in Safari will try to load; if you have a blank page, enter any site address, like `example.com` or `apple.com`, and tap Go.

After you enter any required data, the login system should redirect you to the web page you tried to visit in the first place.

Auto-Join and Auto-Login the Next Time

The next time you visit a hotspot network that you've previously accessed, the OS will automatically join the network and attempt to use the same credentials or button clicks that you used the previous time to gain access. This can lead to problems if that information is no longer valid or if the device doesn't present it correctly. I've also found in many cases, the OS just shows the same empty login screen again.

You can disable reconnecting by turning off Auto-Join, Auto-Login, or both for the connection. The second option appears only when you are connected to the Wi-Fi network, even if you haven't previously logged in or proceeded past the connection web page (**Figure 5**).

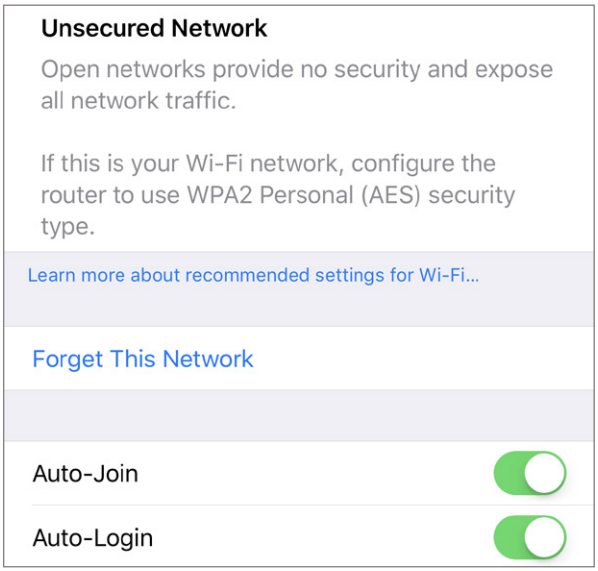

Figure 5: *Settings shows Auto-Login when you connect via a portal.*

To turn off Auto-Join or Auto-Login, follow these steps:

1. In the Settings app, tap Wi-Fi.
2. In the Choose a Network list, tap the info ⓘ button to the right of the network name.
3. In the configuration view, switch off Auto-Join, Auto-Login, or both.

Time-Limited Hotspot Access

Some hotspots limit your use to a specific period of time. This might be implicit, using your unique network adapter's ID—its MAC (Media Access Control) address—or another bit of tracking information based on when you first accepted a network's terms of services.

Some locations with hotspots give you a network code to enter at a portal page, which grants you access for a fixed amount of time. In those cases, you should turn Auto-Login off; otherwise, the next time you connect, it may attempt to enter a one-time use code that's expired, and it may be difficult to connect properly with a new code.

Wi-Fi Troubleshooting

Although Wi-Fi generally works well, you may at times be unable to get a live network connection. Here is troubleshooting advice for common cases.

Can't See Wi-Fi Networks or a Network You Need

If your device can't see any Wi-Fi networks or a network you think should be available, eliminate variables by trying the following:

- With no Wi-Fi networks detected, be sure that Wi-Fi isn't turned off. Swipe to reveal Control Center (or launch Settings). (This has happened to me more times than I'd like to admit.)
- You may be connected to the wrong network. In Control Center, press and hold the Wi-Fi button to expand the networking panel; the name of the network you're connected to appears under the Wi-Fi button.
- It's possible that you are out of range. Move the device closer to where you know (or think) a base station is located. Although every Apple mobile device sports an excellent Wi-Fi radio, Wi-Fi reception can be blocked by thick obstructions, such as solid stone and brick walls, or by walls made of chicken wire covered by plaster.

Note: It's also possible that the base station, not your handheld, is in trouble. And I have seen the Wi-Fi radio in an Apple mobile device fail intermittently or completely, requiring that the device be entirely replaced.

No Wi-Fi Signal Strength in the Indicator

You've selected a network and, if necessary, entered a password, and tapped Join—but the signal-strength indicator in the upper left still shows gray radio waves instead of black. This means that an initial con-

nection was made, but then you quickly moved too far away from the base station, or the base station was shut down or restarted with new information. If the connection process had failed while underway, you would have seen a notification alerting you.

Try connecting again. If that fails, restart your device: Press the Sleep/Wake button until you see a red slider for powering down. Slide it, wait until the spinning indicator disappears and the screen goes entirely black, and then hold down the button again for a few seconds. An Apple icon appears and the device starts up.

Too Many Wi-Fi Networks

You can find yourself swimming in a sea of Wi-Fi networks in your vicinity, which often makes it hard to select the one you want to join. If you know the network's exact name, you can type it in:

5. Launch Settings.
6. Tap Wi-Fi.
7. Slide down until you can tap the Other button (**Figure 6**).

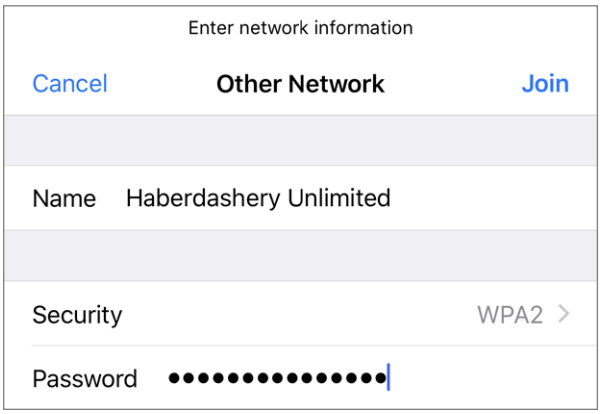

Figure 6: *The Other Network option lets you enter a network name and optional password from scratch.*

8. Enter the network name exactly and, if there's a password:

   a. Tap Security.

b. Select the method (almost certainly WPA2).

c. Tap Other Network to return to the previous screen.

d. Enter the password in the Password field.

9. Tap Join.

> **Tip:** If you don't know the kind of network security on the network you're trying to join and you have a Mac nearby, hold down the Option key and select the Wi-Fi menu, then hover over the network name. A small popup displays the security type.

> **Tip:** Starting in iOS 11, you can also tap a key icon above the keyboard to search through your stored passwords. This lets you pick an existing password, rather than re-entering it, if you have the correct password stored. And since iOS 12, you can also bring up third-party password managers. You can even ask Siri for a password!

Correct Password Not Accepted

As described in the chapter, **Connect to a Secure Wi-Fi Network**, a network that requires either a password or a username and password will reject your device if you enter it improperly.

But what if you're positive you're entering the password or username and password absolutely correctly?

- Check whether you were given the password with correct capitalization, which counts in Wi-Fi passwords as in others.
- Spaces can be part of WPA2 passphrases, but spaces are hard to indicate when written down. Confirm you're not missing a space.

No Internet Service after Connecting

You connected to a Wi-Fi network but cannot access the Internet from any programs you try. Here's how you can figure out what's wrong.

Check a Web Page with Safari

The most common cause of this problem is that you've connected to a network—likely a hotspot network, but possibly a guest network—that requires a password, button tap, or other action.

Launch Safari and try to reach any page, such as google.com:

- If you are redirected to a login page, follow the instructions. You may need to pay for access, or you may have connected to a network that requires a password; consult **Capture the Page** for more information.

> ***Remember to forget:*** *Because you've connected successfully to the Wi-Fi network, even though you haven't been granted access to the Internet, you need to remove the network from the list of those you've previously joined or you'll have this problem every time you're in range. Tap Settings > Wi-Fi, tap the info ⓘ button beside the network name, and then tap Forget This Network. Tap Forget.*

- If Safari throws up a connection error, try the next fix.

Check or Ask about the Base Station

If you're on a network where you can control the base station or ask someone who has access (a friend, barista, network administrator, or the like), you might ask them to confirm that there's no problem.

In some cases, a base station can continue to provide service to users who are already connected, but not properly allow new users to connect. Some have limits, as low as five or 10 connected devices, and that limit may only rarely be hit.

Check IP Address Settings

This may sound obscure, but it's an easy way to see if your device has obtained a network address from the router to which you've connected. To check on your assigned IP address, follow these steps:

1. In Settings, tap Wi-Fi.
2. Tap the network name.

The IPv4 Address section should be set to Automatic for almost all networks; another value should be chosen only if you've been told otherwise. (See **Drill Down to Network Details**, earlier in this chapter.)

If the IP address starts with `169`, then the OS wasn't able to obtain an address from the network. The `169` address range is self-assigned, meaning the device gave itself an address that can't be used on the network, and stopped checking.

Here are several ideas for fixing the IP address:

- Tap Renew Lease; this causes the OS to ask again for a network address. If successful, the IP address will change from a number starting with `169` to an address starting with another range, typically `192.168` or `10`.
- In the main Wi-Fi view, tap the Wi-Fi switch to Off, wait a moment, and tap it back to On. Tap the network's name to see if the address is now assigned.
- If you're at an event or a hotspot venue, ask the network's operator, the front desk, or whomever. The router may have crashed. (You can look around and see if other people look frustrated, too.)
- Restart the device. Press the Sleep/Wake button until a red slider appears. Slide to power off. Wait until the spinning indicator disappears and the screen turns black. Hold the button down again for a few seconds. An Apple icon appears, and the device starts up.

Make a Mobile Hotspot

Every iPhone and every iPad with cellular has a built-in data modem that lets the device access high-speed mobile data networks. This modem lets us use our iPhone or cellular iPad while we're traveling instead of having to buy a separate cellular modem or router with a separate monthly service fee.

Personal Hotspot lets you connect other devices to your phone or tablet as a conduit to the mobile Internet. While the name implies a Wi-Fi hotspot connection, which is one component of it, you may also *tether* via Bluetooth or USB with desktop computers and other devices to extend access. All three methods may even be used simultaneously.

Personal Hotspot's availability varies by carrier, although operators around the world offer it: **Consult this list by Apple** to check on yours.

Note: I refer to a mobile hotspot or Personal Hotspot when I mean all its features, but I use the term *tethering* when the discussion is specifically about Bluetooth or USB.

WARNING! *Most cellular operators put limits on Personal Hotspot use. They may offer a data rate lower than that of your phone (600 Kbps instead of LTE, for instance), cut you off after a certain amount of data (like 15 GB), or throttle you to 128 Kbps (2G) or 3G speeds after a monthly cap is hit.*

Work with Personal Hotspot Settings

Personal Hotspot is always available even when it says it's off. That sounds like a strange way to provide a service, but it makes sense in how Apple approaches it, particularly starting in iOS 13.1 and iPadOS 13.1.

In this new approach, a Personal Hotspot is something that any device logged into the same iCloud account can access on demand. You can also make it available to family members if you use Family Sharing. And if you want to let people or devices outside those two sets have access, you can tap a button and make the device act like any mobile hotspot.

Avoid Blowing Through Bandwidth

Devices that connect to a Personal Hotspot treat it like a regular Wi-Fi or Ethernet network, making it easy to consume huge amounts of cellular data. On your devices that connect to a Personal Hotspot, pause or disable sync and backup services, like Dropbox and Backblaze. Some third-party apps in macOS let you disable the use of specific Wi-Fi networks.

On other iPhones and iPads, you can enable the new Low Data Mode for the Personal Hotspot Wi-Fi network in Settings > Wi-Fi > *network name*. You have to be connected to enable Low Data Mode.

macOS doesn't yet offer a Low Data Mode, though Android does and Windows 10 has some tools. It would be great if every platform was cognizant of the increased use of mobile hotspots, which almost all come with limits or overage charges.

Personal Hotspot has three states:

- **Off:** You would think Off means off, but it means "standby." Off appears in the main Settings app next to the Personal Hotspot item.
- **On:** If you connect with another iCloud–linked device, or a member of your Family Sharing group connects, the Settings app shows On next to its item. The On label also appears if you allow access from other devices or people and one of them is connected.
- **On and Discoverable:** Other devices can also connect. This label appears only in the Control Center if you hold on the network area to reveal the Personal Hotspot button. In Settings, *no label* appears in this state! Yes, it's very consistent.

Let's dig into these overlapping states of being.

Tip: Before you use Personal Hotspot the first time, you may need to open it via Settings > Cellular (iOS) or Settings > Cellular Data (iPadOS).

Access via iCloud Devices

All your Apple devices logged into the same iCloud account can access your Personal Hotspot on demand. The capability is part of Continuity, a set of connections between your Apple mobile devices and between iOS, iPadOS, and macOS. (This feature used to be called Instant Hotspot.)

The limitation is the same as with many Continuity features: Your iPhone or cellular-data iPad and other devices that want to connect to it must all have Bluetooth enabled and be on the same Wi-Fi network.

On another iPhone or iPad device, go to Settings > Wi-Fi and choose the device in the Personal Hotspots list (**Figure 7**).

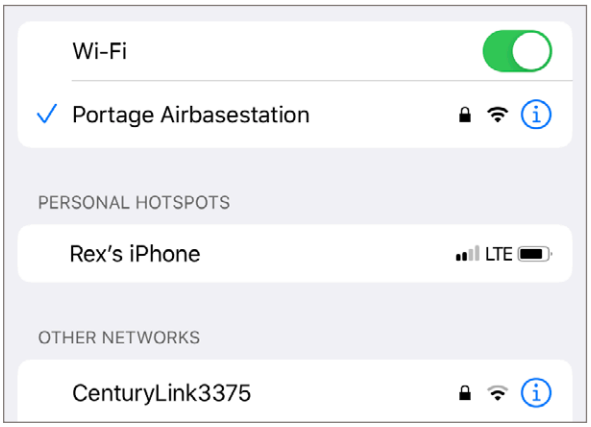

Figure 7: *In Wi-Fi settings, pick a device from the Personal Hotspots list.*

You can also use an option, new to this OS release, in Settings > Wi-Fi: Auto-Join Hotspot. Set it to Ask to Join or Automatic, and you'll be asked or automatically connected when no other Wi-Fi network is available.

On a Mac, select the Wi-Fi menu, and choose the device in the menu under Personal Hotspot (**Figure 8**).

Even if you're not planning to connect, you can see the battery life, signal strength, and connection strength of your device as a compact set of graphics in the menu or list.

Figure 8: *Available Personal Hotspots appear in the Wi-Fi menu in macOS.*

Let Your Family Share It

In the latest OS, you can also opt to make your Personal Hotspot available to others in your **Family Sharing group** in iCloud. If you use Family Sharing, the Personal Hotspot settings will include a Family Sharing menu. Tap it and you can choose to turn it on. You then select which family members must ask for approval and which can join automatically.

Allow Others To Join

The Personal Hotspot is always available to the devices and people mentioned above, but you can also provide access to other hardware and humans who aren't in your iCloud set or Family Sharing group via Wi-Fi and adding USB and Bluetooth tethering.

In Settings > Personal Hotspot, switch on Allow Others To Join (**Figure 9**). You can also enable this mode in Control Center. Swipe to reveal it, hold down on the network area, then tap Personal Hotspot (see **Figure 11**, ahead). I discuss these extra options in **Other Ways To Connect**.

Set a Wi-Fi Password

When you first turn on Allows Others to Join in Personal Hotspot, the OS creates a strong WPA2 password. To connect a non-linked device over Wi-Fi to the hotspot, you must enter this password on that device.

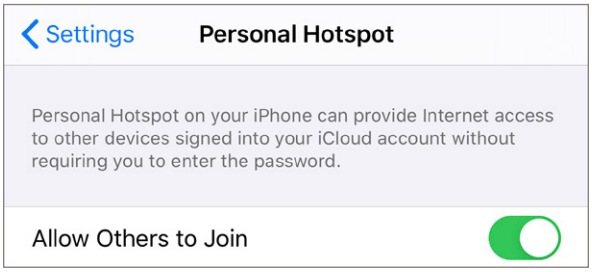

Figure 9: *The Personal Hotspot view lets you control who and what can access it.*

You *must* use a password—Apple doesn't let you have an open hotspot. But you may choose to compose your own. For advice on picking a memorable password that's both secure and easy to enter, see **Create, Manage, and Use Strong Passwords**.

Tip: If you're worried about Wi-Fi at a public location, you can use a Personal Hotspot connection for greater security. Whether via the physical security of USB or the wireless encryption of Bluetooth or Wi-Fi, you're protecting your data more strongly. Although the backhaul to the cellular data network isn't impregnable, it's orders of magnitude less vulnerable than a public Wi-Fi connection.

Use Cell Data while Talking

All iPhones that can handle iOS 13 can let you use data and have a voice conversation at the same time. The technical name is Voice over LTE (VoLTE), referring to the 4G LTE cell standard. (It's also part of new "5G" networks, which so far run 4G technology with a 5G sticker on them.)

VoLTE is often paired with a higher-quality *compression algorithm*, which dramatically improves the quality of a voice conversation by increasing the frequency range. It sounds more natural and less muddy.

Note: Cellular networks have gone through generations: 1G was analog; 2G used digital voice and very low-speed data; and 3G added high-speed data, but it was sort of stapled on, making voice and data impossible to use at once. Even when LTE first appeared, the VoLTE technology wasn't ready. Finally, it's all here!

You can't control whether or not your iPhone will use VoLTE. Two main provisos exist:

- **Carrier must have deployed.** Many carriers around the world have deployed VoLTE. In the U.S., AT&T, T-Mobile, and Verizon have it turned on, while Sprint does not. Some of the country's smaller networks also have it enabled.
- **May have to be on the same network.** VoLTE should work interoperably between carriers, but it doesn't always! As with the first proviso, there's no way to tell and no way to force it to work.

If you meet these requirements, receiving a call or placing one will engage VoLTE, and your Personal Hotspot or other data use will continue at full LTE speeds.

However, if you find yourself on a 3G or slower network, your iPhone will manage a call differently depending on the network:

- **AT&T, T-Mobile, and GSM networks:** GSM networks are used by most carriers worldwide. Data use continues, but is shunted to a slower 3G, 3G+, or some of the rarer 4G network without LTE.
- **Verizon, Sprint, and most CDMA networks:** CDMA networks are rare outside the U.S. Data use, including Personal Hotspot, is immediately suspended.

If you don't answer a call or when you hang up, data use returns to the highest-speed available network.

Name Your Wi-Fi Network

The Wi-Fi network created by a Personal Hotspot has the same name as your device's name. This is typically your name, or that of whichever account you used to set up the device, plus a possessive and the word iPhone or iPad. If you don't feel like broadcasting your account name whenever you turn on Personal Hotspot, you can change it.

To change the name, in iOS or iPadOS, visit Settings > General > About > Name. Tap and revise the name or enter a new one. With the device connected to a Mac, click its icon in Locations in the Finder's Sidebar, then click in its name or select the whole name, type a new name, and press

Return (**Figure 10**). Turn Personal Hotspot off and back on for the new name to be broadcast. (In macOS before 10.15 Catalina, use iTunes and click the device's icon near the top.)

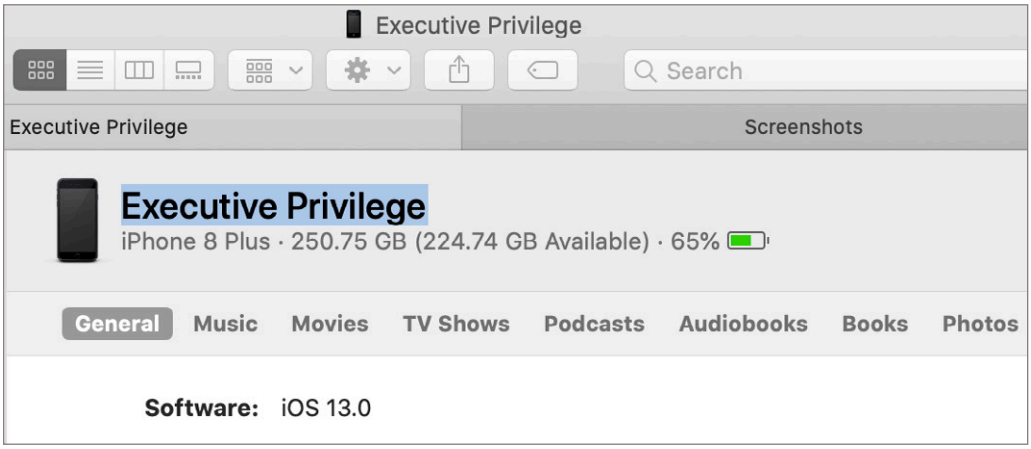

Figure 10: *The Wi-Fi network name is identical to the name of your device.*

Other Ways To Connect

With Allow Others To Join enabled, you and others can use your Personal Hotspot by connecting via one or more of these three ways:

- **Wi-Fi:** Any Wi-Fi–equipped device can connect just as if the iPad or iPhone were a wireless router.
- **USB:** Plugging a computer into your iPhone or iPad offers a high-speed data connection that you know works as long as the cable isn't bad. The downside? Being literally tethered.
- **Bluetooth:** This method requires more steps to make a connection initially, but it gives you cable-free flexibility. Most Bluetooth-equipped devices can connect through this method. No more than three devices may connect via Bluetooth at the same time.

> ***Pick Wi-Fi or Bluetooth?*** *Wi-Fi can consume more battery power than Bluetooth, so you might opt for Bluetooth tethering, but Bluetooth tops out—even in the latest 5.0 spec—at 3 Mbps of raw throughput or about 2.1 Mbps of actual throughput. That's as little as 1/10th of LTE speeds.*

Regardless of your carrier, you can't connect more than five devices across all these methods, although Apple stopped documenting that limit years ago. Additional connections will be refused.

Once you make a connection, a banner appears across the top of the iPhone or iPad's screen (**Figure 11**). iPhones with notches minimize this display to the upper-left corner. The banner shows the number of devices connected, too. The same banner appears on the Lock screen.

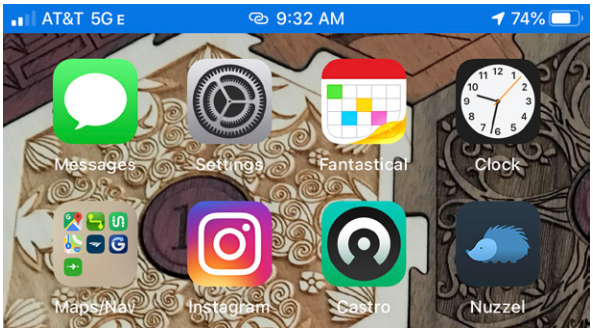

Figure 11: *A banner lets you know whenever Personal Hotspot is in active use.*

> **Note:** Windows computers, Android phones, and other devices can also connect via Wi-Fi and Bluetooth; and Windows can also tether via USB. The process is identical on those platforms to hooking into a Wi-Fi, Bluetooth, or USB shared network.

Access via Wi-Fi

Using Wi-Fi to connect to a Personal Hotspot is the easiest case because no special setup is required. You use whatever method you normally employ to connect to a Wi-Fi network from the device, and I provide directions for several common operating systems just ahead. The name of your iPad or iPhone is the name of the Personal Hotspot network.

Connect via Wi-Fi in macOS

In macOS, you can use the Wi-Fi menu on the menu bar to select the Personal Hotspot network by name:

1. Click the Wi-Fi menu to see a list of available networks.

2. Choose the network's name. If you're part of its iCloud set of devices, it appears under Personal Hotspots as described earlier (**Figure 12**).
3. If prompted for a password, enter it, and click Join.

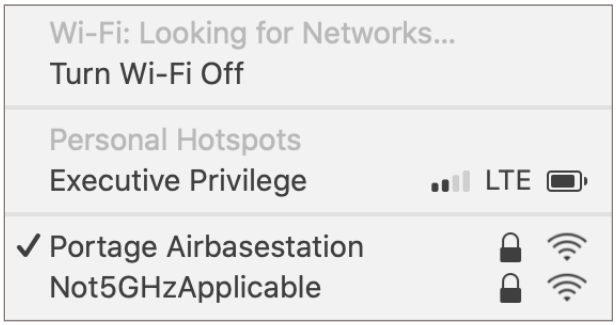

Figure 12: *Select the hotspot under Personal Hotspots.*

Note: If you have iCloud Keychain enabled and connect to a Personal Hotspot that isn't linked to your iCloud account, the password is synced among all your devices. You won't have to enter the password again on any of your other linked hardware.

Disconnect from Personal Hotspot Wi-Fi

To stop using the Personal Hotspot, select the Wi-Fi menu and click Disconnect From *Network Name.* Your link is severed.

Don't join automatically in the future

If you want to prevent the Mac from connecting automatically in the future, follow these steps:

1. Connect to the Personal Hotspot.
2. Open the Network preference pane and click the Wi-Fi adapter in the list at left.
3. Uncheck Automatically Join This Network.

Note: As I write this edition of the book, the above steps don't appear to "stick"—the setting change disappears when you reconnect manually to a Personal Hotspot. I expect this will be fixed in a future macOS release.

Note: Before macOS 10.15 Catalina, you needed to click the Advanced button when viewing the Wi-Fi adapter and then uncheck the Auto-Join box next to the Personal Hotspot network's name.

Connect via iOS or iPadOS

Use the Settings app to connect to the Personal Hotspot network:

1. Select Settings > Wi-Fi.
2. Choose the network from the Personal Hotspots list (**Figure 13**).
3. Enter the password if prompted.

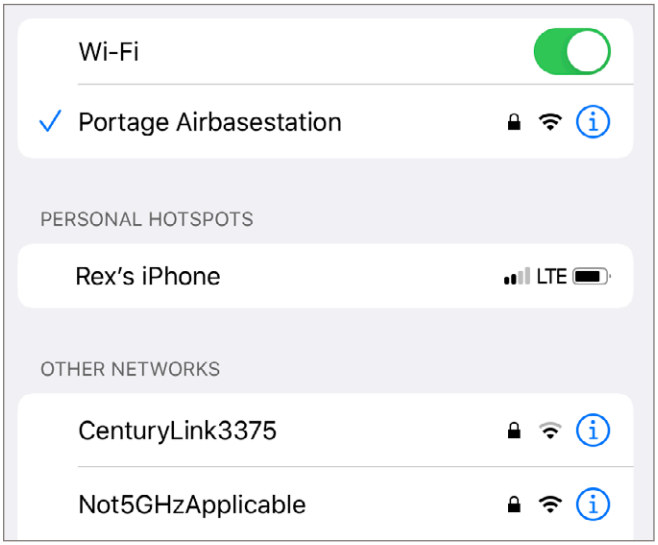

Figure 13: *Look in the Personal Hotspots section (above) or for the chain icon in the Networks/Other Networks list.*

You are now connected. The chain icon appears at the left of the OS's status bar instead of the normal Wi-Fi icon.

To stop using the mobile hotspot right away, choose another network from the list, disconnect Wi-Fi via Control Center, or turn off Wi-Fi.

If the device offering a Personal Hotspot isn't part of your iCloud set of hardware, you can also disable future connections by forgetting the network. While the hotspot connection is active, tap the network name and

then tap Forget This Network. This removes the network's stored setting and also disconnects the device from the Personal Hotspot. However, for iCloud-linked devices, the settings aren't actually forgotten.

Disable Wi-Fi sharing in iOS or iPadOS

To turn off the hotspot on the device that is sharing its connection, just tap Settings > Personal Hotspot and then turn off the Personal Hotspot switch; or, open Control Center and hold down on the networking area, and then tap the Personal Hotspot icon.

You can also block all existing connections from client devices that aren't using iCloud Keychain by changing the Wi-Fi password on the Personal Hotspot screen. This will also prevent devices with a stored password from reconnecting automatically or manually until you provide the changed password. (iCloud Keychain synchronizes the correct password among all connected devices, which means after you reconnect successfully, so will all other devices after they sync.)

Tether with USB in macOS

Connect your iPhone or iPad to your computer using a USB cable. The first time you enable Personal Hotspot and plug the device into a Mac via USB, macOS alerts you that the interface is added and the Mac's Network system preference pane adds an adapter entry (**Figure 14**).

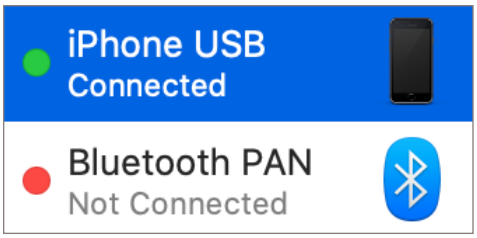

Figure 14: *An entry appears in the adapters list.*

MacOS automatically activates tethering and turns that red dot green.

Note: Apple offers a security feature that disables USB on an iPhone or iPad if it hasn't been unlocked for an hour or more. You may need to unlock your device to get it to tether via USB as a result. A message appears on the lock screen if so.

To halt the active USB tethering connection, disconnect the USB cable. Alternatively, you can disable the iOS or iPadOS adapter profile. In the Network system preference pane in macOS, select the iPhone USB or iPad USB adapter, and then from the gear pop-up menu, choose Make Service Inactive. Click Apply in the lower-right corner.

Tip: The iPhone or iPad USB connection is set by default to activate if no other Internet connection is in place. If you'd like to override that, uncheck the Disable Unless Needed box. Then you can manually enable and disable USB-based Internet access.

Connect with Bluetooth

On your hotspot device, make sure Bluetooth is turned on: Swipe to show Control Center and check that the Bluetooth icon is active. If it's not, tap it. (You can also manage Bluetooth from the Settings app.)

Once you're sure it's enabled, you can make a Bluetooth connection from macOS, iOS, or iPadOS, as I describe next.

Note: I cover Bluetooth in more detail in **Set Up Bluetooth** if you'd like to learn more.

Bluetooth uses less power than Wi-Fi, almost nothing in standby mode, so a Bluetooth connection could allow both an iPhone or iPad and a paired piece of hardware to work longer without AC power.

Bluetooth tethering with macOS

Follow these steps to set up a Bluetooth connection between your hotspot device and a Mac running Yosemite or later:

1. Launch System Preferences, and select the Bluetooth pane.
2. Your iPhone or iPad should appear in the list of devices. Click Pair. (If it doesn't appear, check that Bluetooth is enabled on the iPhone or iPad and that it's within a few dozen feet of your computer.)
3. A pop-up dialog appears with a 6-digit code. On the iPhone or iPad, a similar confirmation dialog pops up (**Figure 15**).
4. Confirm that the code is identical, which prevents a so-called man-in-the-middle attack with someone nearby trying to intercept the connection. (That's very unlikely, but it could happen.) The additional cue

is the name of the device. Click Pair on the hotspot device. On the Mac, your mobile device now appears with the word Connect to its right.

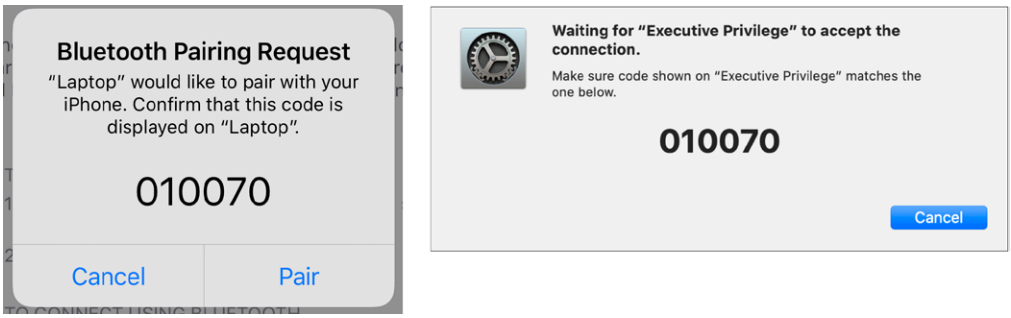

Figure 15: *The iPhone and Mac display the same code.*

5. Now, in System Preferences, click Show All, then select Network.
6. In the adapters list at left, you'll notice a new Bluetooth PAN entry; *PAN* stands for Personal Area Network, and it's the kind of network that Bluetooth creates. Your device should be selected in the Device pop-up menu (**Figure 16**). Click Connect.

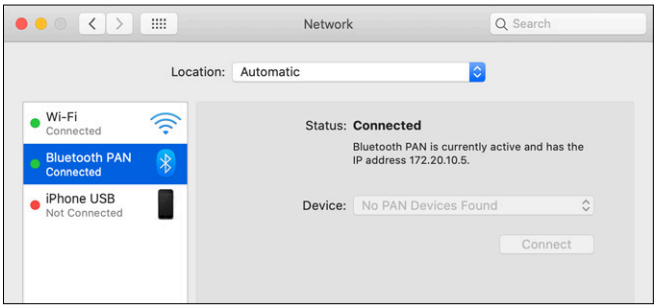

Figure 16: *The Network preference pane lets you manage the connection over USB.*

7. On the Mac, you'll see the Status label set to Connected, and if the Bluetooth system menu ᛒ icon is showing, it will have dots bisecting it. On your hotspot device, the Internet tethering banner will appear.

   To disconnect Bluetooth tethering, you can do any of the following:

- In the Network preference pane, with Bluetooth PAN selected in the adapters list, click the Disconnect button.
- In macOS, from the Bluetooth ᛒ menu (if displayed via the preference pane setting), select the device and select Disconnect from Network.

- On your mobile device, in Settings > Personal Hotspot, tap the Personal Hotspot switch to Off.
- In iOS or iPadOS, open Control Center, hold down on the network area, and then tap the Personal Hotspot icon.
- Turn off Bluetooth networking. In iOS or iPadOS, tap Settings > Bluetooth; on the Mac, look in the Bluetooth system preference pane or the Bluetooth ᛒ menu on the menu bar and select Turn Off Bluetooth.

Bluetooth tethering with iOS or iPadOS

Although all Apple mobile devices have Wi-Fi built in, Bluetooth consumes less battery power and may be a more appropriate choice. You can set up a Bluetooth connection and a hotspot device quite simply:

1. View Settings > Bluetooth.
2. If Bluetooth is off, tap the switch to turn it on.
3. Tap the Personal Hotspot in the list of Devices/Other Devices (**Figure 17**). Both devices show confirmation dialogs. (It appears in My Devices if it was previously paired.)

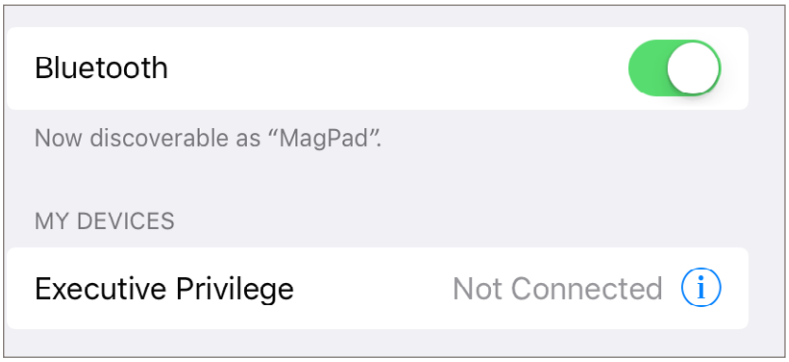

Figure 17: *The hotspot appears in the My Devices list; here, it’s “Executive Privilege.”*

4. If the codes match, tap Pair on both devices.

   The device is now connected over Bluetooth, and a chain icon appears in the status bar instead of the normal Wi-Fi icon.

   To disconnect from the Personal Hotspot:

- **On the connected device:** In Bluetooth settings, tap the Personal Hotspot device and then tap Disconnect.
- **On the hotspot:** Turn off or disconnect Personal Hotspot or turn off Bluetooth.

  To reconnect, open Settings > Bluetooth and then tap the Personal Hotspot, which now appears in the My Devices list.

> **Tip:** You might want to discard a stored Bluetooth pairing from the My Devices list. Tap the info ⓘ button next to the device name and then tap Forget This Device.

Use Bluetooth Tethering from iOS or iPadOS to a Laptop

A side benefit of the capability to tether over Bluetooth is that you can also use your mobile devices to grab Internet access from a laptop. For instance, if you're in a hotel or other location in which you have to pay for each device you connect to a Wi-Fi network, this may make financial sense.

Under macOS, use the Sharing preference pane's Internet Sharing option to share the Wi-Fi connection via Bluetooth PAN. Choose Wi-Fi from the Share Your Connection From pop-up menu, and check the Bluetooth PAN box in the To Computers Using list. Then check the box next to Internet Sharing in the Service list at left.

Consider Turning Off Certain Radios

You might not want your hotspot to be available through Bluetooth or Wi-Fi, as your nearby devices might accidentally connect to it. The only way to prevent that is to turn off those radios. If you use Settings > Wi-Fi or Settings > Bluetooth to disable either or both of those radios, this can also disable a number of other features in the OS, like Continuity and Apple Watch connectivity.

For that reason, starting iOS 11 you can use a standby mode via Control Center. Swipe to show Control Center and tap Wi-Fi or Bluetooth: they switch to Not Connected. This leaves the radios on, but doesn't allow Personal Hotspot connections through those networking methods. (This is explained further in **Airplane Mode**.)

Control Center lets you see Personal Hotspot's status at a glance. Swipe to reveal Control Center and hold down on the networking area to reveal an expanded network view.

This area includes AirDrop and Personal Hotspot in addition to Airplane Mode, Cellular Data, Wi-Fi, and Bluetooth (**Figure 18**). Every mode has text beneath that shows that method or feature's status.

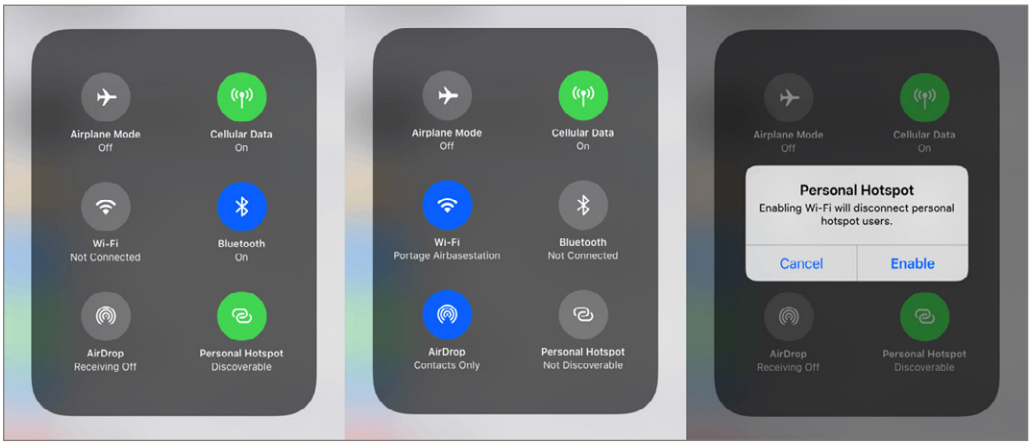

Figure 18: *From left to right: hotspot on and Wi-Fi unavailable; Bluetooth and hotspot on standby; and trying to re-enable Wi-Fi with the hotspot running.*

Choose to Use Cellular Data or Wi-Fi

There are plenty of good reasons to pay attention to whether your iPhone or cellular iPad is accessing the Internet via a Wi-Fi network or mobile broadband. You may need greater bandwidth than the cellular network can provide, or be budgeting data on a low-bandwidth plan or while traveling.

Whatever the reason, you can determine which network you're on and set the type of network to which your device connects. And you can even enable a hybrid mode that taps into cellular data when Wi-Fi is flaky.

Which Network Are You On?

iOS has an indicator in the status bar that shows which network connection is active. The range of throughput is huge (such as 30 to 300 Mbps with the fastest methods), because there are such wide ranges of generations of cellular networks and Wi-Fi base stations in use.

And each mobile device supports many rates for each standard while also offering backward-compatible support for older networks.

Here's what the indicators mean:

- **No service:** Can't connect to any network.
- : Connected via Wi-Fi. The number of waves, from a dot to three, indicates signal strength. Downstream rates from can be as fast as 1 Gbps with an iPhone 11 or 11 Pro and the newest Wi-Fi 6 gateways.
- **Wi-Fi:** Wi-Fi Calling is enabled.

- **5GE:** Marketing letters for the fastest available LTE, rather than the 5G networking technology revision that is not available on Apple phones—or really almost any phones. Downstream rates can top 40 Mbps, but will increase as deployments get denser. Upstream can top 10 Mbps.
- **LTE:** Connected via LTE. Downstream rates can top 20 Mbps. Upstream is several Mbps.
- **4G:** Connected via 4G (on GSM networks only). About 6 Mbps downstream and below 2 Mbps upstream.
- **3G:** Connected via 3G. Maximum rates vary by network from 1.4 Mbps (CDMA) to 4 Mbps (GSM) downstream and hundreds of Kbps to over 1 Mbps upstream.
- **E:** Connected via EDGE, a 2.5G standard (GSM only). About 200 Kbps downstream and 40–50 Kbps upstream.
- **GPRS:** Old 2G networks, about 40–50 Kbps in each direction.

Select Which Service to Use

You can force a cellular device to use either cellular or Wi-Fi service instead of letting it automatically switch depending on whether or not a suitable Wi-Fi network is available. Because iOS and iPadOS don't offer network profiles as in macOS, which would make it easy to switch, you must use the Settings app to enable or disable a service.

To enable or disable cellular data service:

- To use just a cellular connection and avoid Wi-Fi, perhaps to keep a continuous VPN connection or for security reasons, either:
  - Swipe to show Control Center and tap the Wi-Fi icon to disconnect.
  - Tap Settings > Wi-Fi, and then set the Wi-Fi switch to Off.
- To rely only on Wi-Fi, accepting that you may have times during which you have no Internet connectivity:
  - Swipe for Control Center and tap the Cellular Data icon to disable it.
  - Tap Settings > Cellular Data (iPad) or Settings > Cellular (iPhone), and then turn Cellular Data off.

Note: In the case of an iPad, turning off cellular data disables all mobile network access; for an iPhone, voice calling, voicemail, and messaging remain available.

If a Wi-Fi network is acting flaky, you can avoid the problem in one of three ways:

- Use Wi-Fi Assist (**Figure 19**). This option, set in Settings > Cellular (iPhone) or Cellular Data (iPad)—swipe way way *way* down to the bottom—taps into mobile broadband when Wi-Fi connectivity is too poor to use. Apple says it won't download attachments, use background downloading, or let third-party apps stream audio or video so as not to burn through all of your cellular data plan. Wi-Fi Assist shows the total data it's used, if any, in small text beneath its label since the last time statistics were reset.

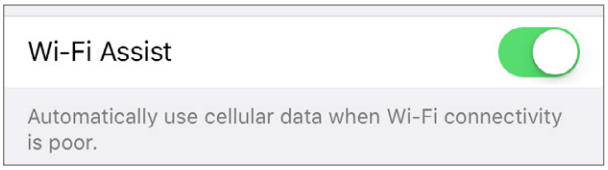

Figure 19: *Wi-Fi Assist swaps to cellular as needed.*

WARNING! *Some people have had problems with Wi-Fi Assist, where they believe (based on their bills) that it consumes cellular data for kinds of activities Apple says the feature shouldn't, and even when the user believes their iPhone is continuously connected to Wi-Fi. This makes me suggest that you disable it—it's turned on by default!—unless you have a particular situation in which you feel it's worthwhile.*

- Switch off Wi-Fi, and force the use of cellular data.
- Use the method noted in **Forget This Network** to disconnect the Wi-Fi network. Wi-Fi is still enabled, but not used when it has no network connection.

Manage Cell Data Usage

When Apple introduced the iPhone, it convinced its first carrier, Cingular (subsequently bought by AT&T), and then other carriers to offer unlimited data plans in the U.S. and a few other places. As smartphones multiplied and networks became congested, carriers pushed back and started limiting "unlimited" plans and offering fixed amounts of data, while charging overages beyond that.

In 2019, the pendulum has swung way back in many places. Carriers in many countries charge a flat rate and throttle throughput after a certain amount of data has been used. Some carriers offer something close to unlimited to most people: 20 to 50 GB of data per month before throttling. There are still many provisos, but overage fees have largely disappeared.

Carriers Shift to Throttling

All four major U.S. cellular carriers have no overage fees, and some offer what are effectively unlimited data by throttling after a set amount of data has been used in an individual or pooled family plan in a billing period.

Limited-use plans from AT&T, for instance, offer cheaper options for a single line or families that pool 3 GB or 9 GB. After you exceed that limit, your account throttles to 128 Kbps for the remainder of the billing period.

"Unlimited" plans from all four carriers rely on congestion throttling. In that scheme, you will get at least 128 Kbps or 3G after some amount of use, depending on the network. However, you can still achieve LTE rates if the area in which you're using your device isn't congested at the moment. (The one exception is Verizon's lower-tier plan, where congestion throttling can happen at any time.)

Tethering for hotspot use also varies from carrier to carrier, typically limiting usage as a fraction of an "unlimited" plan. With T-Mobile, for example, you get 50 GB of unthrottled use each month on your smartphones and tablets, after which you're given lower priority for data on congested networks. However, Personal Hotspot isn't available on its cheapest plan, and is limited to 3 GB and 15 GB per month on its middle- and top-tier plans.

Tip: Some smaller carriers in the U.S., like Red Pocket and Ting, have national coverage and let you set relatively small amounts of data use—like 500 MB to 1 GB— to keep monthly costs lower, sometimes half as much as the lowest major-carrier plan.

Keep Usage Restrained

You can have full-speed mobile access when you need it without breaking your limits if you ration usage. What you need is a strategy.

Enable Low Data Mode in Cellular Settings

Starting in iOS 13 and iPadOS 13, you can enable Low Data Mode in Settings > Cellular (iOS)/Cellular Data (iPadOS) > Cellular Data Options. This turns off background data use by third-party apps and limits activity by the OS (**Figure 20**).

This means you have to check email manually and perform other updates "by hand." It effectively limits data use to the foreground app you're using. This can be a great tool for reducing accidental data usage.

Tracking Cellular Usage on an iPhone

An iPhone shows your locally tracked consumption of cellular data via Settings > Cellular > Cellular Data under Current Period. This number has two problems:

- It's not guaranteed to be accurate. Your carrier's records are definitive (**Figure 21**). In practice, it's pretty close.

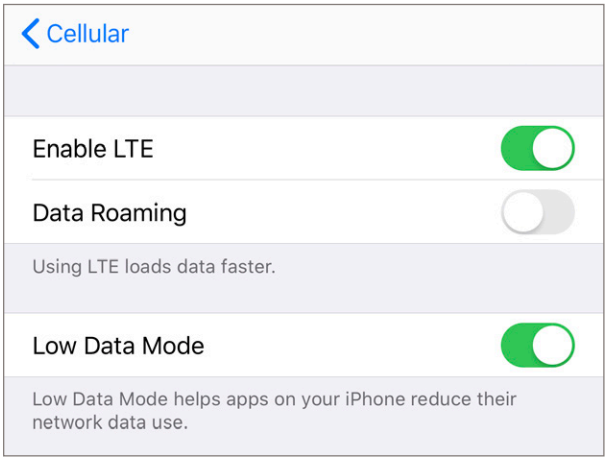

Figure 20: *Low Data Mode reduces cellular data usage by background apps.*

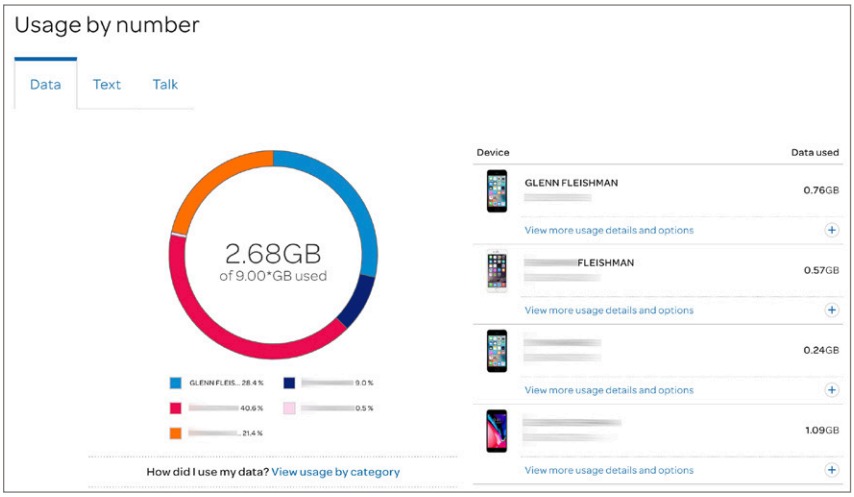

Figure 21: *AT&T's online data statement is the only one you can rely on for billing.*

- It isn't aligned with your billing period. Rather, it's a total of all data consumed since the last time you tapped Reset Statistics at the very bottom of the Cellular or Cellular Data view.

  If you'd like this number to be more useful, set yourself a reminder in your calendar for the first of each month (or the start of your billing period if it's another increment) to visit Settings > Cellular and tap Reset Statistics.

You can find out how much data you've used specifically for Personal Hotspot by tapping its item the Cellular/Cellular Data view. It even tells you usage by devices that it can identify via tethering (**Figure 22**).

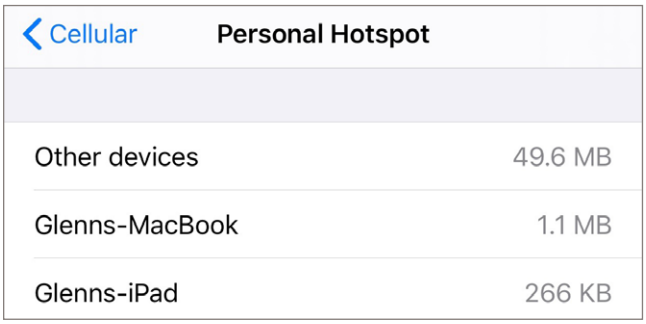

Figure 22: *Discover Personal Hotspot's portion of overall cellular data.*

Check Cellular Usage on an iPad

A Wi-Fi + Cellular iPad has an additional way to track usage via the Settings > Cellular Data > View Account screen, which shows details from the carrier, including the billing period, how much data is included, and the data consumed so far in that period.

Turn Cellular Data On Only When You Need It

There are times when you'd prefer not to have an active cellular connection or cellular data link on an iPhone or cellular iPad, notably when you're close to the throttle limit of your service plan or traveling outside an area included in your data plan. You can change how the cellular radio interacts with a network in two ways:

- To turn off data only, in Settings > Cellular (iOS)/Cellular Data (iPadOS), turn off the Cellular Data switch. You can also tap the Cellular Data icon in Control Center. This disables the data link only. With an iPhone, you can still place and receive voice calls and send and receive SMS/MMS text messages.
- To shut off the entire cellular connection, set Airplane Mode to On in the upper left of the main Settings screen, or tap the Airplane Mode button in Control Center. Airplane Mode turns off Bluetooth, Wi-Fi, and cellular

radios, although you can re-enable Bluetooth and Wi-Fi separately. See **Airplane Mode** for details. It also dramatically extends your battery life in most cases.

You can also control other cellular data parameters:

- Turning off Cellular Data Options > Enable LTE will eliminate use of LTE and so-called 5GE networks and rely on slower connection methods. This is useful when LTE/5GE networks near you are spotty and you're having trouble staying connected as your device swaps back and forth between 2G/3G and LTE/5GE. This may also reduce battery use.
- In some markets, the Enable LTE option may read Voice & Data, and let you pick 2G, 3G, or LTE as network options.
- Data Roaming can ensure that you don't consume expensive mobile bytes while you're outside the home area for your carrier. In some cases, you might have limits; in others, you might be charged.

Limit Your Activities on the Cell Network

Unless you are connected to the Internet via Wi-Fi, limit your online activities to those that low-data purposes, such as checking email or viewing web pages.

Various items in Settings let you limit whether cellular data can be used for an app or activity, including:

- Use the options in Cellular (iPhone) or Cellular Data (iPad) to prevent excessive use of certain services from consuming a lot of your data allocation. You can turn on and off specific apps, and see their data consumption (see **Figure 23**).
- In Cellular (iPhone) or Cellular Data (iPad), swipe to the bottom and you can disable syncing iCloud Drive over cellular.
- In the iTunes & App Stores, you can disable cellular data for automatic downloads. But if you enable Apps or App Updates for automatic download, you can also separately choose to be asked whether to download each app or only asked about apps larger than 200 MB.

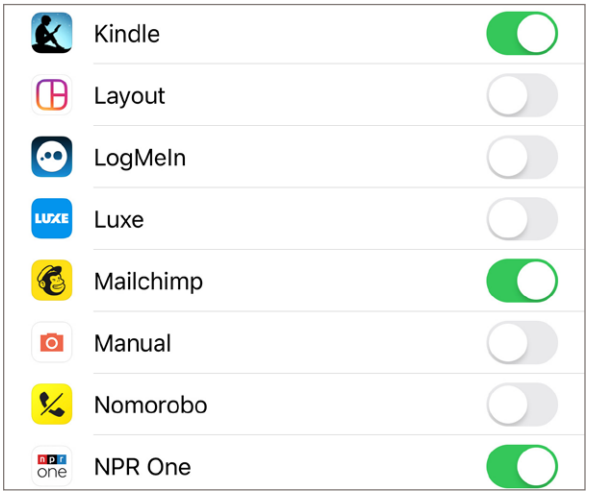

Figure 23: *Opt out of using cellular data for certain iPhone apps.*

- In Music, turn off the Cellular Data option to rely just on the library present on your device. You can also tune your option, allowing streaming with High Quality Streaming disabled.
- Cache data you need. Plan ahead and download for offline use from cloud or other services. For instance:
  - Use Google Maps offline. While it doesn't burn up lots of data while online, its offline mode lets you consult interactive maps when there's no network connection. Enter a place name, tap the name at the bottom, then tap the three stacked dots at upper right. Finally, tap Download Offline Map.
  - Use the Music or Videos apps, find items you want, and tap the cloud icon to download them locally.
  - Amazon and Netflix users can download certain movies and TV shows via the respective app for offline playback.
- You can also enable or disable kinds of cellular use via settings within certain apps even when you've allowed the app to use cellular bandwidth. For instance, the podcast app Castro has a cellular data switch in its Downloads area to let you opt to download episodes over either Wi-Fi and cellular or Wi-Fi only (**Figure 24**). But even with that switch set, you can still stream episodes over a mobile network (and Castro warns you that you're streaming).

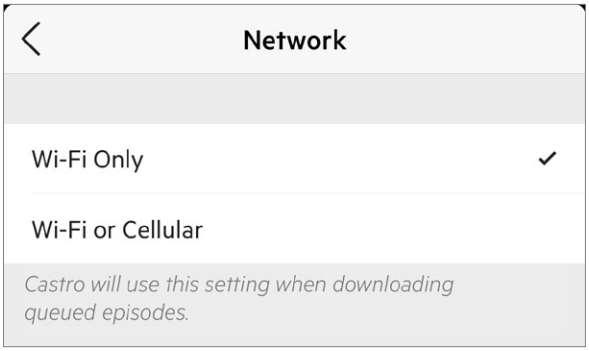

Figure 24: *Castro lets you choose to limit downloads to Wi-Fi.*

More generally, you should avoid using or disable the cellular use in Settings for:

- Audio-streaming apps, such as those used by radio stations and networks. Usage is generally small, but it can add up.
- Video-streaming apps like Hulu Plus, YouTube, Netflix, and Vimeo. It's easy to run through a gigabyte or more in an hour, depending on your device and connection. Some carriers automatically throttle video streaming or even include it as a separate feature to reduce unnecessary data use.
- Photo-browsing apps like Flickr. Depending on the app, even swiping past a photo might download a megabyte or more.

Note: Depending on your carrier and other parameters, you should receive push notifications, text messages, or both as you approach or exceed whatever the included monthly cellular usage total is before throttling.

Place Calls via Wi-Fi

Cellular phone calls are just data. The stream of audio data that composes them, however, can be routed in different ways depending on the generations of cellular technology that a phone supports and on how carriers choose to configure their networks. Wi-Fi Calling effectively extends cellular calling to home and office Wi-Fi networks. It's seamless once enabled besides displaying a tiny Wi-Fi label in the status bar.

Wi-Fi Calling is great when a good cell signal isn't available, often inside a building or house. Carriers that offered similar features used to provide incentives for using Wi-Fi, like unlimited domestic calling. But now they just extend your voice plan to Wi-Fi, whether it's unlimited or otherwise.

Note: All four major U.S. carriers support Wi-Fi Calling, but it varies with smaller carriers and with phone operators outside America. **Consult Apple's page** that shows features supported by carriers worldwide.

Note: Wi-Fi Calling is distinct from Voice over LTE (VoLTE), a method of routing voice calls over LTE mobile networks. I discuss that in the Personal Hotspot chapter, in the section "**Use Cell Data while Talking**."

Turn On Wi-Fi Calling

Apple doesn't turn on Wi-Fi Calling by default. Instead, you have to enable it, and then walk through a variety of steps that vary by carrier.

Enable Wi-Fi Calling on Your Main Device

Start in Settings > Phone > Wi-Fi Calling (**Figure 25**). Once you tap the switch, you're prompted to enable Wi-Fi Calling.

Figure 25: *You have to tap the switch and then agree to enable Wi-Fi Calling.*

> **Tip:** If you know your carrier offers Wi-Fi Calling, but its switch is dimmed out, Apple suggests restarting the phone. If that doesn't work, try resetting your iPhone's network settings by going to Settings > General > Reset and tapping Reset Network Settings.

If all goes well, you proceed through a set of steps that warn you about emergency calls, and have you fill out the address at which you typically use the phone with Wi-Fi Calling (**Figure 26**).

It's relatively easy for 911 service to pinpoint you on a cellular-connected call, because your phone has to connect to a nearby tower. For a Wi-Fi-based call, location can be provided by GPS and other factors, but it's not as neat a process. Hence the form to fill out.

When you place an emergency call with Wi-Fi Calling active, Apple says the iPhone will first try to reach a cellular network. If a cell network can't be used, the address you enter for Wi-Fi Calling may be the one that's sent as a fallback to responders.

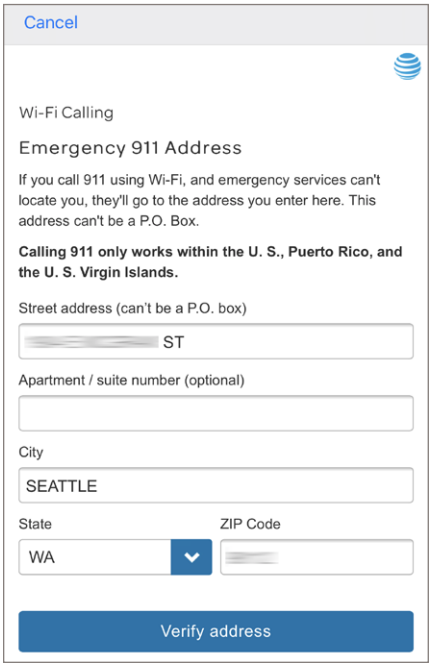

Figure 26: *Your address entered for Wi-Fi Calling becomes the default used if no better location can be derived from your phone.*

When you've entered your address and tapped Verify Address, the carrier checks to make sure the information you entered matches a legitimate address. If not, you're prompted to correct it; otherwise accept it. You're told that Wi-Fi Calling will be available in a few minutes; tap OK. Whenever it's active, the word "Wi-Fi" appears following the carrier's name in the status bar.

Once Wi-Fi Calling is active, you can enable and disable it at will by tapping its switch (**Figure 27**). This may be necessary if you wind up on a Wi-Fi network with inconsistent quality.

Enable Wi-Fi Calling on Other Devices

Apple's Continuity feature, introduced a few OS releases ago, allows you to make cellular calls from iPads, iPod touches, and macOS devices on the same Wi-Fi network as your iPhone. Wi-Fi Calling extends that, letting you call even when your iPhone isn't nearby! (However, you can't use other iPhones!)

Figure 27: *Once Wi-Fi Calling is enabled, you can disable it with a tap or update the stored emergency address. You can also use this view to control whether other devices can use Wi-Fi Calling.*

> ***Which devices work with Wi-Fi Calling?*** *An iPad or iPod touch has to be running iOS 9 or later; an Apple Watch needs watchOS 2 or later; and a Mac has to have El Capitan or later installed, and be a model released in 2012 or later, except the 2012 Mac Pro.*

First, make sure Add Wi-Fi Calling for Other Devices is active in Settings > Phone > Wi-Fi Calling or the same panel in Settings > Cellular (see **Figure 27**, above). Then, in Settings > Phone > Calls on Other Devices, tap Allow Calls on Other Devices (**Figure 28**). This may already be enabled if you were previously using Continuity for cell calls.

> **Note:** Not all carriers offer what Apple clunkily describes as "Wi-Fi Calling on supported iCloud-connected devices." It's offered by the big four U.S. carriers, however.

Now tap Add Wi-Fi Calling for Other Devices. It may take a moment for this to become active. On each iPhone, iPad, or macOS computer logged into the same iCloud account, you can now use Wi-Fi Calling. You may

get alerted on every device with a warning asking if you want to upgrade to Wi-Fi calls on the device you're on. You can click Turn On or Not Now.

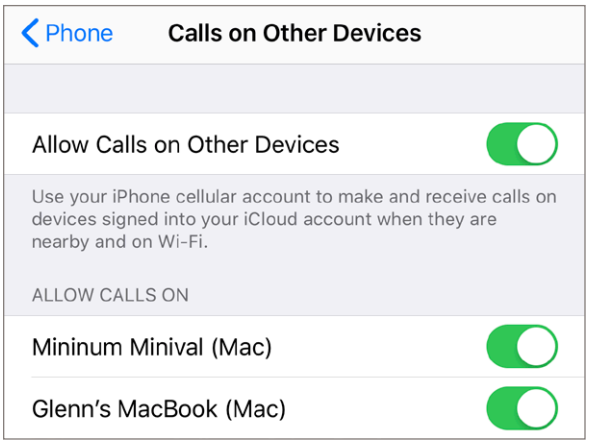

Figure 28: *You can share Wi-Fi Calling among all your iCloud-linked devices.*

If you don't see that dialog, or you click Not Now, you can upgrade at will. In iOS or iPadOS, go to Settings > FaceTime > Calls from iPhone, and tap Upgrade to Wi-Fi Calling. In macOS, launch FaceTime, and then select FaceTime > Preferences > Settings, check Calls From iPhone, and click Upgrade to Wi-Fi Calling. You're asked to confirm in both cases.

A dialog with a six-digit code appears on the device you're adding, if it's the first time for that device. Enter that your iPhone and tap Allow (**Figure 29**). You can update your emergency address on any linked device, or disable cellular-linked calls, too.

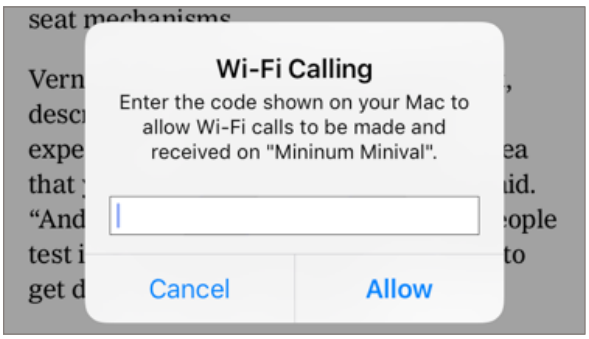

Figure 29: *The first time you use another device with Wi-Fi Calling, it shows a six-digit code that you have to enter on your iPhone to authorize it.*

Airplane Mode

Before you're flying so high with some guy in the sky, you need to disable radio communications on your mobile device. The Airplane Mode switch makes this simple.

The U.S. allows the use of handheld personal electronics below 10,000 feet, even though laptops and other large devices are supposed to be stowed so they don't become projectiles. (1,000-page books are still fine, bizarrely.)

Cellular radios remain banned, and one ostensibly isn't supposed to use Bluetooth at all, and should not turn on Wi-Fi unless in a plane equipped with Wi-Fi service.

The FAA Caught Up with Science

Until a few years ago, the FAA enforced a kind of commercial urban myth: that the cellular radios in cell phones as well as the circuitry in personal electronics like an ebook reader could cause interference with the avionics (electronic flight systems) on commercial aircraft.

This was out of an abundance of caution even years after it was clearly proven that there was no such risk—and after it was shown that cell phones are routinely left on, or even used, in flight without any adverse effects.

What's Airplane Mode?

Airplane Mode is available to all iPhones, iPads, and Apple Watches, and is a simple way to set your device to a legally required quiet mode during flight. In the Settings app, tap the switch next to Airplane Mode. You see an airplane ✈ icon in the top status bar when the mode is active.

Saves battery life, too: *If you don't need to use any of the radios for network access, peripherals, or location, Airplane Mode is an effective way to extend battery life, too.*

With a Watch, turning on Airplane Mode one enables it on its paired iPhone and vice-versa.

When you turn on Airplane Mode in the Settings app—or by swiping to show Control Center and tapping the airplane ✈ icon—the OS turns off three separate radio systems on an iPhone, cellular iPad, and cellular Watch: cellular, Wi-Fi, and Bluetooth. On a Wi-Fi–only iPad or any iPod touch or non-cellular Watch, Wi-Fi and Bluetooth are disabled.

GPS works in Airplane Mode: *Once, Airplane Mode disabled the GPS radio, even though there was no reason for that, as the radio passively receives signals from satellites. For years now, you can use GPS positioning with a map that has data stored offline, to track your path with GPS coordinates, and to geotag photos and other documents.*

On flights on which Wi-Fi is available for Internet access, you can separately tap and re-enable Wi-Fi in the Settings app. Some people also use Airplane Mode to reduce battery usage by disabling its radios, and turn Wi-Fi on for local network access.

When you turn off Airplane Mode, all your previous settings for access are flipped back on. With a Watch, you have to separately disable Airplane mode on both the Watch and its paired iPhone.

To Sleep, Perchance To Transmit

When you push the Sleep/Wake button on the top or side of your device to put it to sleep, you might think the entire device is suspended. But this standby mode is pretty active. Certain background operations continue, and a cellular iPad, cellular Watch, and any iPhone can receive email and other updates via push over a cellular data connection.

The OS also maintains Wi-Fi connections on a minimal continuous level. Sleep is more like lightly daydreaming. That's a reason to use Airplane Mode: to prevent all of this from happening when you don't intend it to.

When Radios Turn Off and When They Don't

You can choose to separately turn off some radios:

- Wi-Fi: In Settings, tap Wi-Fi, and set Wi-Fi to Off.
- Bluetooth: In Settings, tap Bluetooth, and set Bluetooth to Off.
- GPS: Tap Settings > Privacy > Location Services, and set Location Services to Off.

> ***Is GPS really off?*** *GPS is a receive-only system; with Location Services off, ostensibly, the GPS receiver isn't powered up and attempting to find data.*

> ***WARNING!*** *Disabling Location Services prevents the OS from using GPS, Wi-Fi, and cell-tower based information to determine location.*

There is no way to entirely disable the cellular radio separate from Airplane Mode. You can only opt to disable cellular data and some cellular modes, as discussed in **Manage Cell Data Usage**.

The buttons in Control Center in iOS and iPadOS for Wi-Fi and Bluetooth don't turn those radios off, but put them into a kind of standby mode. When you hold down on the networking area, it expands to show six networking features or radios with text labels beneath. Tapping Wi-Fi or Bluetooth toggles them between a blue active state and a white Not Connected state.

Apple distinguishes between this standby state and fully off to allow the OS to continue to work with Apple-specific features like AirDrop, Handoff, and Location Services, and keep connected to hardware like the Apple Watch and the Apple Pencil.

Wi-Fi re-enables if you tap its button, connect to a network via Settings, or walk or drive to a new location. Bluetooth re-enables if you tap its button or connect to a peripheral. Both leave standby mode when you restart your device and at 5 a.m. local time.

Set Up Bluetooth

Bluetooth wireless networking lets you connect peripherals like battery-powered headphones, earpieces, headsets, and keyboards to an iPad or iPhone for listening to music and entering text. It's also the glue that binds together devices for Continuity's Handoff features and connects the Apple Watch with an iPhone by default.

While this book covers aspects of Bluetooth elsewhere, read this chapter to learn how to set up and manage Bluetooth devices.

> ***Tethering:*** *Bluetooth can provide Internet service to an iPhone or iPad from another piece of hardware, such as an iPhone with Personal Hotspot enabled, a laptop, or a cellular router with Bluetooth as an option. See the earlier chapter* ***Make a Mobile Hotspot*** *for details.*

Bluetooth Basics

The Bluetooth SIG, a trade group, certifies devices as Bluetooth compliant for particular profiles, which include things like text entry, stereo audio, file transfer, and modem access. Apple's mobile devices work with any device that meets the Bluetooth spec for several profiles, including audio, peer-to-peer transfer, and external keyboards.

When you connect with Bluetooth, the process is known as *pairing*. Some devices can be paired with several hosts (like computers or mobile devices); others can pair with only one host at a time, and must be re-paired to switch. Bluetooth devices are discoverable when they are set to allow a pairing connection.

Bluetooth is handled from the Bluetooth view (Settings > Bluetooth). This view lets you turn Bluetooth on and off and displays a list of Bluetooth

peripherals under My Devices and Other Devices. The My Devices list shows any devices that have been previously attached to the device and the current status of such devices. The Other Devices list displays any discoverable devices within range. (It's labeled just Devices before you connect any Bluetooth device.)

Bluetooth and Low Energy (LE)

Bluetooth 4 brought a low-power mode called Bluetooth LE (sometimes called Bluetooth Smart) to the mix. It lets devices with tiny batteries that are meant to be changed infrequently communicate in tiny, power-conserving bursts. You could have Smart devices in your home's alarm system, and an app could let you tap to see if any windows are ajar, for instance.

Apple has used Bluetooth LE extensively in later releases of iOS, iPadOS, and macOS to enable signaling between devices for AirDrop (see **Pass Files with AirDrop**) and some of the Continuity features, like Instant Hotspot (see **Turn On via Another Device**).

Bluetooth LE is also used to communicate with the Apple Watch, and is a key part of HomeKit, Apple's home-automation technology. With both the Watch and HomeKit, Wi-Fi is a fallback when Bluetooth signals don't reach, but it consumes much more power on both ends.

Apple supports Bluetooth 5 in many of its devices, which builds on features in version 4, while increasing throughput and range.

Pairing Any Device

To start pairing, follow these general steps (the specifics for particular profiles are given later in this chapter):

1. Tap Settings > Bluetooth.
2. Activate Bluetooth discovery on the other device if required. This may require enabling a setting or holding down a button (sometimes a special pairing button) for several seconds.

   On your mobile device in the Bluetooth view, the other device appears, naturally enough, in the Other Devices list (**Figure 30**).
3. Tap the desired device. The OS attempts to connect.
4. Depending on the device, the OS will do one of the following:

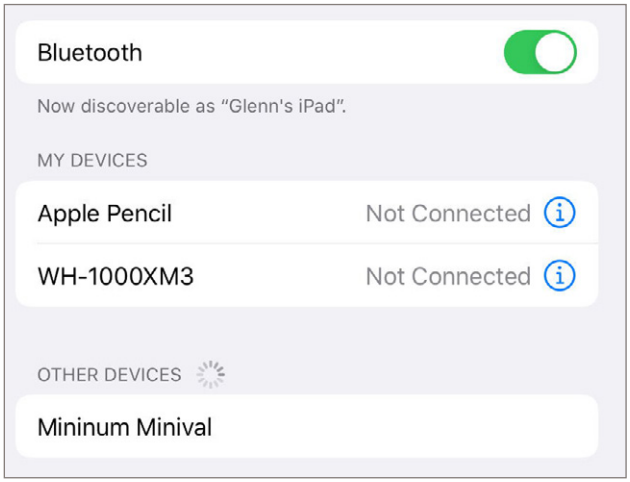

Figure 30: *An unpaired device (my Mac mini) is discovered.*

- Simply proceed: The OS pairs without requiring a code or confirmation. You'll see this with simple devices.
- Show a Pair button: In some cases, you don't need to type a pairing code, but you get a dialog like the one in **Figure 31** on each device. Compare the code, and tap Pair on each to confirm.

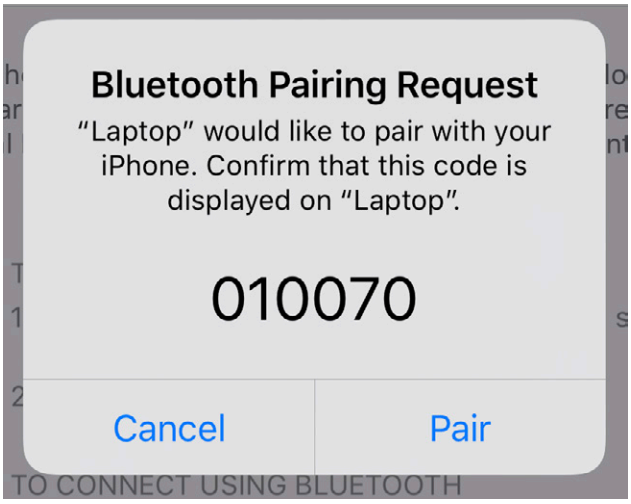

Figure 31: *iPhones, iPads, and Macs just ask you to confirm.*

- Show a field in which you enter a code: The code will either be provided by the other device or—in the case of a peripheral without a way to choose or display characters—noted in its manual. It's typically `0000`.

- Display a code that you enter on the other device: Your device generates a PIN (called a "passkey" here) to be entered in the pairing device.

The paired device is now shown as Connected in the list.

> ***Prevent accidental pairing and attacks:*** *The reason you're asked to confirm a code is to ensure that nobody else is attempting to control the two devices trying to pair. The cryptography behind this prevents your two devices from seeing the same code if someone had managed to interpose themselves into the pairing. You could see a different code if someone else nearby happened to be trying to pair a Bluetooth device at the same time, however!*

Settings shows a Connected label for paired devices that are turned on and available, and Not Connected for those that aren't in range or are turned off (**Figure 32**).

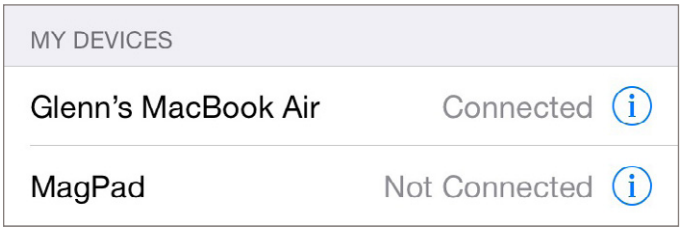

Figure 32: *This MacBook Air is paired and connected; the iPad is paired but not connected.*

Disconnect hardware from Bluetooth by tapping the info ⓘ button and tapping Disconnect.

> **Tip:** To remove a pairing, select the peripheral in the Devices list, tap the info ⓘ button, and then tap Forget This Device.

> ***WARNING!*** *If you walk away from a Bluetooth keyboard while it's still on, it can maintain a connection over a long distance. I was mystified as to why I couldn't get an on-screen keyboard to appear on my iPad when two rooms away from an Apple Wireless Keyboard until I recalled I hadn't turned it off.*

Hands-Free Profile

The Hands-Free Profile in Bluetooth lets you have audio conversations using the mic and headphones (or speakers) on a variety of devices, such as over-the-ear or in-ear headsets. You pair a device just as described in **Pairing Any Device**, earlier.

On an iPhone, you can answer incoming calls by tapping the answer button on the headset. When you place a call, the last chosen mic/headphone is used, but you can pick from the available options, even as the call is underway, by tapping the Audio button. In the example in **Figure 33**, I could choose from a Jawbone mic/speaker device, the iPhone's earpiece/mic, or the speakerphone option on the iPhone.

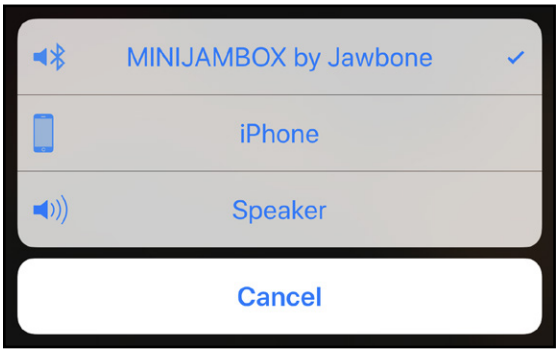

Figure 33: *When placing a call, you can choose a Bluetooth device.*

Picking an audio source also works to let you use a headset for other programs, such as Skype or FaceTime, that don't require a cellular network or an iPhone.

Audio Devices

Once you've paired stereo headphones, you can use them just as you would headphones plugged into any iPad or iPhone. You can tap the start, stop, and other controls in an app playing back audio, or, if your Bluetooth headphones or headset has these controls, you can handle those options remotely.

Tip: While AirPods are wireless audio devices and use Bluetooth, Apple has created a simplified and improved pairing process for iPhones and iPads that bypasses normal Bluetooth settings.

Apps that allow audio playback should show a special AirPlay icon when multiple audio output options are available. You can also swipe to reveal Control Center and change all mobile audio output to another audio device. (See **Stream Music and Video with AirPlay** for more about that technology.)

Tap the icon to pick an audio destination, which includes the device's built-in speakers, active Bluetooth headphones, and any Apple TVs or AirPlay speakers connected to your network (**Figure 34**). Audio continues to play throughout and seamlessly switches whenever you tap.

Figure 34: *Tap the AirPlay button in the audio playback controls to choose among available audio output destinations.*

If you have devices that support AirPlay 2 for multiple simultaneous audio streaming, they appear with a circle to their right. Tap the circle to add the output to your set of streaming devices.

You can stop using Bluetooth audio destinations in several ways:

- Turn off the Bluetooth device.
- On your iPhone or iPad in Settings > Bluetooth, in the entry for the headphones, tap the info ⓘ button, tap Forget This Device, and then tap OK.
- Move the iPhone or iPad and the Bluetooth device out of range of each other. I like this option least, because Bluetooth can work over a long range. If, for example, you leave your headphones at home and take your mobile device with you, then this option makes sense.

  In all cases when the Bluetooth device can't be reached any longer, audio output reverts to the speakers automatically.

Pass Files with AirDrop

AirDrop lets you pass photos, URLs, contact cards, and any arbitrary file from a Mac, iPhone, or iPad to another of any of those kinds of hardware on the same Wi-Fi network. It's a neat way to bypass email, text messaging, or a sync service like Dropbox.

Configure AirDrop

AirDrop is one of the simplest pieces of iOS and iPadOS technology. There's only one set of choices to make (**Figure 35**).

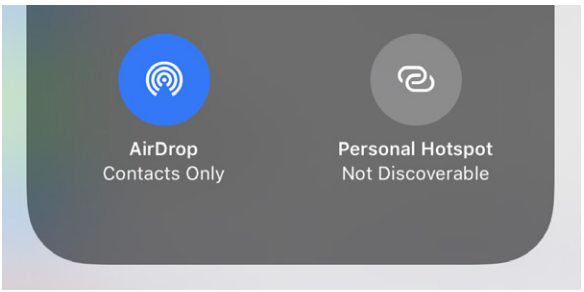

Figure 35: *Control Center is where you set AirDrop access.*

1. Swipe to show Control Center.
2. Hold down on the networking area, which displays the AirDrop icon and its status at bottom left (cellular devices) or upper right (Wi-Fi iPad).
3. Tap the AirDrop icon.
4. Tap one of the options (**Figure 36**):
   - Receiving Off disables AirDrop.
   - Contacts Only shows your device only to people whose email address is in your Contacts. This is the default option.
   - Everyone lets anyone on the local network see that you're available.

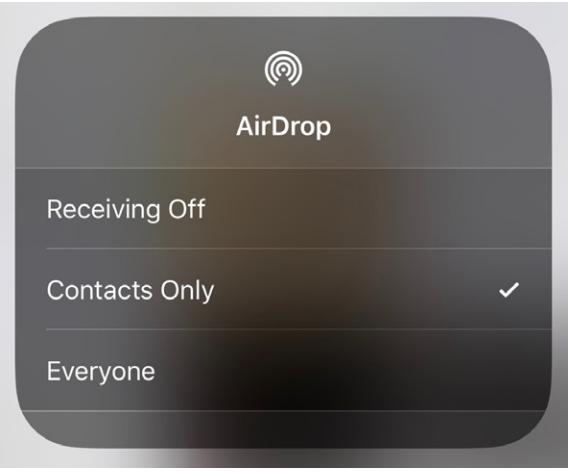

Figure 36: *Pick how AirDrop advertises itself on a network.*

> ***WARNING!*** *Some people have reported receiving unwanted images, including obscene ones, in public places if they have AirDrop set to Everyone. My advice is to leave it set to Contacts Only.*

Regardless of this setting, anyone who has your iCloud account email address in their contacts will appear for you in the latest OS as a more-privileged destination than folks who don't have you as a contact.

Share with AirDrop

AirDrop is available in any share sheet in iOS, iPadOS, and macOS: You can send URLs, files, photos, contacts, and other items to anyone nearby.

When you tap the Share icon on an iPhone or iPad, AirDrop becomes available in two ways. First, any nearby person for whom you're a contact appears among a list of possible recipients in a top row starting at furthest left with an AirDrop icon overlaid (**Figure 37**).

Second, you can tap an AirDrop icon in the second row. Tap it and you see folks who know you and all "Everyone" destinations. The list is divided into People (those in your contacts) and Devices (both your own devices logged into the same iCloud account *and* anyone set to Everyone). People have their contact name displayed; devices, their sharing name.

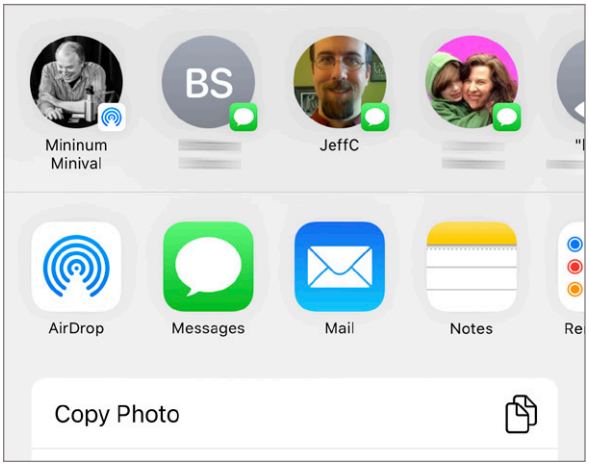

Figure 37: *The share sheet shows people who list you as a contact at top and the AirDrop button in the next row. (Names blurred for privacy, except Jeff's.)*

Tip: Starting in iOS 12, AirDrop allows password sharing from entries in Settings > Passwords & Accounts > Website & App Passwords. Read more about this option in **Create, Manage, and Use Strong Passwords**.

Share via iOS or iPadOS

To share over AirDrop, tap the Share icon and then tap a contact or tap AirDrop and tap a contact or device. For devices logged into your iCloud account, the item is automatically received. For everyone else, they're prompted to accept or decline the item. When a file or other item is accepted or received, the label Sent appears on the icon. (**Figure 38**).

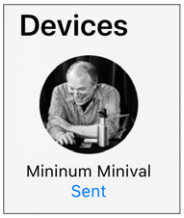

Figure 38: *The Sent label appears to confirm delivery.*

Apple added ultrawideband (UWB) technology into the iPhone 11 and 11 Pro, which allows more pinpoint short-range location finding. With

AirDrop, point an 11 or 11 Pro at someone else with one of those models who has you in their contacts or has AirDrop set to Everyone, and their name appears first in your list of potential recipients (**Figure 39**).

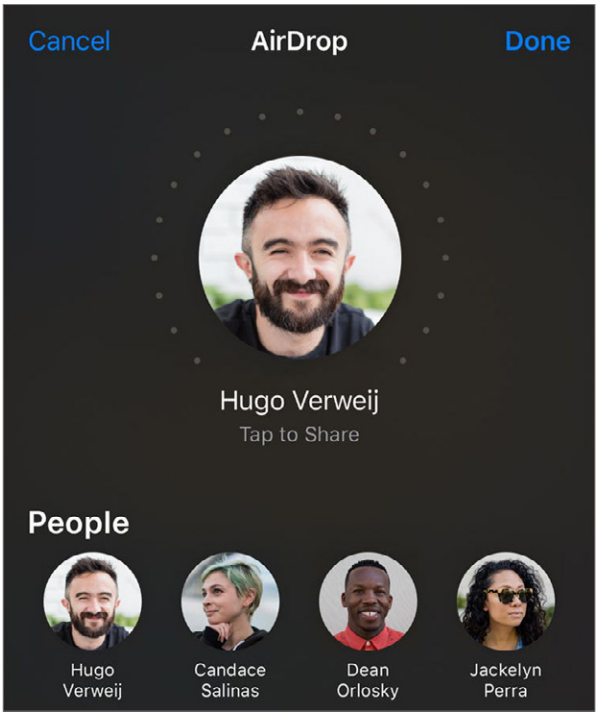

Figure 39: *UWB will let an iPhone pinpoint a recipient you're pointing your phone at (Photo by Apple).*

Receive an Item in iOS or iPadOS

The OS prompts you to accept an AirDrop transfer from someone else (**Figure 38**). If you click Accept, the item is received.

Incoming items are handled differently by type:

- Image files are added to your Photos collection, the Photos app is launched, and the image is opened.
- URLs are opened in Safari.
- Other files are opened by the appropriate app or by file format, if one is installed. For instance, a Soulver file from macOS opens in Soulver for mobile devices.

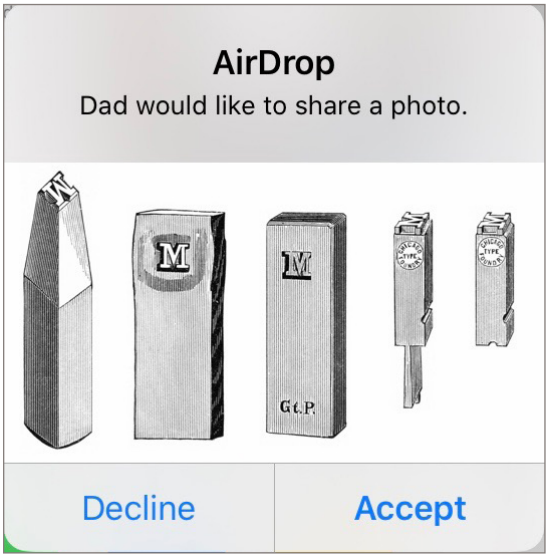

Figure 40: *You're prompted to accept incoming files from other people.*

- If an exact app match isn't available and the file is in a format other apps can handle, like PDF, the OS shows an Open With list (**Figure 41**). For PDF, I saw a list of about 20 apps on my iPhone. This includes Files, so you can save the file to iCloud Drive or other destinations. The Cancel option may require scrolling way down to the bottom.

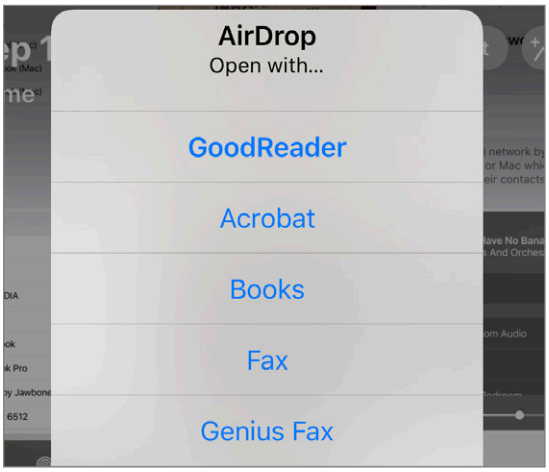

Figure 41: *With a file other apps can read, the OS prompts you for possibilities.*

- Finally, if no app can open the file at all, the OS presents you with a simpler dialog showing the file icon, and three options (**Figure 42**). Tap App Store, and iOS or iPadOS opens the App Store and tries to find a match. The link doesn't mean an app exists. Open with Files lets you save to a Files destination. Decline rejects the link.

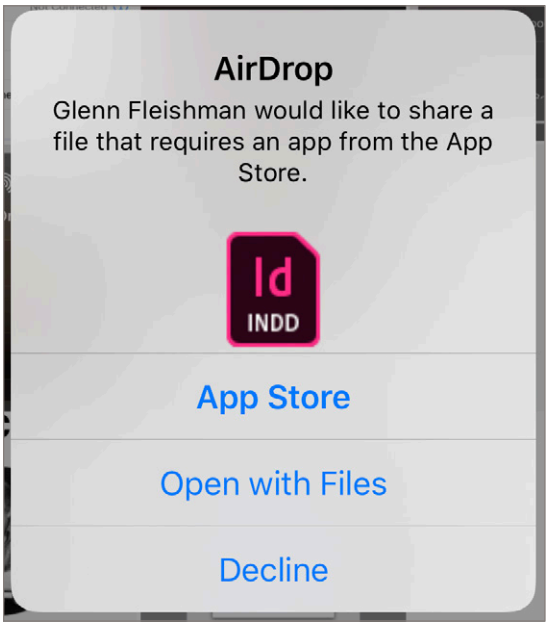

Figure 42: *For a file format the OS doesn't know what to do with, it still offers options.*

Stream via AirPlay

Apple's AirPlay technology lets you stream audio and video from Apple equipment to a variety of other hardware, including stereo receivers, computers, the Apple TV, HomePods, and more.

What's just as good is that Apple licenses the specification so that other companies can extend AirPlay to be more useful. In this chapter, you'll learn how to set up AirPlay, but also how to use it more broadly than with Apple's software and hardware.

AirPlay 2, a version that can pass audio to multiple speakers at once, appeared in 2018 across all Apple OSes and iTunes for Windows.

Select AirPlay Devices

This chapter has to start a little backwards, because before you can use AirPlay, you need a destination—or two or more with AirPlay 2! It's easier to walk through how you can configure your iPad or iPhone to point to an AirPlay receiver, and then look at the many kinds of uses.

To select any AirPlay-compatible device on the same Wi-Fi network as your mobile device, follow these steps:

1. Swipe to reveal Control Center.
2. Tap the AirPlay icon at the upper-right corner of the music player. (If no AirPlay destinations are available, the AirPlay icon doesn't appear.)
3. Select the device you want to use as a destination (**Figure 43**).
   - Your device is shown at the top with a checkmark.
   - Bluetooth audio devices appear with an audio Bluetooth icon.

- Other audio-capable devices are shown with a stereo speaker icon.
- Video-capable devices are shown with an Apple TV icon, whether or not they are actually an Apple TV.
- If destinations support AirPlay 2, they appear with a circle to their right, and you can to tap to add them, instead of switching to them.

4. If the OS is currently playing media, you should see a play/pause button you can tap to return to the playback view.

Figure 43: *Available AirPlay destinations are identified by type.*

Connecting with a Passcode or Password

An AirPlay device can be locked with either a four-digit passcode or a password.

- For code access, the device to which you're connecting will display the four digits. Enter those in the mobile device to connect.
- With a password, you enter the password set on the destination device.

Some Apple and third-party apps offer direct AirPlay device selection. The same options appear. In some cases, you might see a Done button rather than play/pause. You can also tap elsewhere to exit the view.

Your mobile device retains media control, so you can use volume up/down buttons and on-screen controls such as pause and rewind.

Ways to Use AirPlay

AirPlay lets you stream audio or video over your local network, and there are a number of ways this is useful in iOS and iPadOS. In this section, I explain how to do the following:

- Send audio or video from your iPhone or iPad to an Apple TV.
- Send audio to a computer or mobile device using Airfoil, or receive it on your iPhone or iPad using Airfoil Touch.
- Mirror the mobile display to a Mac using the Reflector app.

> **Tip:** You can send AirPlay audio and video to any device that shows up in the list. For example, I have a Yamaha receiver with AirPlay. On my local network, I select the Yamaha, which automatically turns on and selects its AirPlay mode for input.

Configure an Apple TV for Audio and Video

Turn on your Apple TV, navigate to its Settings menu, and then select AirPlay (**Figure 44**). You can now:

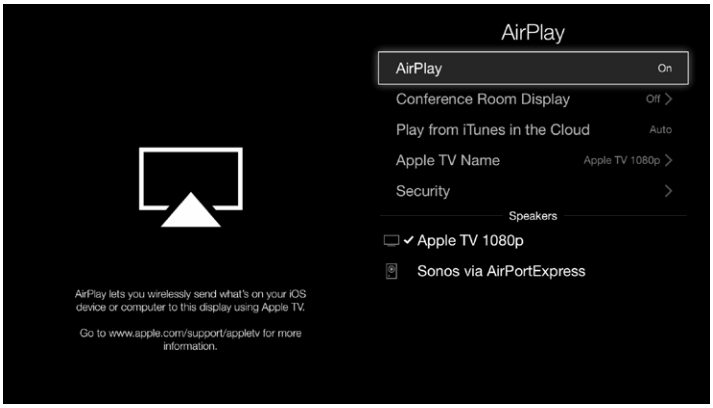

Figure 44: *Apple TV lets you set AirPlay's name and whether security is active.*

1. Select AirPlay to toggle it on or off.

2. Select Apple TV Name to set the device's identifier in the AirPlay list used by other hardware and software on the network.
3. Tap Security and set a password.

Send Audio with Airfoil

Rogue Amoeba makes **Airfoil**, a straightforward software package for streaming audio from macOS and Windows to other devices. Airfoil lets you pick a piece of software as its input and one or more destinations for audio while setting individual volume levels (**Figure 45**).

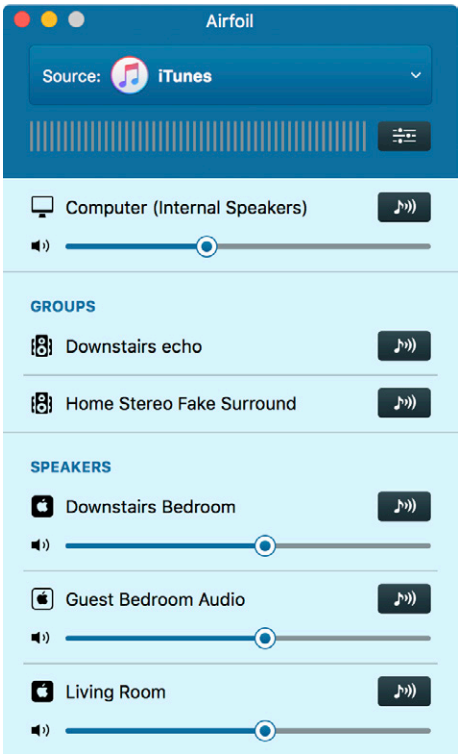

Figure 45: *Airfoil lets you stream audio from any app or the system to one or more AirPlay or proprietary Airfoil destinations.*

But Rogue Amoeba also offers complementary and complimentary (free) software that lets you use iOS and iPadOS more effectively.

First is **Airfoil Satellite**, available for macOS and Windows. It turns a computer into an AirPlay destination, so you can stream audio from an

iPhone, iPad, or Mac. Systems running Airfoil Satellite appear in the AirPlay list in iOS and iPadOS.

Second is **Airfoil Satellite for iOS** (free), which acts as a remote control for Airfoil for Mac or Windows, and lets you stream audio using a proprietary protocol from Airfoil to your iOS or iPadOS device.

Note: Airfoil can stream to any AirPlay device, including Airfoil Satellite for macOS and Windows. It can also stream to Airfoil Satellite for iOS, iPadOS, Android, and Linux, which use its proprietary standard and don't appear as AirPlay devices.

Mirror an iPhone or iPad Screen

AirPlay is often used for audio or to push video playback to another device. But it can also stream your active iOS or iPadOS display to an Apple TV. In Control Center, tap the Screen Mirroring button and choose an Apple TV destination.

However, if you want to stream the display to a Mac, you've got a third-party option. **Reflector** from AirSquirrels ($14.99) acts as an AirPlay video target. Select it as a destination in your AirPlay menu, and the iPhone or iPad display—minus any indication of taps—appears in a window on your Mac. You can set passcode or password access.

Being able to stream your full mobile experience is useful for live demonstrations and to record for later playback of demos.

Tip: You can also record your device's screen directly. In Settings > Control Center, tap Customize Controls, and then tap Screen Recording. Now a Screen Recording button appears in Control Center. Tap it and it starts recording the screen, and puts a red bar behind the status bar to remind you that you're still recording. Tap the button in Control Center again to stop recording.

PRIVACY

The online world is a tough place to keep your personal and financial details private. Even companies we should be able to trust often push at the limits of reasonable and ethical use of our information—especially in tracking us and aggregating our online profile from a thousand little shards into one complete picture.

Our privacy encompasses our personal information (our name, address, phone number, height, weight, and eye color), our financial information (bank accounts, credit cards, purchases, credit score, and much more), and data about us, like our current location, our browsing habits, and our typical travel patterns.

Privacy and security are complementary concepts. In this section, you'll learn how to use controls and filters to limit the ability of Apple and third parties to track you and to retain data to which you give them access. The next section, Security, addresses keeping information intended to be secret away from the prying eyes of others.

Privacy Leaks

What information, either owned by you or about you, should you be concerned about other people getting their hands on? In this chapter, I take a brief walk through a few different ways to slice that question so that you know in the coming chapters precisely what you want to allow, monitor, and block.

The difference here between privacy and security is that to constitute an invasion of privacy it doesn't necessarily require that a malicious party or malware obtain the information discussed below. Where it tips into security issues, discussed in the last section of the book, is when you're explicitly preventing unwanted intrusion that is malicious, criminal, or on behalf of government agencies.

Where Data Lives

Data is a monolithic term, but when we talk about your data being accessible to other parties, or leaking, we should define where it comes from:

Stored data on your device. The OS, its apps, and remote systems may be able to access, with or without permission, information you have stored on your mobile hardware. This can include contacts, photos, and emails.

Device hardware. The OS offers highly granular permission control for every kind of hardware element, whether a microphone or an activity sensor. This information can be extremely private. An app that can record you speaking or that can shoot video without your knowledge and stream or upload it later would be terrifying.

Data in transit. Information traveling between your iPhone or iPad and a legitimate destination could be intercepted or tampered with.

Information stored at a web site. Any interaction with a site can lead to it storing information about you, whether associated with an account and willingly provided or tracked and associated with a unique ID.

Cloud-stored data. Many services we use rely on data stored in the cloud, a collection of servers without a specific location, as information can be fluidly stored among whatever servers are available for primary storage and redundancy. Clouds may diffuse storage within a data center, among servers across a country, and even at locations around the globe.

What Kinds of Data

Beyond where data is located, you should also consider the kinds of information that you store on your iPhone and iPad and how it might be used. Just the way in which you use the Internet could provide fodder for legitimate and illegitimate purposes.

Behavior

Whatever you do can be tracked, although Apple makes it hard for some of this information to leak or be requested by anyone other than itself. Almost all of the following requires permission from a user (discussed in the next chapter) unless a malicious app was installed, which is unlikely.

Differential Privacy

Starting in iOS 10 and macOS Sierra, Apple added *differential privacy*, a technique of acquiring data that, if implemented and operated well, strongly resists tracking back a particular behavior or response to any individual user. It accomplishes this by adding random noise to all data before it's sent from your hardware.

The technique dates back decades to *randomized response*, which was developed to get honest answers to questions risky to answer. If an American survey subject were asked in the 1950s whether or not they were a member of the Communist Party, the safe answer was always "no," even if the interviewers assured them of privacy.

But there's a way around this. Give the subject a coin, and have them flip it. Heads, they always say "yes." Tails, they always give an honest answer. With a small number of people, the results remain poor. With a large enough number, however, the statistical noise of the coin flip can be reversed out without knowing which subjects answered honestly.

Differential privacy uses the equivalent of hundreds of random coin flips, and destroys information as it creates an answer to send to Apple, so there are no intermediate steps that can be recovered and analyzed, either. (Google has used this approach for years to collect usage statistics within Chrome.)

Apple started using this method for a few kinds of information in iOS 10: QuickType and emoji suggestions, Spotlight deep link suggestions, and Lookup Hints in Notes. Starting in iOS 11, it added the types of data people use with HealthKit (but not values collected), and web site loading speed and battery usage. Apple strongly suggests third-party developers use this approach via built-in libraries.

Privacy researchers have raised concerns with Apple's implementation. And it's also unclear how to opt out of collected data, a big missing piece on Apple's part.

While Apple introduced this in 2016 with some fanfare, the company essentially didn't discuss it in 2018 and 2019, and it's unclear whether it's been rolled out further or what its future plans for the approach are.

Apps

The OS can track which apps you install and which of them you launch. A developer in 2011 created a framework for other developers that relied on listing all app-registered schemas—the app-specific part of a URL—to get a partial sense of all apps installed. (For example, `fb://friends` comprises `fb`, the schema for Facebook's app, and `friends`, a destination the app interprets and then opens as the Friends list.) That framework, as well as a proof-of-concept app, has since been effectively banned.

Apps themselves can also track precisely what you do inside them. While this seems obvious, what the app does with that information is always a question. Is it sent anonymously in some form to troubleshoot and

improve the program? Is it aggregated anonymously to change how the app behaves? Does it use differential privacy to randomize data so that there's no chance your individual actions can be figured out later? Is all your information sent to servers to be processed—and is it retained or deleted, and if so, how does the app maker ensure this?

Where iOS and iPadOS are concerned, Apple offers extensive privacy policies that explain how your data is tracked, transferred, stored, retained, and deleted. I go into this in depth in Privacy Settings.

> ***WARNING:*** *It's also possible for someone to use AirPlay or on-device recording to capture everything appearing on your screen. However, AirPlay has to be set up through a few taps on the device, while recording displays a red banner in the status bar.*

The Web and Web Searching

It's of interest to others how you surf: what you are looking for, which search results you click on, where you wind up, which web sites you have bookmarked, and what pages you view on them—even how long you spend on any page or how you move a cursor on that page. And, of course, when you purchase things.

Because you're using search engines and web sites, the destination where you wind up and what you do there is captured by wherever you visit. What those sites do with your information is a matter of the privacy policy on each site.

> **Tip:** Content-blocking Safari extensions can help to block unwanted tracking and targeting; there's a whole section on them in the next chapter.

However, iOS and iPadOS also send various information to Google, Bing, and other search engines in different places—sometimes in Safari, sometimes in Spotlight, sometimes elsewhere. I cover how to control what information is sent in Privacy Settings. The Duck Duck Go search engine is specifically designed not to retain information about you between searches, and it can be set as your default Safari search engine.

In the past, some clever hacks have let web sites trigger a browser into sending some or all of its browsing history. While the last of those was fixed a few years ago and mobile Safari doesn't have any known weaknesses, it's worth considering how often you want to wipe your browser history to prevent tracking.

Metadata

In the era after **Edward Snowden's revelation**, most people know what metadata is: it's information that describes other information, like the destination of an email message rather than the contents of the message. The OS lets you send instant messages through iMessage and SMS/MMS as well as via third-party apps; use cellular and Wi-Fi calling via Phone; use Skype and other VoIP programs for audio/video calls, chatting, and file transfer; and upload photos that have your location tagged sometimes down to the nearest ten feet or so.

All of those activities involve recipients, locations of where you and they are at a given time, and the frequency and duration of contacts without revealing any of what you send back and forth.

Sensors and Receivers

I noted hardware as a category above, but the more specific elements that can be tracked include:

- What you're saying (via the microphone) or doing (via the front-facing or back-facing camera). Apple displays a red bar below the status bar (which it also changes to red) and lists the program currently accessing the mic (**Figure 46**). When recording has paused but the app has still reserved the mic for its use, it shows that, too. (With Apple's Voice Memos app, it just shows the time elapsed.)
- Where you are using GPS, cellular, and Bluetooth. If your location is currently being accessed, Apple puts a location icon in the status bar, unless you've disabled it. (See **Location**.)
- Your speed, heading, and altitude, via a GPS, barometer, magnetometer, and accelerometer.

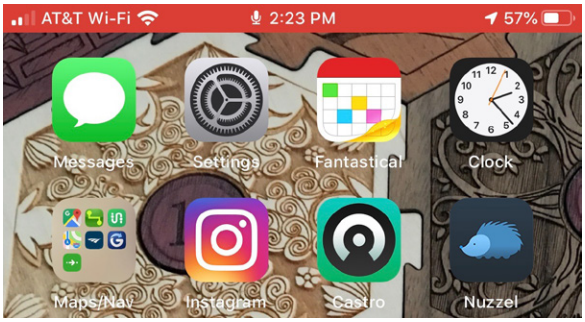

Figure 46*: While the OS is recording, it puts a red banner at top to let you know.*

What Can Be Extracted and Learned

Finally, we should review the kind of information that could be extracted so you can consider what you opt to store:

Your fingerprints and your face. Although Apple locks all this away in a one-way Secure Enclave portion of a chip—for Touch ID and Face ID—the fact that one or more fingertips or your face unlocks a device can be a giveaway: It proves you own or have access to it, which can be evidence in a trial or otherwise used against you.

Contacts. All the emails, phone numbers, and personal data you've stored.

Email. Not just the email on your device, but if you've configured it typically, all the email also stored on your email provider's servers.

Messages. The OS stores your messages locally and indefinitely. If you enable Messages in iCloud, they're also synced to iCloud, stored there, and synced to all other iCloud-linked devices you use.

Historical sensor data. HealthKit, the OS, and various apps can retain a trove of data about you gathered from hardware sensors.

Photos. With iCloud Photos, Google Photos, or other cloud-based photo services, you're storing not just pictures and video taken by the device, but also any available from the cloud. Photos typically also have global coordinates embedded in their metadata.

Faces. If you use the facial-identification feature in Photos, you're storing information about the people with whom you interact.

Where you've been and where you're going. Your current location and related position information can be obtained, and some apps retain where you've been, including things as disparate as which cellular towers your phone has recently checked in with. With travel apps and mapping apps, itineraries and destinations may also be available.

The GDPR and California's Privacy Law

In 2018, two remarkable sets of regulations appeared. The General Data Protection Regulation (GDPR) went into effect in May 2018 for residents of the European Union (EU). In June 2018, the California Consumer Privacy Act was passed; it becomes the rule of law in the state in January 2020.

The GDPR requires companies to provide to residents of the EU and a few affiliated regions substantial and clear disclosure about what aspects of personal information a site or service tracks and collects, how it's stored, and the names and relationships it has with third parties that also collect data or use data collected over the Internet. Residents have the right to request all the information that companies possess about them, and to have that information deleted. Web sites need to ask permission to collect data or track a user for anything that's not a core function of the site used solely to make the site work.

The European Commission says this regulation applies broadly: to any organization operating within the EU *or* providing services or goods to someone living in the EU. If you are an EU resident, you're aware of this, because of the proliferation of notices and data-collection statements by sites you use and visit. If you believe your rights have been violated, you can file a complaint, and have it taken seriously. The penalties can be quite enormous.

The California law isn't quite as broad, but it also affords a lot of rights of disclosure to people living in the state, and by companies providing services within the state and to state residents. Because so many major Internet companies are headquartered in California or have substantial operations there, and because it can be difficult at times to know whether someone is in a given location or not, many web sites and other Internet services will likely try to comply with the California law for all customers.

It's also likely other states will pass laws in harmony with California to spread the benefit.

Apple Blocks Tracking

Advertising-technology companies have built elaborate ways to track us across web sites, apps, and even real-world purchases that we make. The goal is to assemble a valuable profile of us, full of demographics (our age, race, income, and so on) and our purchase habits. This allows ad-tech companies to collect the greatest fees from advertisers, who believe super-targeted ads produce better outcomes.

Consumers increasingly have had enough, and hundreds of millions of people use ad blockers, anti-tracking software, private browsing, and other tools to disrupt unwanted online tracking. This includes Content-Blocking Safari Extensions in iOS and iPadOS, a feature that lets users install apps to block the loading of trackers and other kinds of web-based content.

Apple has taken a strong stance in this area, and over the last few years has rolled out a variety of features designed to deter tracking without blocking advertising or preventing advertisers from measuring the results of ads. In this chapter, I discuss Apple's approach, including a new addition in 2019 in the latest Safari across all its platforms.

Safari Blocks Cookies

Browser cookies can feed a browser a unique identifier that's stored locally. Every time a browser makes a web-based request for a page or other item that matches the same domain, it also packages and includes the cookie as part of the set of headers sent to that web server. Cookies are often used to plop a long-term or per-session identifier into a browser after a login or during an otherwise anonymous visit.

Starting in iOS 11 and macOS 10.13 High Sierra, Apple revamped how it approaches cookie storage and user choice. Previously, you had to select one of four options that had a lot of nuance behind them, and it wasn't always obvious which one was correct.

Now, there are just two switches: Prevent Cross-Site Tracking (on by default) and Block All Cookies (off by default).

> **Note:** Several years ago, a few privacy researchers mooted the idea of a Do Not Track browser signal that would let a user tell web sites they didn't want to be tracked. While the idea gained traction—Apple and others included it—for a lot of reasons I discuss in **this Fast Company article**, the idea ultimately fell apart.

Cross-site tracking lets ad networks and others feed cookies to your browser that can identify you across the Internet, essentially connecting your visits behind the scenes. This is why when you search for, say, "small superglue containers," suddenly superglue ads appear to you everywhere you browse.

Starting with Safari in 2017, Apple added a sequence of timeouts for cookies based on the source from which they're served to you. It calls this Intelligent Tracking Protection (ITP).

It's a little complicated, but ITP differentiates between first-party cookies, those fed to your browser by the site you're visiting, and third-party cookies, those fed from other domains. But it also uses built-in clues and relies on machine learning (using data kept entirely on your device) to identify third-party cookies designed entirely to track you across sites.

Tracking cookies get generated without user interaction, typically by resources loading instead of someone entering a user ID and password and logging in or engaging with some kind of feature on a site.

First-party data remains in place indefinitely, because it can only be used if you return to that site. If you don't, there's no harm in retaining it.

But for third-party data, Safari works this way:

- For the first 24 hours after you have an interaction with a site, third-party cookies and data remain active and available from other sites. This is much like how it works today.

- After 24 hours through 30 days, that third-party web data can only be retrieved through a connection with that original first-party site. That blocks cross-site tracking, but makes it possible to retain other, legitimate data. A new interaction with the original site resets the 24-hour clock.
- After 30 days, Apple deletes the third-party cookie and other web data permanently.

ITP isn't perfect, because an increasing amount of ad and tracking technology integrates directly with a site's servers or uses a domain controlled by the first-party site, making the cookie appear first party. But I don't think this first pass at ITP is the end: Apple's analysis and monitoring would let it tag "first-party" cookies as tracking cookies as well.

If you don't like any of this nonsense, switch Block All Cookies to On, but it will likely break many sites you visit. A better option is Private Browsing, described just below.

> ***Nuke all data:*** *You can get rid of all data associated with web site visits by tapping Settings > Safari > Clear History and Website data. If you're signed in to iCloud and have Safari syncing enabled, it also nukes this information from Safari on every Apple mobile device and Mac.*

Apple Breaks One-to-One Ad Tracking

While those earlier changes to Safari attempted to break unwanted tracking, it didn't solve the problem overall. Apple opted to push harder for user privacy by adding a new system to Safari in its third-quarter 2019 release across iOS, iPadOS, and macOS. The new system prevents advertising from directly tracking a user who clicks an ad and then performs actions on the resulting site.

Instead of allowing one-to-one tracking of users, the connection will be blurred so that an advertiser can only track the total impact of a small number of different ads over short periods of time.

The new approach, called Privacy Preserving Ad Click Attribution, first appeared in a Safari Technology Preview in March 2019, and then rolled

out to everyone in iOS 13, iPadOS 13, and macOS 10.15. (It's also part of a proposed standard at the World Wide Web Consortium.)

With this new ad-click attribution model, an advertising site will not be able to attach extensive and unique identifiers in a link nor track a user with cookies. It will also require so-called "first-party" links, where the tracking information is entirely fed by the web site a user is visiting instead of embedded code or web page portions (called "iframes") delivered by a third party.

Instead, ad attribution only lets an advertiser and ad network tag ads and actions in a very limited fashion:

- An ad network can only tag ads on a given publisher's site with one of 64 unique numbers (from 0 to 63) and the associated advertiser's domain. That seems small, but it means every advertiser can track up to 64 ads on each publisher's site every 48 hours. (That duration? Read on.)
- If a user clicks that ad, only that number is passed along. Safari strips off the cookies and any data in the URL that might provide identification. The user winds up at the advertiser's site, where they can log in or provide other information independently, if they choose.

> **Note:** Starting in iOS 12, Apple already clamped down on methods some sites and tracking software used to fingerprint your browser outside of cookies and URL values by silently testing out which features your browser supports.

- If the user carries out an action on the advertiser's site, such as making a purchase on an ecommerce site, the advertiser can send back a code to the ad network, again in the range 0 to 63. That may also seem like a small number, but it's enough to encode time of day of purchase, whether it was of high value, and other general information.
- For the ad network to pass back the advertiser's signal about a transaction, it sends a redirection request to the user's Safari browser, which causes the browser to retrieve a very specific web site path with that information encoded.
- Safari now does *nothing* for a random period between 24 to 48 hours, and then sends a single request—with no cookies or other information—back to the advertiser with the original ad ID and the code from the transaction the site.

The publisher, ad network, advertiser site, and Apple never have access to this information, as it's all stored and handled locally in Safari. The random period of time prevents any of those parties from knowing which user clicked on an ad.

But it lets the advertiser and ad network know in aggregate how many people clicked and what kinds of actions they performed. The advertiser can also still use tracking on their own site, watching a user's direct interactions with them.

The IP address from which a browser makes a request will also still be sent, but users on laptops, smartphones, and tablets have constantly changing addresses as they move about, while residential Internet service providers often aggregate traffic under a limited number of Internet-facing addresses.

What they can't do is use that data to associate someone with all their other activity across multiple sites.

Ad attribution doesn't eliminate privacy issues, but it's another hammer in the coffin of constant unwanted, undisclosed user tracking.

Block Content in Safari with Apps

Developers can create custom add-ins that monitor and block Safari-based connections for items on web pages known as content-blocking Safari extensions. Why block content? To reduce the time it takes to load a page that's otherwise laden with advertising and trackers, to decrease bandwidth consumed over cellular connections, to suppress unwanted advertising, and to prevent the easiest ways of tracking your activities.

It's not all about ads and behavior, though. Specialized blockers, and settings within more sophisticated blockers, can remove the display of comments on sites by blocking major content systems, keep popover boxes from obscuring your screen, remove social-network-related widgets and buttons, or blacklist entire categories of sites (such as those that show adult-oriented imagery).

Is it ethical? *Many web sites depend on advertising to pay the bills. Blocking ads from displaying, even if you never click them, can reduce revenue, because it makes the site's audience reach seem smaller. Thus, by blocking the ads, you're indirectly preventing revenue. The flip side? No site* fully *discloses how you'll be tracked and information about you sold and traded.*

Starting in 2015, Apple let developers create apps that can block content from particular URLs or from patterns that match URLs. The app provides the interface, if any is required. Some apps are just a set of filters you can't manipulate, while others have extensive options and customization. These filters apply to pages both in Safari and pages in browsers embedded in apps. (In 2016, Apple extended the feature to macOS.)

Content blockers don't analyze what is on a web page, nor do they examine other media and files referenced by a web page, such as Cascading Style Sheets (CSS) documents, images, video, JavaScript, and the like.

Rather, a blocker has a list of filters, which comprise these elements:

- A specific URL or a pattern that can match a range of URLs.
- A behavior: block the item entirely, block just associated browser cookies from being set, or block specific page elements (named items in CSS).
- An optional content type to match: document (which is generic), image, style sheet (for CSS), font (fonts can be quite large), raw (anything not specified), SVG document (a browser-rendered vector image format), media (images, audio, and video), and pop-up windows.
- An option to block only if it's fed from the "first party" (the web site you're visiting) or only from a third party, typically used for tracking.

Note: You can find the full technical details about how content-blocking extensions work at the **Surfin' Safari blog**, a site maintained by Apple's WebKit team.

Filters are set by the app, and then compiled by the OS every time they're changed, so that they are handled very quickly in Safari. Apple created these as opposed to allowing JavaScript-based extensions, which are available in Safari for macOS, because JavaScript imposes a much heavier load per page, delaying viewing pages and burning battery life.

As noted in the list above, blocking behavior doesn't have to keep an item from loading entirely: There are two alternatives.

Blocking cookies can prevent many kinds of tracking by companies that comply with industry rules, government regulations, and ethical standards. Some content-blocking apps will include cookie filters.

The other kind of page-specific blocking allows a filter to suppress CSS. This might sound a bit obscure if you don't design or develop web pages, but it's straightforward. HTML defines the bones of a page, like the girders of a skyscraper, and contains the innards—text and images and other stuff—just as an office contains workers and furniture and printers.

> **Tip:** Apple lets you set Automatic Reader View for web sites starting in iOS 11 and Safari 11 for macOS. This bypasses loading most of the content of a page, showing just crisply formatted text and some images, which has the effect of "blocking" most non-text content. For options, hold down on the Reader List icon while viewing a page.

CSS is the glass and metal panels covering the skyscraper, while also painting the outside and creating the walls and cubicle barriers: It defines how things appear, including the dimensions and placement of both fixed layout areas and boxes that seemingly float above the page.

A CSS "selector" defines the scope of what style definitions apply to. They can be used to attach to an HTML element (a tag), reused for multiple parts of a page (a class), or define a specific structure (an identifier or ID), which is used for those floating boxes among many other purposes. By allowing a blocking filter to strip out specific selectors, it can suppress advertising overlays or other annoying or intrusive behavior.

While this all sounds terrific, now for the bad news: There was a lot of initial interest by developers, who released a variety of extensions. Over time, many of them have ceased development or work erratically. The blocker I currently use no longer seems able to add exceptions, a highly useful feature, which means I have to switch to the Chrome app to view some pages. For this edition of the book, I don't recommend a particular blocker, and I am waiting to see how Apple's latest anti-tracking changes affect the need for Safari extension-based blocking.

Privacy Settings

Apple states repeatedly that it's committed to keeping its customers' data private, and it does seem to do a better job than other companies because it's primarily interested in selling us stuff—hardware, software, and services — rather than pushing advertising at us.

However, there are both centralized and scattered settings that let you control on a large scale and in small ways all sorts of data that leaks from your iPhone or iPad to Apple and beyond.

Note: Apple's **full privacy policy** spells out in great detail how it promises to handle your personal data and information about you.

Setup without Much Sharing

It's a privacy conundrum: Apple encourages you to enter personal or private details and connect your mobile device to its services before it lets you choose how you want to share data. You can work around this a bit with a new device or when you erase one to start from scratch.

Note: You can also set up one device by having another one nearby and entering your existing device's passcode. This may bypass some privacy options, however.

Start setup. On the Choose a Wi-Fi Network screen, Apple won't let you proceed until you either select a Wi-Fi network or, on a device with an active mobile data plan, tap Use Cellular Connection (**Figure 47**). The moment you do this, some information about your activities starts transmitting immediately—although it's not much at this point!

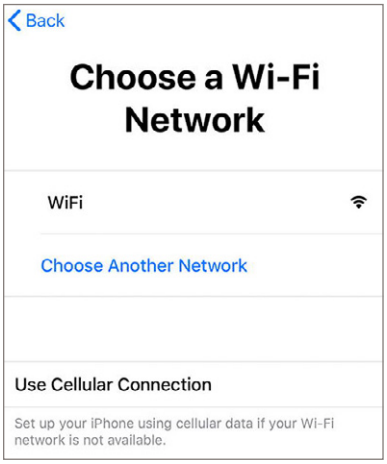

Figure 47: *You have to pick a network.*

On the Location Services, choosing Disable Location Services ensures nothing related to your position is sent. (If cellular service is available, even if you chose Wi-Fi in the previous step, your device's pings to cell towers are recorded, however—that's unavoidable.)

On the Apps & Data screen, don't enter an iCloud account's information, but instead choose Set Up as New iPhone (**Figure 48**). On the Apple ID screen, click Don't Have Apple ID or Forgot It?, then confirm you want to skip. You can connect your Apple ID and iCloud account later.

Figure 48: *Don't restore a backup, but start from scratch.*

Continue to the Siri screen, where you should select Don't Use Siri. On the Diagnostics screen, choose Don't Send. The device is now set up.

Now you can read through this chapter and decide which features to enable, whether related to privacy or to the way in which your information is synchronized to the device.

Control System Privacy

Much of the information the OS captures about you and sends to Apple's servers is used to improve your "experience." For example, Siri can't work without sending your voice off to central processing, and it learns more about you over time as you correct its dictation and travel. But you can also reset Siri at any point, and it forgets forever the connection between any interaction and your device.

Apple typically tries to capture the least amount of information it needs, and when it needs to make a connection between you and that data, it associates your information with a tag that isn't connected permanently to your identity. You can disassociate from that tag and forget most or all of that information with a click.

In this chapter, I examine the many places in the OS where you control what you allow Apple to know about you, and how to either prevent sharing details (such as your location) or cause Apple to delete your data.

Note: The Settings > Screen Time > Content & Privacy Restrictions options let you lock all privacy settings in whatever state you like in a separate privacy section.

Control Privacy Related to Advertising

Apple scatters its settings related to how it gathers information from you to better target ads by interest and location. There are two settings you can disable:

- Privacy > Location Services > System Services (found at the very bottom): turn off Location-Based Apple Ads
- Privacy > Advertising: turn off Limit Ad Tracking

You can also reset an identifier that's tied to your Apple ID account and used to associate targeting information in Privacy > Advertising. Tap Reset Advertising Identifier, and the link between you and the data gathered is severed.

Siri

iOS and iPadOS's voice-processing technology mostly lives in Apple's cloud, and thus you need a live network connection to use Siri and Dictation. When you speak to Siri, it passes what you say to Apple's servers for a response—and other information to help provide better cues as to what you mean, some of which information is never stored and some that is stored anonymously.

Apple Was Listening to Siri without Alerting Users

Apple faced a backlash in mid-2019, when *The Guardian* revealed that contractors listened to a small percentage of Siri recordings as part of Apple's process to improve voice recognition. This included private and even illegal information, such as credit card numbers being read aloud and the details of drug deals! The information wasn't deidentified, but associated with a random ID for up to six months. That meant that all audio from a single device would have the same identifier.

Apple apologized, halted its testing, and promised changes. It will shift to use only employees instead of contractors. It said it would only refer to machine-created transcripts to check on behavior instead of listening to audio, unless users specifically opted in to provide Siri recordings for improvement. It will also delete any audio that was unintentionally recorded.

These changes will go into effect in third quarter 2019, when Apple will offer the opt-in option in its operating systems.

Siri comprises several kinds of tasks:

- Actions in response to requests, like opening an app or setting a timer.
- Shortcuts, which string together a series of actions.
- Contextual responses that relate to information about where you are or who you are, like weather or calling your spouse.

- Dictation.
- On-device searching, once called Spotlight, which integrates results from Apple and third-party apps that provide indexed results to Siri.
- Search engine results via Safari.
- Reading aloud text that you ask it to, like your the last text message that you received on your iPhone.

Let's look here at the first four bullet points, and discuss Safari-related Siri behavior in the next section on Safari.

What Siri Knows about You

Apple's privacy document for Siri and Dictation explains that it collects the following details:

- Your name and nickname
- Names, nicknames, and people's relationships to you that are stored in your Contacts
- Song names in your collection
- HomeKit-enabled devices
- Names of photo albums
- Your current location (if available)
- Some portions of data from third-party apps that use Ask Siri to understand what you're saying or for dictation

Apple connects this to you using an anonymous identifier. You can sever this link whenever you want, by disabling both Siri and Dictation.

You can't just turn off Siri: It requires multiple changes. In Settings > Siri & Search, turn off Listen for "Hey Siri" and Press Home for Siri (**Figure 49**). When you tap the second switch, you're prompted with a warning that Siri will be turned off altogether. (If just one was enabled, turning it off also triggers the warning.)

To turn off Dictation, go to Settings > General > Keyboards, and turn off Enable Dictation. This severs the link between your device and Apple, although on its servers, Apple may retain a fair amount of:

Figure 49: *Disable Siri and the link to your device is tossed, but not all data collected.*

"...audio files and transcripts of what you said, related diagnostic data, such as hardware and operating system specifications and performance statistics, and the approximate location of your device at the time the request was made."

If you're uncomfortable with any of that ever being sent or retained even in that disassociated form, disable Siri and Dictation and never use them.

You can also selectively disable location hints for Siri and Dictation: set Settings > Privacy > Location Services > Siri & Dictation to Never.

Siri and On-device Searching

Siri handles on-device search results in a conceptually complicated fashion. In Settings > Siri & Search, you'll see three items under Siri Suggestions: Suggestions in Search, Suggestions in Look Up, and Suggestions on Lock Screen. These switches, which default to on, allow Siri to make suggestions within apps or when using Search, the Look Up feature, its News app, Photos' Memories section, or Apple's keyboard, as well as when you have the screen locked (**Figure 50**).

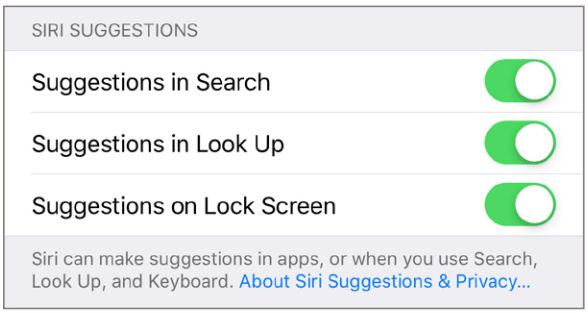

Figure 50: *Spotlight suggestions for search and look up pass information through Apple.*

You may want to disable Siri from the lock screen by turning off Allow Siri When Locked, a choice introduced in iOS 12, to prevent other people from using Siri if they have access to your device.

Apple uses this information to personalize results in a number of places, and it syncs this personalization through end-to-end encryption among all your devices associated with the same iCloud account.

To create these matches, it uploads what it describes as "generalized topics of interest," like whether you like "cooking or basketball." It also sends search queries and related information to its servers to fulfill your request, but Apple says the information isn't associated with you, and it doesn't include any data related to stuff stored on your device.

Further, Apple gathers location information, and details about music and video subscriptions you may have and sends that. Apple says it doesn't include any personally identifying information or account details, and uses this data to improve results and not for other purposes.

However, this amount and variety of information collection may seem like too much to you. If so, you can flip either or both switches off. This will make searches less precise and adaptive, but it may be worth the tradeoff to you.

You can also disable individual apps from contributing information towards searches, such as finding files stored in Dropbox or matching text in messages in Mail. Apps are listed below the Siri Suggestions switches.

Tap an app, and then you can see what kind of information it contributes towards search results—which might be used by Apple to improve Siri overall as well—and can disable that switch (**Figure 51**). The list used to be quite short, but can now fill a screen; not every item will appear for every app:

- **Show Siri Suggestions in App:** Siri can make suggestions within the app for filling in field or making choices.
- **Learn from This App:** What you do within the app can be used to inform Siri in how it offers suggestions in other apps.
- **Show in Search:** Results from the app appear in Siri searches.

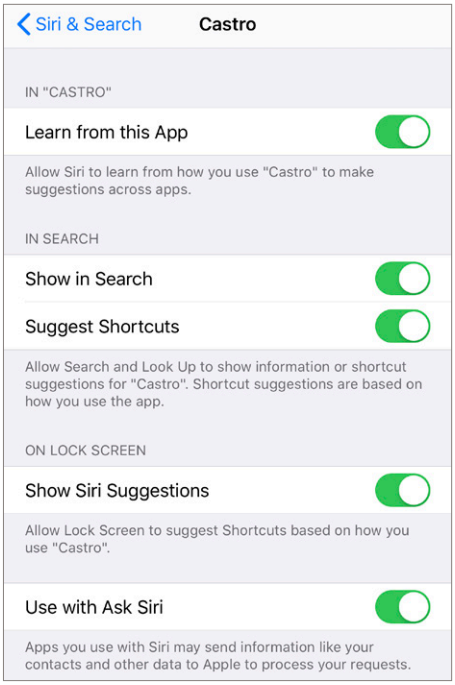

Figure 51: *You can tweak each app for how it works with Siri.*

- **Suggest Shortcuts:** While you can create shortcuts from scratch, Siri also suggests them. Leaving this setting on lets it analyze the app's usage to come up with suggested shortcuts.
- **Show Siri Suggestions (on Lock Screen):** Just what it says!
- **Use with Ask Siri:** Some apps may want to send information to Apple that can include private data in order to produce a better result. This is only one of all these app-specific options that is disabled by default.

Safari

When you use a web browser, you're always leaking information about yourself. Use a search engine, and it knows what terms you typed in, what kind of device you're using, and your IP address. When you visit a web site, it knows what pages you request, of course, but may also track mouse movements and use tracking IDs to identify you from previous visits and across multiple unrelated sites. Some financial sites now use your interactions with a page **to thwart fraud**.

Duck Duck No? Heck Heck Yes! *Duck Duck Go is a search engine that promises not to retain or resell personal information. Many people who dislike the tendrils of Google opt to use Duck Duck Go instead. You can set it as your preferred search engine in Settings > Safari > Search Engine.*

The OS has several options to reduce the amount of information leaking about you, discussed in the previous chapter.

Even innocuous features such as autofilling forms and storing passwords increase your risk if someone gains access to your phone or you visit a malicious site. Fortunately, Apple also has tools that help protect you.

Note: Apple release Sign in with Apple to let you create an account at third-party sites. You can opt to use an anonymous email address Apple relays to you!

Apple's Suggestions

To provide the best answer in a Safari search, Apple sends information about you to a search engine or its own servers. When enabled, Search Engine Suggestions in Settings > Safari transmits your query to the search engine you chose and then displays the results it offers. (Preload Top Hit downloads the first match in the background.)

Safari Suggestions displays all sorts of things—search results, apps, movie showtimes, and more—based on the terms you enter, your location, and the music and video subscriptions on your mobile device.

You can disable either or both Suggestions options entirely, or turn off location awareness, via Settings > Privacy > Location Services; swipe down to the bottom (past all the apps that use location data) and tap System Services, where you can disable Location-Based Suggestions.

Sharing and Commenting

Apple offers privacy protection for sharing and commenting that blocks privacy loopholes some sites have used to extract information about you. When you use a share button or leave a comment via a web site, Safari blocks tracking you without your permission.

Passwords and AutoFill

Although automatically providing or filling in information would seem like a plus—as long as those details remain under your control—you may prefer not to have any such information stored permanently on your mobile device. And with iCloud, some information is synced across all devices with the same Apple ID and settings.

> **Tip:** For more in-depth information about using the built-in password management with apps and Safari, and about the third-party password system 1Password, see the chapter **Create, Manage, and Use Strong Passwords**.

For example, you may not want your information filled in on a form automatically. Some web pages use live server/scripting interaction so that even if you never click or tap a submit button, any information entered into a form is sent. You also may not want someone else with access to your iPhone or iPad—even perfectly legitimate access—to log in or fill in information on sites.

With Settings > Passwords & Accounts > AutoFill Passwords enabled, whenever you visit a web site and enter account information and passwords for login, Safari will offer to capture and store them. A pop-up dialog will present three options: Save Password, Never for This Website (never asked again), or Not Now (asked on next visit).

You can disable Autofill Passwords at any point, and all password entries remain intact in the OS (and in iCloud Keychain) but no longer appear in Safari or other apps.

Safari's preferences for autofilling forms (Settings > Safari > AutoFill) also let you enable and disable pre-filling your contact information (tap Credit Cards on or off) and credit card details in Saved Credit Cards. Safari autofill credit cards are managed separately from Apple Pay.

Watching the Watchmen

Beyond content-blocking extensions, discussed earlier, you can also control several elements of how web sites interact with you.

Block Cookies

Because Apple has a complicated strategy regarding cookies, I've discussed both its approach and the settings in the previous chapter.

Fraudulent Website Warning

This little switch in Safari preferences apparently protects you against phishing sites: Sites that appear to be legitimate but are fraudulent and counterfeit, to which you're often directed by links in email or subverted advertising. Apple hasn't provided details for years about how it assembles the list, and I've never been warned in years of using it.

If you encounter a site that's in its blacklist, you'll be warned and asked if you want to proceed. This prevents the page from loading and attempting to fool you or even install malware. (Malware is a slight risk for iOS and iPadOS users, but a risk nonetheless.)

Camera & Microphone Access

Everybody tries to be sneaky, and sites a few years ago were using a combination of tools to try to record or stream audio and video from your device without asking permission. Apple blocks this by default in the Camera & Microphone Access setting.

Check for Apple Pay

You can pay for transactions within a Safari web browser using Apple Pay on an iPhone or other device. This scheme uses Continuity, Apple's catchall term for linking Macs, iPhones, and iPads together for proximity-based activities, including Handoff, where you can start reading on one device and continue reading on another.

Apple Pay in Safari requires that a web site can detect whether the browser can hand off a transaction. This leaks a tiny bit of information about you; you can disable this—but then you can't use Apple Pay.

Private Browsing

Not a preference but a mode: You can use Safari in a way in which all your normal settings are overridden and nothing is retained from the browser window you use once it's closed (**Figure 52**). Specifically, your

history in that window is forgotten, the tab isn't synced with Safari on other devices through iCloud, Do Not Track is set to On, cookies aren't permanently stored, and local storage isn't accessed.

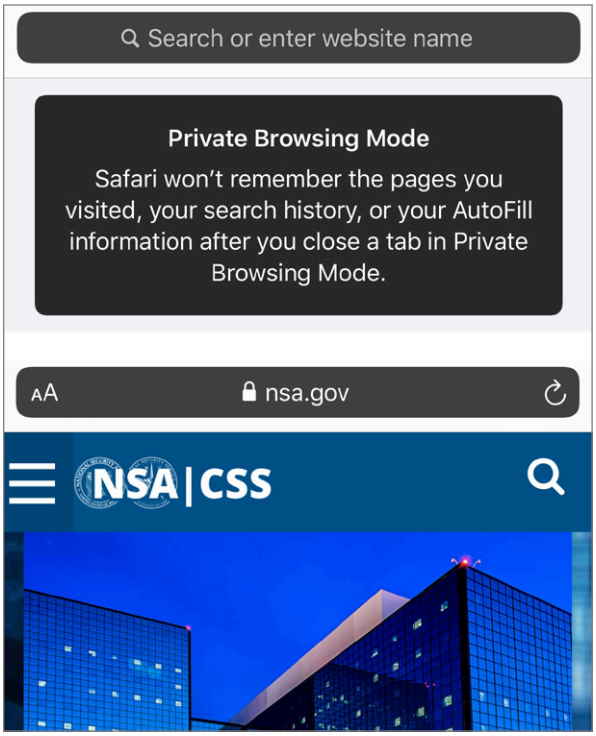

Figure 52*: The Private Browsing mode explains itself (top). A page loaded (bottom) keeps the dark top bar to remind you.*

In Safari, tap the Windows button and then tap Private at the bottom of the screen on an iPhone or iPod touch, or at the top of the screen on an iPad or on some iPhones in landscape mode. You can also hold down on the Safari windows icon in the browser (or the Safari icon on the home screen) and select New Private Tab.

The color scheme switches from light to dark to remind you that you're browsing privately. To exit the mode, tap the Windows button and tap Private again. However, private browsing tabs remain in a paused state rather than closing when you exit. If you want those tabs shut, hold down the windows icon and choose Close This Tab or Close All *X* Tabs before you exit the mode.

Because history isn't retained from private sessions, it's a reliable way to zero out your past, even if someone else were to obtain access to your device. This applies to "evercookies," persistent cookies that use insidious storage techniques, which are nearly impossible to delete.

Website storage

An improvement that was added several years ago to HTML and browsers allows web sites to store information in a database format in a browser. This is especially useful paired with JavaScript: A site can load and the JavaScript code can consult settings or other information stored locally without a round trip to the server, speeding up how a page might display.

In Settings > Safari > Advanced > Website Data, you'll see a list of sites that store information and how much data they're using. A selection of sites that use the most data initially appears; tap Show All Sites to view everything. You can swipe left on a site and tap Delete to remove the associated data, or tap Remove All Website Data to kill all local storage.

Location

The OS's ability to provide a set of coordinates that fairly precisely describes your current location on Earth works amazingly well. So well that you may have reasonable concerns about when, how, and to whom your location is shared. iOS and iPadOS offer a lot, lot, lot of settings and options. While most are centralized, Location comprises many disparate things you have to consider when limiting what sees your coordinates.

Turn off Location Services, and location information stops being gathered and fed to apps and the system—at least by Apple, as I'll explain in this section. (The sole exception, Apple says, is to provide your location when someone uses the device to place an emergency call.)

The How and Why of Location

Apple uses a combination of onboard radio systems to produce a set of standard geographical coordinates, sometimes with a margin of error when data isn't precise enough.

Satellite navigation systems can provide location accuracy within meters, or even better with more satellites or when combining multiple systems. (Modern iPhones pull satellite data from four systems: the U.S.-operated GPS, Russia's GLONASS, Europe's Galileo, and Japan's QZSS.)

But the OS also uses Assisted GPS, which lets it plot satellite positions more rapidly and accurately, relying in part on data sent via a live Internet connection. It can also use cellular network information (cellular network transmitters' exact positions are fixed and known), Bluetooth (to communicate with nearby gateways, if their locations are identified), and Wi-Fi (relying on a worldwide database, which Apple constantly updates, of the broadcast names and signal strengths of Wi-Fi networks).

The OS and apps make use of location for all sorts of purposes. Of course, advertisers want to target you, because they make more money in pushing things at you that relate to where you are. But your position can also be attached to photos (called geotagging), track a stolen iPhone or iPad, help you find a family member, bring up a list of nearby restaurants, and tell you the current weather for the micro-climate you're standing in.

Note: Apple explains **in a support document** how the OS makes use of your location.

Apps Can Bypass Some of Apple's Location Protection

Apple controls the way in which apps access OS location information, but apps can request data over the Internet. The mere act of tracking software embedded in an app making a web request from its server passes along the Internet Protocol (IP) address of your iPhone or iPad.

Depending on which network your device is connected to, the IP address could provide no information, a general region, or practically your address. The *Wall Street Journal*'s Joanna Stern **found in mid-2019** that many apps break smartphone OS makers' rules, and one tracked her by IP to within a few blocks.

There's no way to avoid this particular kind of tracking, though I'm sure Apple is working on it. One interesting idea is the subscription VPN product **Guardian Mobile Firewall**, which uses a constantly updated list of tracking and ad URLs it finds in apps and blocks them while you're using the VPN—and it generates a list of what it's blocked, too.

Opting In and Opting Out

The OS sometimes uses your location without prompting, but you can opt out of nearly all of those situations later; apps, however, must always request permission. As of iOS 13 and iPadOS 13, apps must offer three choices: Only While Using the App, Allow Once, and Don't Allow.

The first choice covers when an app is active in the foreground, but it also applies if the app provides a continuous background function, like Google Maps navigation.

The second choice is new in iOS 13 and iPadOS 13, and has rankled some developers. Previously, users could choose Always Allow from this popup, but researchers, reporters, and government agencies found significant abuse of location tracking in the last few years. Many apps include third-party tracking and measurement software for gleaning information about users, and some of that software tracks location information, even when the app doesn't disclose. (Some apps include so many of these code libraries, they aren't even aware they're sending this information off-device.)

Apple says these choices eliminate background location gathering by apps that don't truly need it. If an app requires background access, the app can direct a user to Settings > Privacy > Location Services > *app settings*.

This direction can be through a button in the app. There, the user can select from Never, Ask Next Time, While Using the App, and—for any background usage—Always (**Figure 51**). The app has to provide an explanation that appears on that screen in small type explaining why Always should be chosen if they want to include that as an option.

When an app accesses your position, Apple indicates this through the status bar in one of a few ways:

- A hollow arrow when an app has recently requested location information (like that shown in **Figure 53**).
- A filled-in arrow if it's received your location in the last few seconds
- Blue status bar: the app is continuously accessing your location and that app isn't in the foreground

You can also gather and set more information in Settings > Privacy > Location Services, where you find nearly everything associated with system-level and app-specific position permission.

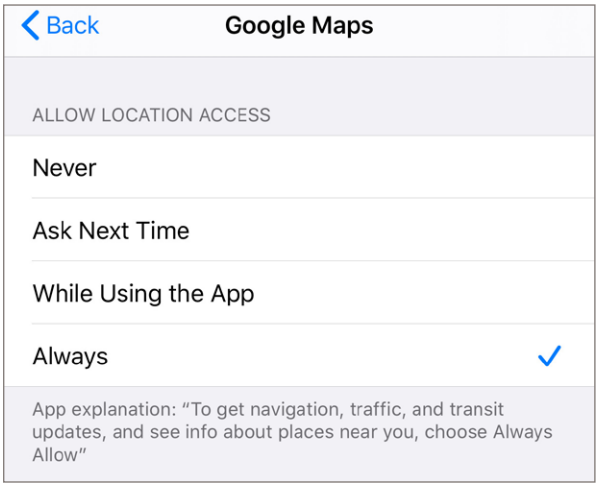

Figure 53: *Apps have to justify their use of Always, which appears only in the per-app location settings and occasional prompts (see* ***Figure 53****).*

At the top, a list of Apple and third-party apps appears alphabetically with a label about how the app may currently access your position. The OS may also mark an app or service with a location symbol (**Figure 54**):

- Purple, when in continuous use (filled in) or recently used (hollow)
- Gray, when used within the last 24 hours
- An outline, for an app that supports geofencing, which monitors when you leave or enter a defined location or area

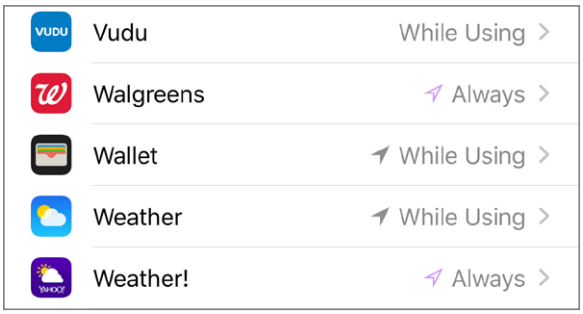

Figure 54: *The arrow colors indicate how location services were recently used.*

Tap an app, and it shows how an app claims it will use your position, like, “To get real-time traffic updates, reminders to leave, and personalized recommendations, choose Always Allow” for Google Maps.

Even after granting permission, the OS will prompt you occasionally for apps that update location in the background to make sure you still want them to do so (**Figure 55**). In iOS 13 and iPadOS 13, this became very specific and includes a map showing all the places you’ve been pinpointed, lists how many times, and again includes the text the developer wrote about why having always-on access is necessary for some app functions.

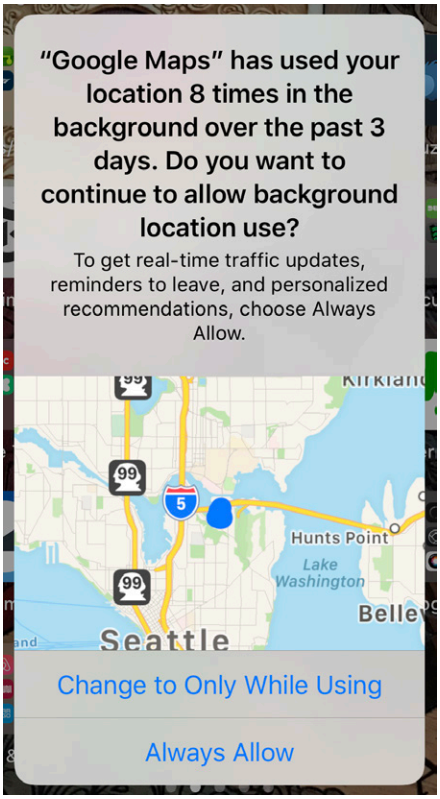

Figure 55: *The continue-to-use dialog shows locations and tells you specifics about how often the app has consulted your whereabouts.*

Location permissions for System Services

System Services, at the bottom of the Location Services screen, contains a host of very specific permissions for how the OS makes use of location.

Some of them allow the hardware to function more accurately, like Compass Calibration. Some are strictly useful, like setting your time zone automatically.

The list becomes longer with every release of the OS, and in version 13 contains items like Apple Pay Merchant Identification, which provides better location information on Apple Pay charges, and Location-Based Suggestions, for giving you Siri results that rely on where you are, and HomeKit, which can behave differently when you're near devices under your control or using them remotely via a relay.

There are a few items you may want to disable or consider disabling:

- Wi-Fi Networking sends continuous snapshots about Wi-Fi networks picked up from your location to improve Apple's positioning database.
- Significant Locations tracks your regular haunts, and Apple says the data is stored only locally, to help with "predictive traffic routing" and other services. It requires authentication, like Touch ID, to access. It's a little freaky when you consult it and see how well your device knows you.
- Product Improvement includes four different items that Apple says it relies on to improve maps, including traffic and routing.

Photos

In the latest OS, you can choose to remove location information from photos before you share them. Apple located the setting in an odd place. With images or videos selected, an Options link appears below the count of items with a label indicating if its location is included (**Figure 56**).

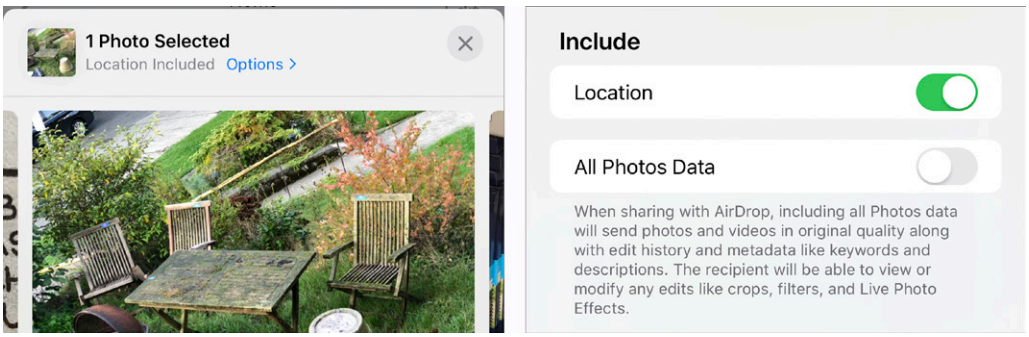

Figure 56: *You can omit location details when sharing, but have to opt out each time.*

Tap Options, and a few new settings appear. For the purposes of this section, the Location switch is the important one. Tap to disable, and the location is stripped. The option isn't persistent; you have to choose it each time you share photos.

Bluetooth in Apps

Apple also restricted how Bluetooth can be used within apps in the latest OS. Previously, Apple promoted what it called "iBeacons": Bluetooth-equipped transmitters that can contain coupons, kiosk-style information, or other installation-specific details.

Used within apps, it seemed like iBeacons could help users navigate stores and find information more readily. Unfortunately, it appears Bluetooth detection was most frequently used to observe user behavior and enhance marketing profiles about them.

Thus, in iOS 13 and iPadOS 13, apps have to ask permission to use Bluetooth and must provide text, just like with Location Services, about how Bluetooth will be employed. For instance, the Nordstrom app says it "may…use Bluetooth to know when you're nearby." You can click Don't Allow or OK, instead of the multiple options in Location Services.

You can change an app's permission after you allow or deny it access via Settings > Privacy > Bluetooth.

Share My Location

The most consensual of all position-providing services, Share My Location, lets you send you position to people you know, either once (as a map) or continuously for a period of time or indefinitely. You can use the Messages app, Find My, and Family Sharing to send your location or control who sees where you are (**Figure 57**).

Because the feature is exclusively opt in, you can't accidentally share your spot with people you didn't choose to. However, you can suspend sharing by setting Share My Location to Off, and then no one with whom you're connected can track you; when you re-enable the setting, the connection to them resumes as before.

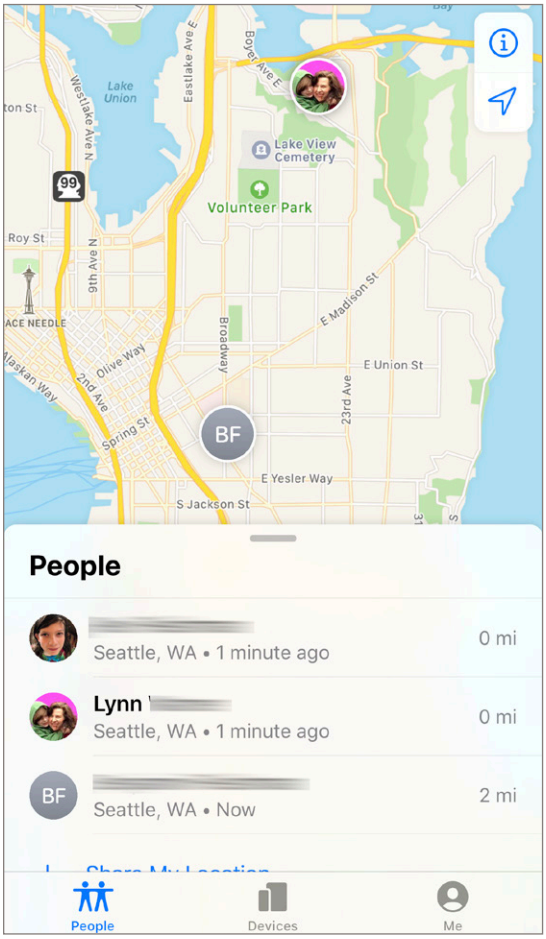

Figure 57: *In the Find My app's People view, you can see the current position of everyone who has shared their location with you and currently has that sharing enabled.*

You can remove people from the Friends list (and Family list with Family Sharing enabled). Tap the name, and then tap Stop Sharing My Location.

With Messages, you can opt to share your location with people over iMessage or SMS in one of two ways. Begin by starting a conversation with someone or, if you have a conversation in the Messages list: Tap their name, their avatar, and the info ⓘ button. You can either tap Send My Current Location, which sends an image of a map slice and a pin for your current spot on the map, or tap Share My Location, which lets you pick one hour, till the end of the day, or indefinitely (**Figure 58**). You can then manage that connection from the Share My Location settings.

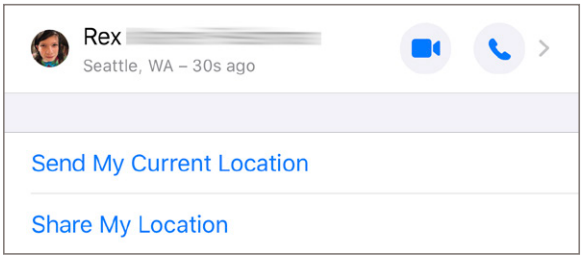

Figure 58: *You can share your location as a static map of where you are, or as a constantly updated position for a short or long period of time.*

Tip: You can also access Share My Location's settings from Settings > *account name* > Find My.

Privacy Settings and Allowing Access

There's one more section to talk about, which is the main Settings > Privacy screen, where you manage access to apps that you've previously given permission to for specific kinds of OS-level or hardware access, such as to your contacts or the microphone.

Apple controls access to many kinds of personal data and device hardware by prompting you the first time an app wants to use either data or hardware, letting you confirm or reject it. This came about after apps would access your contacts list and upload it to their server for processing, including inviting other people to use the app or their service!

If you confirm access, the OS creates an entry in the Privacy settings in the appropriate category. You can visit any category and disable access for any app listed there. You can't delete the app from the list except by uninstalling the app.

When you've disabled access for an app, the next time you use that app and try to employ a feature that requires one of these caches of data or a hardware element, you'll be told that the app currently lacks access. You're directed back to Privacy to change the setting so it will be re-enabled in the app.

Keeping Creeps Away

Every technological breakthrough has a downside. iMessage was a big step up over text messaging: Encrypted to just the members of a conversation, allowing long messages, including rich media. It was kind of perfect. Except Apple never thought about it being used for harassment.

There was no way to block unwanted incoming iMessages, even though carriers offered various tools to block incoming calls and, in some cases, text messages from numbers you specified. The same was true for FaceTime audio and video.

It took until iOS 7, several years ago, for Apple to add the first blocking tools, which it's gradually broadened since then. In this chapter, I look at built-in, automated, and third-party options for blocking unwanted contact.

Block Numbers and Email Addresses

Apple lets you block incoming voice calls, text messages, iMessages, FaceTime calls, and email messages.

Because email addresses can be used with iMessage, FaceTime, and email, and phone numbers can be used with SMS, calling, iMessage, and FaceTime, it makes sense to have a single block list across all these services.

You can block phone numbers and email addresses one at a time:

- In Phone, you can select any number and tap the info ⓘ button (or select any contact) and then tap Block This Caller.

- In Messages, tap a conversation, tap the avatar, tap the info ⓘ button, tap the right-pointing arrow at the far right (not the icons next to it), and tap Block This Caller.
- In FaceTime, tap the info ⓘ button next to any Video or Audio entry, and tap Block This Caller.
- In Mail, tap a sending address and then tap Block This Contact.

  Once you tap and confirm with Block Contact, all associated information is added to the Blocked list (**Figure 59**).

  The list of blocked phone numbers and addresses appears the same whether accessed from Settings > Phone, FaceTime, Messages, or Mail. You can tap an entry to view all associated details, or swipe left and tap Unblock to allow them access to you again.

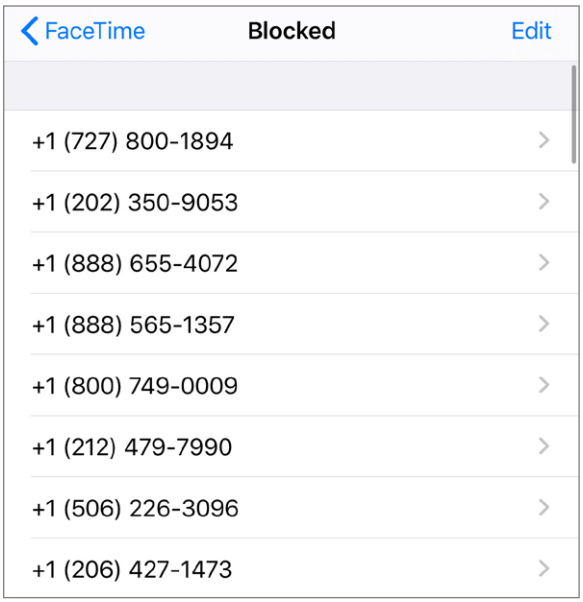

Figure 59: *The Blocked list shows all banned email addresses and phone numbers.*

Note: Caller ID is used to block phone calls, but unfortunately it's not a secure method of identification. A harasser can turn off Caller ID or, with third-party services, change the number that appears.

You have a few additional options that let you control incoming messaging in some services, too:

- In Settings > Phone, you can opt to Silence Unknown Callers. Calls without Caller ID go straight to voicemail without ringing.
- With Settings > Messages > Unknown & Spam > Filter Unknown Senders, you can send iMessages from those not in your contacts to a separate list.
- In Settings > Mail > Blocked Sender Options, you can choose whether to have blocked messages moved automatically to the trash, or mark as blocked and left in your Inbox.

How Does Manual Blocking Appear to Those Blocked?

When a blocked phone number's owner places a call, the line rings once, they hear a generic message about the person being unavailable, and they are dumped into voicemail. If they leave a message, it's listed separately at the bottom of the Phone > Voicemail list. The recipient isn't notified of the call.

Messages are shown to the sender as Delivered, but are dropped into the memory hole: the recipient doesn't see and isn't informed of them. Regular SMS and MMS text messages are likewise swallowed up without the sender knowing otherwise. With FaceTime, a placed call rings indefinitely without the recipient being notified. Email messages are received, but marked as blocked or placed into the trash.

Note: Apple added a new option in iOS 12 called Unwanted Communications for app developers to let users report junk messages and calls directly within Phone and Messages apps. I haven't seen apps yet take advantage even a year later.

Call-Blocking Apps

There's a special place in hell for telemarketers who acquire numbers illegitimately, and an even worse place there for those who try to defraud. (I don't much like legal and legitimate marketing calls from companies I do business with, either.) Fortunately, many flimflammers seem to re-use the same phone numbers or rely on a common pattern of behavior as they appear via Caller ID.

That makes Apple's extensions for blocking and identifying incoming calls extremely handy. Starting in iOS 10, Apple let app developers hook into the incoming call framework to either modify the Caller ID label or block the call entirely.

Several apps and systems already existed for Android, and some companies had pre-existing relationships for licensing user-contributed databases of spammy, scammy, and scummy calls to phone carriers.

You can find a variety of free, one-time fee, and subscription call-blocking apps in the App Store. Hiya, which I've used since the introduction of iOS 10, has a perfectly good free tier and is simple to use (**Figure 60**). (Hiya sells its services to carriers, and uses the free app to improve its database. A paid tier lets you perform reverse phone-number lookups.)

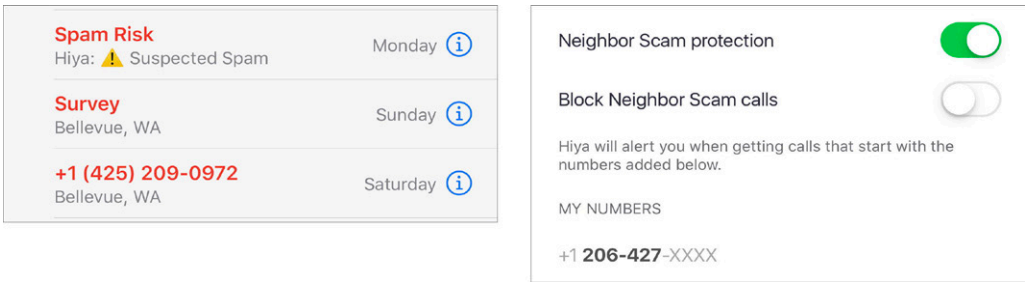

Figure 60*: Hiya marks calls as part of the incoming identifier (left). It offers options like neighbor scam protection (right), which marks or blocks calls from similar numbers.*

Once installed and launched in the OS, you use Settings > Phone > Call Blocking & Identification to enable one. Then you can configure options in the app for whether you want alerts, which are inserted into the Caller ID message, or outright blocking.

> **Note:** Sometimes the first time I try to enable a call-blocking app in Phone settings, the OS tells me the action failed. Trying again or visiting the app and then returning to Settings often fixes whatever weirdness was happening.

These apps don't collect incoming phone numbers. Rather, they have to download their databases to the OS, which results in regular updates to keep pace with newly added scam numbers. If you use these apps, you can report missed scams or add details about calls you answer, which does then submit that number to their database. Hiya currently requires

that you enable Hiya—1 and Hiya—2 in Settings, because its database is too large to fit into a single file per Apple's guidelines.

An alternative or supplement to OS-level call blocking is to use a carrier-provided tool that blocks and adds a spam, scam, or other label at the network level, not on your phone. All four major carriers in the U.S. offer apps that provide network-level features; all but Sprint make a basic tier of the app available free. The premium tier and Sprint's paid app add reverse call look-up and a few other options.

With these apps, calls your carrier is confident are fraudulent never ring your phone, or your phone might light up for a moment, at which point the call is blocked. You can optionally receive additional notification, depending on the app.

***WARNING**: Hiya, AT&T Call Protect, and other apps require access to your Contacts list in order to ensure those numbers aren't blocked. Without allowing access, the app won't function. While these companies all promise to not use your data for any other purpose—and AT&T can already obtain all the phone numbers you call or receive calls from—this might be a privacy nonstarter for some people.*

Filter iMessages and SMS

Apple has two additional tools to help sort through incoming contacts. You can filter iMessages and use third-party apps to scan the content of text messages.

Sort Messages by Whether in Contacts

Messages offers a subtle way to segregate incoming iMessages between people in your Contacts and those who are not. Enable it in Settings > Messages > Unknown & Spam > Filter Unknown Senders. Incoming iMessages that match any phone number or email address in Contacts appear in a Contacts & SMS tab. Conversations already underway appear in that tab, even if they're not in your Contacts.

All SMS/MMS messages show up there, too, because many text messages are confirmations, second-factor codes, and other information that would otherwise go missed.

Any new incoming iMessages after you change that setting that don't match a contact go into Unknown Senders. Such messages don't trigger your usual notifications flags, and you have to remember to review it occasionally to see if you've missed anything.

Tap Report Junk from an unknown sender to send details to Apple.

Filter SMS with Third-Party Apps

There's one final option that I have mixed feelings about. Third-party apps can process text messages from anyone who isn't in your contacts and analyze them for spam.

With this enabled, the Messages app's right-hand head at the top changes its label to either Unknown & Junk (with iMessage Contact filtering enabled) or SMS Junk.

Apple says SMS/MMS messages stop being sent to the filter from numbers that you add to Contacts or that you reply to three times.

I find shipping off SMS messages poses too great a risk for a general recommendation, regardless of the honesty and integrity of the company on the other end. You might feel differently if you're subject to an enormous amount of text-based spam or harassment.

SECURITY

Security encompasses many forms: What ways can you manage password use and create unique, secure logins? How do you deal with a device being stolen? How do you protect its contents when it's out of your control? How do you prevent people from snooping on your network sessions? Can you recover your device if it's lost? In this part of the book, you'll get answers that will make you feel better when using a device in all situations.

Create, Manage, and Use Strong Passwords

Apple's built-in password-management system creates, manages, and fills in strong, unique passwords for every web site you visit and every app you use that has opted to work with the system.

While Apple has tightly integrated its own approach, it also offers full-fledged integration of third-party password managers.

Tip: For a lot more about the ins and outs of good password management, read Joe Kissell's **Take Control of Your Passwords**.

What Makes for a Good Password

Most of the advice you read about choosing a good password is bad, including the "strength" bars on web sites that purport to reveal the quality of password you picked.

Fortunately, password generators, including from Apple and third parties, have gotten with the ticket. Here are the accurate facts:

- Pick a long password made of words you can easily remember and type or tap when you need to enter it regularly, like with a password vault or your iPhone or iPad passphrase.
- When forced to use a complex password (letters, numbers, and symbols), it needs to be longer than 9 characters—preferably 12 to 14.
- Use a unique password every time you create an account *anywhere*, and change old passwords that you've reused to new, unique ones.

- Rely on a password manager, such as the Apple provided one.
- Sign up for **Have I Been Pwned?** to get notifications of breaches that include your email address.

Now, on to the particulars.

A long password made of randomly chosen words is as strong as a short one that's a random collection of letters, numbers, and punctuation. For any password you have to enter, pick one that's 20 or more characters long and that you can remember. Make up a story to help you remember, even. For instance, for `rabbit-airplane-canada` picture a rabbit flying an airplane to Canada.

> **Note:** If you'd like to read more about using words in passphrases instead of incomprehensible nonsense, read my 2015 *Fast Company* article, "**Everything You Know About Passwords Is Wrong**," in which I talk to an expert researcher on password selection and cracking.

In many cases, a web site or app forces you to pick a password that contains uppercase and lowercase letters, numbers, and punctuation. You also rarely need to enter those by hand, and so a complicated password is fine—but make sure it's long. A web site password checker might tell you `Apple10!` is very strong and acceptable, but it's only 8 characters and includes a word found in a dictionary. It could take seconds to minutes for a cracker using common brute-force software to crack it. Pick 12 to 14 characters for complex passwords.

Apple's suggested passwords combine complexity and simplicity by being relatively long but (unless a web site doesn't allow it) comprising only letters and dashes.

Every password you use should be unique at every site and service. That sounds horrible, which is why you can use Apple or third-party software to generate them for you. In both the OS and third-party software, you can see a list of all stored passwords that you have reused.

Finally, **Have I Been Pwned?** is a great resource run by an Australian security researcher and trainer, who carefully vets and collects information from database breaches. If he adds a breach to his site and you've

registered with it, you receive email that warns you that your email address was in the breach—but not whether your password has been broken. It's a great idea to change it regardless. (1Password can automatically check against the database for you.)

Work with iOS and iPadOS's Built-in Manager

Whenever you visit a web page or use an app that requires a password, tapping in the password field (or sometimes also the user name or account name field) prompts you with a stored password that the OS thinks is the best fit.

That's typically either the first password stored in iCloud Keychain or the local OS store of passwords, the last password you used previously for the site or app, or the first password in a third-party manager if Apple doesn't have one stored for you.

To apply a stored password, you're prompted for Touch ID or Face ID before the system fills in the password.

Note: If you have iCloud Keychain enabled, the OS syncs your password to all other devices connected to the same iCloud account and on which you have iCloud Keychain active. Apple uses a cryptographic approach for syncing in which it never has access to keys necessary to decrypt your data—only your devices possess those.

Tip: You can enable and disable iCloud Keychain in Settings in iOS and iPadOS and via the Apple ID system preference pane's iCloud settings in macOS.

Passwords & Accounts

Passwords & Accounts is the main interface through which you manage the OS's use of both, well, passwords and accounts (**Figure 61**).

The top item is Website & App Passwords, where the real action happens. Tap it and then validate via finger or face, and you'll see a list that can be scrolled through or searched within (**Figure 62**).

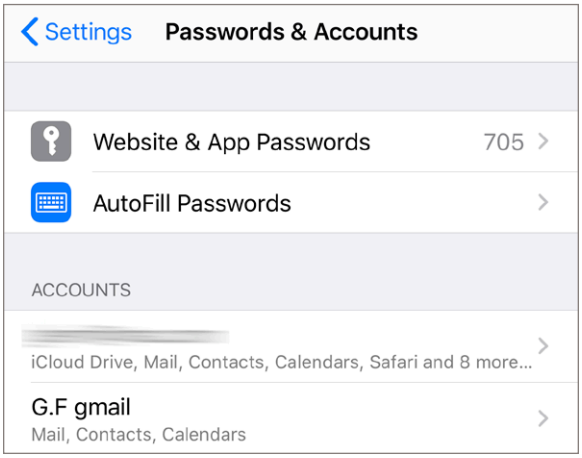

Figure 61: *Manage accounts and passwords via a single view.*

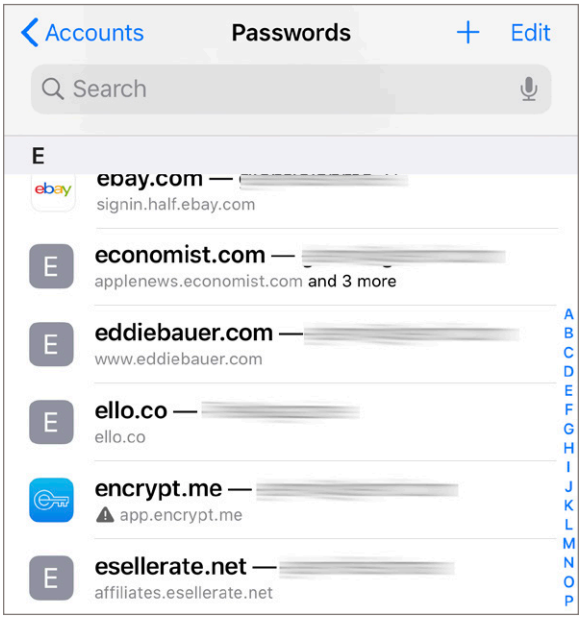

Figure 62: *This is a heavily redacted list of entries for my passwords.*

Change an entry

Select an entry and tap Edit, and then you can change any of the details (**Figure 63**). Of course, changing the user name and password doesn't affect what's at the web site, but it does let you manually update entries.

Figure 63: *Tap to edit or to remove associated web sites from the entry.*

You can also tap the remove icon next to associated web sites to stop offering the entry as an autofill option when you visit the site or an app that's associated with the site.

Share a password

You can now easily share passwords, but only via AirDrop (**Figure 64**). It's a good compromise between ease and security. It's simple: Tap the password, pick AirDrop, and select the destination.

Figure 64: *AirDrop lets you share a password to a nearby device.*

Tip: See the next chapter for two methods of sharing Wi-Fi network passwords that Apple introduced in iOS 11, and aren't widely used even now!

Switch away from password reuse

The OS warns you about re-using a password across sites or apps. A caution sign appears below the entry name along with a count of how many other sites also use the password (**Figure 65**).

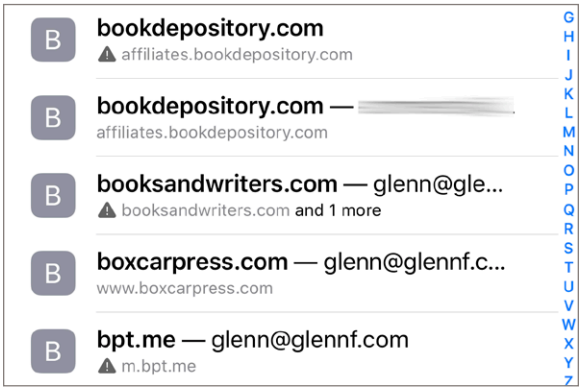

Figure 65: *The caution sign warns that a password is used at multiple sites.*

Tap the entry, and you'll see a Change Password on Website option. Tap that, and you're taken via a web sheet (not a trip to Safari) to the site to log in and update the password with a suggestion. Once that's accomplished, the OS takes you back to the password entry.

> **Tip:** Apple has tried to establish a standard web address for every site to use for its credentials-changing page. While there's no agreement yet, Apple went ahead and picked `https://domainname/.well-known/change-password`. When you click Change Password on Website, the OS tries to load that page, and if it fails, loads the home page instead. (In some cases, it may load an error.) You can add a redirection at that location on web sites you control to point to the password-changing page.

Apple doesn't provide a listing of all reused passwords as a kind of audit of problems. (You can find that feature in 1Password.)

Siri retrieves passwords

This might sound like a huge security hole, but you can ask Siri for passwords. The reason it's not a problem is that Siri doesn't *speak* the results. If you say, "Hey, Siri, what's my password for Netflix?", the OS takes you to the entry in Passwords & Accounts, but you have to authenticate yourself with Touch ID or Face ID before the entry is shown.

iOS and iPadOS Help with SMS Login Codes

If you use two-factor authentication (2FA) at many web sites, you receive a short numeric code via SMS (text message) after you enter the correct

user name and password for an account. This verifies that the person logging into an account has its password, but also possesses an associated physical device that can receive the code. It deters hacking.

However, it can be tedious to enter these codes, because they arrive via Messages. If you have notifications enabled for Messages, you see the code briefly and have to tap it in before it fades away. Or, you switch to Messages, copy the code (or try to memorize it), and switch back to enter the code.

Apple has streamlined this dance. When a recognized style of code arrives in Messages, Apple automatically drops it in as a prefilled item in the QuickType bar (**Figure 66**). When you tap into the field to enter the code, QuickType shows it; simply tap the code to fill the field. It's remarkably efficient. (It works in Safari in macOS, too!)

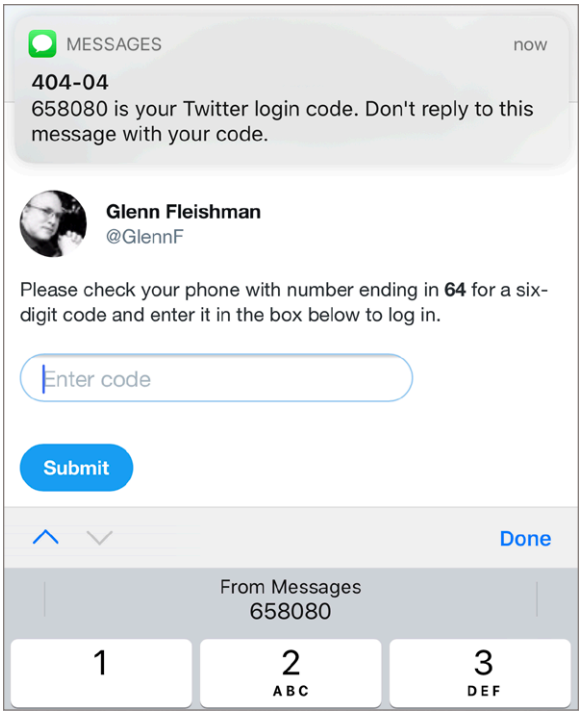

Figure 66: *SMS codes appear as autofill text in the QuickType bar.*

The idea is to convince more people to use 2FA by making it this easy—but there are risks, as I describe next.

Use Passwords in Web Sites and Apps and Devices

iOS and iPadOS neatly incorporate password management with Safari for individual web sites and with apps. This makes it much easier to log into an account used by an app that you've already stored via the web or another device, or to create an account with a strong, unique password.

Safari

Visiting a site's account-creation page in Safari automatically offers a strong password that tries to meet the rules stated on the page. The password isn't just created, but a large sheet appears with a nice explanation about what has just happened ("iPhone created a strong password for this website."), what will occur next, and how to find the password once it's stored. It also offers an option to pick your own password. The presentation is thorough and clear (**Figure 67**).

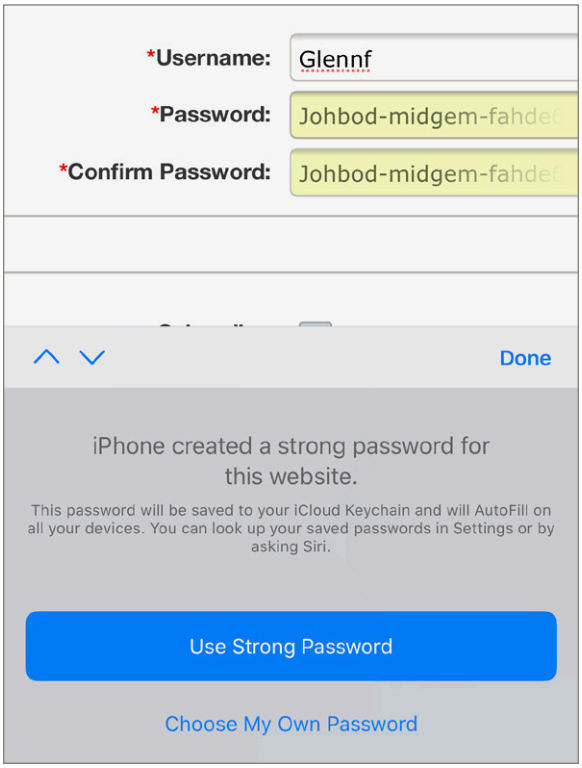

Figure 67: *Creating passwords for new accounts explains itself well.*

When you visit a site for which you have a stored login, the OS presents a large friendly blue button with the user name that you can tap to use. You then validate yourself with Touch ID or Face ID to enter the password (**Figure 68**).

Below the Use "account name" button, however, note there's both a keyboard icon and a password icon. Tap the keyboard to enter a password manually, and tap the password icon to view all matching ones for the site.

From that Choose a Saved Password To Use list, you can also pick options at the bottom (**Figure 69**). If you have a third-party password manager installed (as described next), it appears in the list along with iCloud Keychain. You can also pick Suggest New Password, in case you're trying to set up an account.

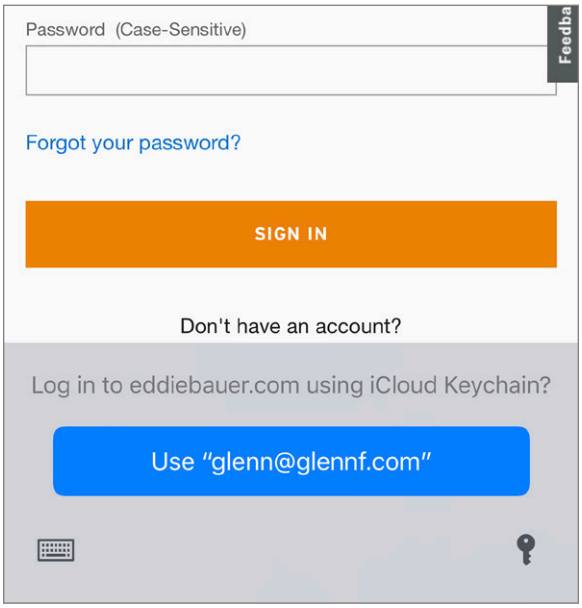

Figure 68: *The large friendly button makes it clear what action you can take.*

Other Apps

When you use an app that's correctly designed to talk to the OS for an account login, you see a login sheet that's exactly like Safari's. It's that simple! This includes both creating passwords and filling them in.

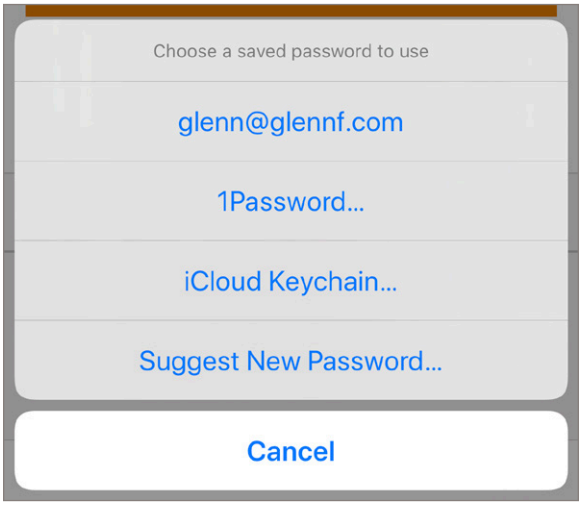

Figure 69: *The OS shows both its own matched, stored passwords and those associated with third-party password managers.*

Fill in on Apple TV

A nifty feature extends the connection between Apple TV's tvOS and iOS/iPadOS: You can type to fill in passwords on an iPhone or iPad using the prompt you receive when text fields appear in tvOS and your device is nearby. But you can also use password suggestions from the QuickType bar! As with Safari and apps, Apple TV password entry includes items from third-party password managers.

Use Third-Party Password Managers

Third-party password managers are full-fledged iOS and iPad OS citizens. The QuickType bar is the centerpiece, reducing the number of steps and some of the frustration in finding a password in a third-party system. You can also create passwords for web sites.

Apple still privileges its password-management system, so if an account matches one in the local keychain, it will present that first. However, you can opt to pick from a list by tapping the key icon (see **Figure 69**, above). That shows you other options in a list identified by app. Tap the app name to bring up the Share sheet approach for more options.

It's a little more complicated when creating an account. These are the steps in a third-party app; here, I'm using 1Password:

1. Tap in the password field on a create account page.
2. The OS shows its account-creation option with a big blue button. Tap Choose My Own Password.
3. Tap the key icon in the QuickType bar.
4. Select 1Password.
5. Use Touch ID or Face ID to validate yourself.
6. Tap Create Login and fill in all the details you want to use.
7. Tap Next.
8. The password field is filled in, but you may have to re-enter your user name or email. You can use AutoFill Contact or enter personal details, too.
9. Finish the account creation by tapping Register or whatever the final stage button reads.

My Password Manager Recommendation: 1Password

1Password is an ecosystem of apps that allows secure creation, storage, and synchronization of passwords. It has native apps for iOS, iPadOS, and Android, desktop apps for macOS and Windows, and a robust web app that keeps all encryption and decryption in the browser, so the company has no access to your private details.

Its developer, AgileBits, switched mostly to a subscription model a few years ago, in which a modest monthly or yearly fee gives you free access to all associated apps across all platforms, as well as a custom 1Password domain for yourself, a business group, or a family.

You can use the apps at no cost, but you don't get 1Password.com-based sync and a number of other features. I have a family subscription, which covers five users, and it's been a great benefit for my wife, my kids, and me, especially sharing passwords among us.

Although other ecosystems exist, I've used 1Password for years and find it the most amenable to use. The way 1Password works within Apple's mobile OS is very similar to **LastPass**, another great choice that many people I know have likewise committed to for years. (This is a freely made endorsement: I'm not paid anything for the recommendation.)

If you'd like to become a whiz at 1Password and take full use of its features, including sharing among workgroups and families, make sure to read Joe Kissell's **Take Control of 1Password**.

Connect to a Secure Wi-Fi Network

Most home networks are secured, and business networks almost universally employ some way of keeping outsiders out. Connecting to these secured networks is often as easy as entering a password, but not always. This chapter helps you handle any difficult security situations you encounter.

If you're setting up Wi-Fi security for a network, this chapter also discusses what sort of security to use and how users with mobile devices will connect.

Wi-Fi security divides into three main types: methods used for small networks, methods for large ones, and outdated methods you should avoid.

Note: Cellular networks have their own security methods that users can't affect.

WARNING! *Public hotspots, whether free or fee, typically have no encryption protecting data; if they have security enabled, it's via a shared password that provides no effective protection from other people on the network. When you connect, I recommend using only secured services or a virtual private network (VPN) connection. Read* ***Connect with a VPN*** *for details.*

Connect to a Small Network

Nearly all home and small-office networks that have wireless security enabled require the entry of a short password or passphrase. Enter the password when prompted, tap Join, and, if entered correctly, you're done.

The password is stored for the next time you're near the same network, and it's automatically supplied by the OS. If you don't want to join the network automatically the next time you're nearby, or don't want to store the password on your device, launch Settings, tap Wi-Fi, tap the info ⓘ button next to the network, and tap Forget This Network. (This only works while you're connected to the network, however.)

If you have **iCloud Keychain** enabled, entering a Wi-Fi network password into any synchronized device means that you won't have to enter it again. Thus, you might connect to a network via the OS that you've already connected to in macOS and not be prompted, and vice versa.

> ***WARNING!*** *Readers have told me that they can wind up in an iCloud Keychain loop: they delete a network on one device, but iCloud Keychain resyncs it from another before the deletion takes place and syncs outward! There's no real solution: persist at removing the network until it "sticks."*

Share a Wi-Fi Password

iOS and iPadOS have two easy ways to share a Wi-Fi password with someone in the vicinity: One relies on Bluetooth, the other on a QR Code.

Share a Wi-Fi password with someone in your contacts

You have a simple way to share a Wi-Fi password with someone nearby that requires just a single tap. Both the person already connected and the person connecting must have Bluetooth enabled, and the sharing person needs the iCloud account email in their contacts of the other person.

I explained this in depth back at the start of the book. See **Join a Network** for instructions and an illustration.

Share Network Access with a QR Code

Back in iOS 11, Apple added a nifty visual way to share network details with a minimum of fuss: You can use a QR Code and the Camera app! Developed in the Android world, Apple added support for this hotspot sharing format, which encodes the network name and its password.

To create a Wi-Fi QR Code, you have to use a web site or an app; Apple doesn't have a built-in tool. I suggest QiFi, which uses JavaScript to create the code entirely in your browser without sending your credentials off to a server to create the code.

You can join a network via a QR Code by just pointing your iPhone or iPad camera at it (**Figure 70**). (Settings > Camera > Scan QR Code has to be turned on, which it is by default.) The OS alerts you to join the network. Tap the message, then tap Join Network.

You can also add a shortcut in Control Center via Settings > Control Center > Customize Controls, and add QR Code Reader. It now appears when you swipe and open the Control Center. When you scan the code, you're prompted directly to join a network with a single tap.

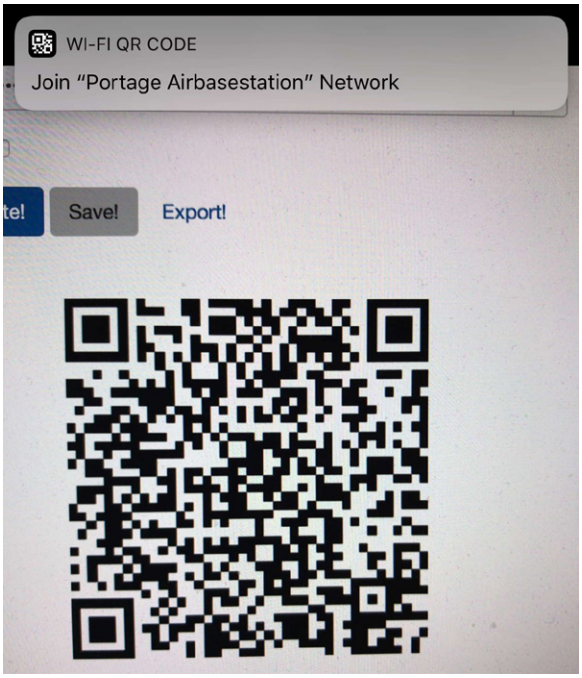

Figure 70: *Join a Wi-Fi network (or share one) via a QR Code. (Not my real password!)*

WARNING! *The password isn't encrypted in the QR Code! It's just encoded in dots. So you don't want to post this online or leave it lying around. It's great for public hotspots, however, or in your home.*

What's Behind Simple Wireless Security

The best or only practical security method for connecting to a Wi-Fi network in a home or office is Wi-Fi Protected Access 2 (WPA2), supported by more or less every device sold with Wi-Fi for nearly 15 years.

> **Note:** You may have read about WPA3, a newer Wi-Fi security standard. It brings welcome features, including encryption that's unique to each user between their hardware and a network gateway—even on a network without password protection! Apple started supporting WPA3 encryption in iOS 13, iPadOS 13, and macOS 10.15, but it's not yet widely available in Wi-Fi gateways.

WPA2 comes in two forms: personal and enterprise. The personal part refers to protecting the network with a password—sometimes called a passphrase since it can comprise multiple words. It can be up to 63 characters long and include symbols, letters, and numbers. The passphrase is run through mathematical churns to produce something stronger.

A base station's administrator sets the passphrase and then provides it to anyone who needs to connect to the network. If you've set up the network yourself, you're the person who picks the passphrase.

If you're setting up a base station, pick a good passphrase. The best WPA2 passphrases are at least 12 characters long; 20 is better. (For more password advice, skip back to the previous chapter.)

Connect to a Corporate or Academic Network

There are stronger ways to secure a network, and if you use an iPhone or iPad in corporate or academic settings, you will likely encounter WPA2 Enterprise. This flavor puts up a wall that lets you interact only in a limited fashion with the network to provide login details before your device is granted full access to the network and, typically, the Internet beyond.

WPA2 Enterprise networks are most frequently secured by a username and a password. However, a digital certificate (described below) can also be used for login. The OS supports these and other types of WPA2 Enterprise. Let's look at each option in more detail.

Username and password login

In the simplest setup, you must enter a username and a password provided by the network administrator or IT department to connect your device to a WPA2 Enterprise network. Often, these are the same credentials you use for file service, email, and other network resource access, such as your email mailbox name (the part to the left of the @) or full address (`user@domain.com`) for that network.

To connect to a WPA2 Enterprise network of this sort, select the network, enter your username and password, and tap Join. It's that easy. If you get an error, check your entries. If they are correct, then contact network support: You won't be able to troubleshoot this any further, because there are no settings to tweak in the OS.

> ***WARNING!*** *Some networks may have policies that limit these sorts of logins to specific days and times, among other parameters. That's rare outside of high-security corporate networks, though.*

Certificate-based login

In the case of WPA2 Enterprise, a digital certificate may be an alternative to a username and login as the certificate can't be written down on a sticky note or extracted in some fashion. A certificate combines cryptographic details with identity information to verify a login.

Typically, an IT worker creates and provides you with a certificate and installs it for you. However, an iPhone or iPad can receive a certificate via email, and install it when you tap it as an attachment.

Use Two-Factor Authentication

Apple's two-factor authentication (2FA) for Apple ID lets you secure access to your accounts with a password plus something extra that you have under your control. In this chapter, you learn how to set up 2FA, how to secure your extra pieces against discovery or loss, and how to reset an account.

What Have You Got in Your Pocket?

Apple lets you tie in an Apple ID for several purposes in iOS and iPadOS: for iCloud sync, iCloud Drive, App Store purchases, iMessage, and more. However, without making an extra effort, an Apple ID is protected only by the password you set. It can be reset and potentially hijacked in a number of ways should someone gain access to your email or know your security questions for resetting a password.

The way around this is two-factor authentication (2FA). A factor is a bit of proof that you are who you say you are. Requiring two factors of different sorts makes it more likely that you are the legitimate owner of an account or have authorized access for a service.

A two-factor system generally employs *something you know*, such as a memorized password, coupled with *something you have* or possess—such as a phone, a smartcard, or other hardware—or *something you are*, like a fingerprint. Usually there's an emergency backup, too: a one-time code that can be used in a pinch, or a process to prove your identity.

In Apple's implementation, when you enable two-factor authentication, you keep your existing password on your Apple ID, and add at least one phone number that can receive SMS (text) messages or voice calls, and one or more trusted mobile devices or Macs.

WARNING! *Once you turn on 2FA, if you can't recall your password* or *lose access to your phone number and all your trusted devices, you have to go through a recovery process with Apple to regain access to your account, which can take up to a week. If you can't prove to Apple you're the legitimate owner, you have to create a new Apple ID, which makes you lose access to any associated purchases, unsynced items, backups, and the like.*

Tip: Apple added automatic second-factor filling via SMS in iOS 12 for other companies' sites, as I discussed in **iOS and iPadOS Help with SMS Login Codes**.

Note: Apple initially offered a harder-to-use *two-step verification* for improved account security. It dropped this older method a few years ago, but allows accounts that have it active to keep using it until any device connected with the account logs in from macOS 10.13 or later or iOS 11 or later. The account is then automatically upgraded to 2FA. Two-step is managed via Apple's Apple ID site.

The Risk of SMS 2FA Factors

Even though a number of 2FA systems don't primarily rely on SMS, and let you use a code-based system like Authy or Google Authenticator, most of them fall back to SMS if you simply click a link—no other validation is required. This is true of Apple's system.

This is unfortunately increasingly risky, especially to protect email, financial, and other accounts that can be used in a cascade of cracking to steal your identity.

You may have heard about SIM (Subscribe Identity Module) hijacking, but if you haven't, you need to know. A SIM is used with the majority of cell phones worldwide (and AT&T and T-Mobile in the U.S.) as a unique identifier for billing and to which the carrier assigns a phone number. You'll note that if you move the SIM from one iPhone to another, the phone number follows it? That association lives in the carrier's database.

With SIM hacking, someone uses social engineering—they call up a cell phone company or go into a store and fool someone—to get your phone

number shifted from your SIM to one they control. With messages coming to your phone number, some sites allow a password reset or other access, because you allegedly have the second factor, since you received the link via that phone number.

> ***WARNING!*** *SMS Forwarding, part of Continuity, forwards text messages to macOS, iOS, and iPadOS, including security codes. If you have any concerns about someone having access to your Mac, disable SMS Forwarding.*

This vector has been used to steal millions in cryptocurrency from online wallets, hijack Twitter CEO Jack Dorsey's @jack account briefly, and transfer real cash from bank accounts to scammers elsewhere.

Don't get me wrong: *It's better for people to use SMS codes than not to use 2FA at all!* But a shift still needs to take place to move away from SMS having the same *power* as a password. Sites should stop allowing account resets via SMS-transmitted messages. They should also allow a sophisticated user to disable SMS entirely, relying only on authentication apps or one-time-use-only codes provided at most sites when you sign up for 2FA.

A More Secure Second Factor for the Web

There's a less-risky form of 2FA making its way into the marketplace that requires a hardware USB token and relies on public-key cryptography. The technology has been in place for years for particular purposes, but it accelerated in 2019 with the broad support by all desktop browsers—including Safari for macOS—and Android mobile browsers of *Web Authentication* (WebAuthn for short). WebAuthn allows secure second-factor logins via web browsers, avoiding SMS and authentication apps, and doesn't require anything proprietary.

With WebAuthn, you purchase a USB stick and use it when you register for WebAuthn protection at sites that support it, like Dropbox and Google. The stick provides unique encryption information to the site that allows the site to verify you when you return.

When you next login, the site prompts you to insert the USB stick and tap a button on it. The stick then produces a signed cryptographic message that only the registered site can verify and only that stick can produce. The site confirms the message and lets you in.

As I write this edition of the book, it's not clear if Apple will support WebAuthn in Safari for iPhone and iPad, but there is a Lightning/USB-C token you can purchase from Yubico, **the YubiKey 5Ci**, that works with individual apps, like 1Password and the Brave browser.

Turn On Apple's Two-Factor Authentication

You enable 2FA on your account on a device by logging in: Tap an opt-in button in Settings > iCloud in iOS or iPadOS, or click an opt-in button in Passwords & Security in macOS's Apple ID preference pane.

> ***WARNING!*** *Apple says that opting in to 2FA is permanent, following a two-week grace period. From that point on, you've irrevocably switched over.*

Enable Two-Factor

1. Go to Settings > iCloud > *account name* > Password & Security. You may be prompted to enter your password when you tap *account name*.
2. Tap Turn on Two-Factor Authentication and tap Continue.
3. You start by entering a phone number at which you can receive a text message or voice call; you can choose which (**Figure 71**).

   Select your country, enter your number, pick Text Message or Phone Call (to get an automated call), and tap Next. A code arrives. (If no code shows up, tap Didn't Get a Verification Code?, which lets you re-send it.)

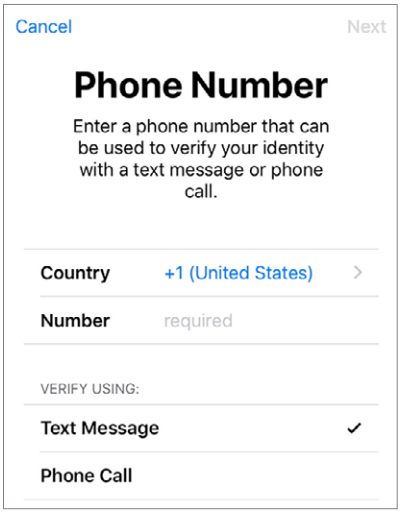

Figure 71: *The process starts with entering a phone number.*

4. Enter the verification code and setup is complete.

The Password & Security settings now show Two-Factor Authentication set to On, and list your Trusted Phone Number (**Figure 72**). As you add phone numbers and devices, they appear here, as well as at the Apple ID web site. You can also remove trusted devices and phone numbers.

Figure 72: *iCloud settings show that two-factor authentication has been enabled.*

Disable Two-Factor

As noted earlier, Apple doesn't allow 2FA to be turned off after two weeks. And it removed an explanation in settings about how to disable it. Here's how, if you're still within that two-week grace period: Visit the **Apple ID site**, log in, click Edit next to Security, and then see if you have a link labeled Turn Off Two-Factor Authentication. If so, click it, choose new security questions, and click Continue. You'll be asked to confirm one last time, and then you're back to a password-only account.

Log In with 2FA to Apple Sites and Services

When you log in to iCloud in iOS, iPadOS, or macOS, log in via a web browser, or attempt to purchase an item through any of Apple's digital stores with a device that hasn't previously done so, you'll be prompted to validate your password-based login with a code sent to a trusted device.

After logging in via Settings > iCloud or the Apple ID preference pane in macOS, that iPhone, iPad, or Mac becomes a trusted device. With a login to iCloud.com, you can opt to trust the browser.

Note: Because macOS has separate user accounts, trusted device status is set for each user account individually. Each macOS user can log in to a different iCloud account.

Note: Apple requires 2FA to use its new Sign in with Apple login service.

Generally with 2FA, you enter your Apple ID email and password and receive an alert at all your trusted devices. You pick one that receives the code. You can also bypass this to receive a code via a trusted phone.

Log in to 2FA on a Trusted Device

With a trusted device, you have an extra confirmation step:

1. Open Settings in iOS or iPad or go to the Apple ID preference pane.
2. Enter your user name and password.
3. At all your trusted devices, you're prompted with an Apple ID Sign In alert, which shows the account name, the nearest city, and a zoomed-out map, along with Don't Allow and Allow buttons (**Figure 73**). Click Allow.

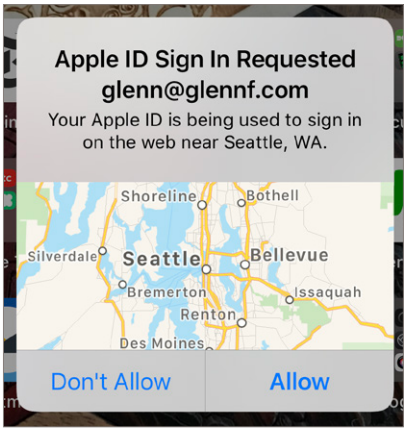

Figure 73: *To avoid unwanted logins, you're shown a geographic alert. It might not be that accurate and it's definitely not zoomed in precisely.*

WARNING! *If you choose Don't Allow, the remote login can't proceed, and Apple prompts you with a warning. It says, "If you think someone is trying to sign in to your account, you should change your password."*

Note: If you click Don't Allow by accident, get a new verification code on a trusted device. Visit the Password & Security view (in iOS and iPad OS, Settings > *account name*; in macOS, the Apple ID preference pane), and tap or click Get Verification Code.

4. On the device from which you clicked Allow, a Verification Code alert appears. Enter the verification code on the requesting device.
5. Tap OK or click Done on the trusted device on which you clicked Allow.

   If you have any login trouble, you can resend the code, choose to use a trusted phone number (described next), or contact Apple support.

Log in to 2FA using a Trusted Phone Number

If you don't have access to a trusted device at the time at which you want to log in, you can use a trusted phone. Follow these steps instead:

1. Open Settings in iOS or iPadOS or go to the Apple ID preference pane.
2. Enter your user name and password.
3. On the requesting device, click Didn't Get a Code.
4. From the Verify Your Identity dialog, select a phone number if you have more than one, and then choose Text Message or Phone Call, before clicking Continue (**Figure 74**).
5. Enter the number you receive via text or by automated voice call into the requesting device or software, and you're done.

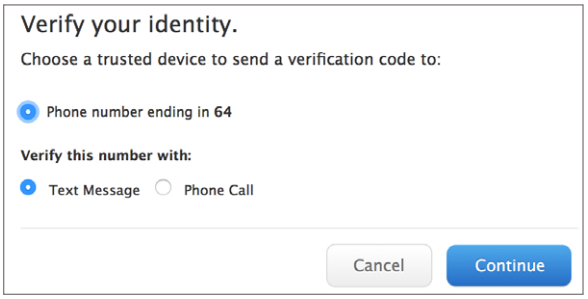

Figure 74: *You can opt to use a phone number instead of a trusted device.*

Log in with 2FA in a Browser

Apple also supports 2FA logins for many kinds of browser-based services, including iCloud.com, Apple Developer resources, and iTunes Connect for publishers and podcasters. Follow these steps to log in:

1. Visit the web page in question, click Log In, and enter your user name and password.
2. Follow steps 3 to 5 for "Log in to 2FA on a Trusted Device," or click "Didn't get a verification code?" (**Figure 75**) and follow steps 3 to 5 for "Log in to 2FA using a Trusted Phone."

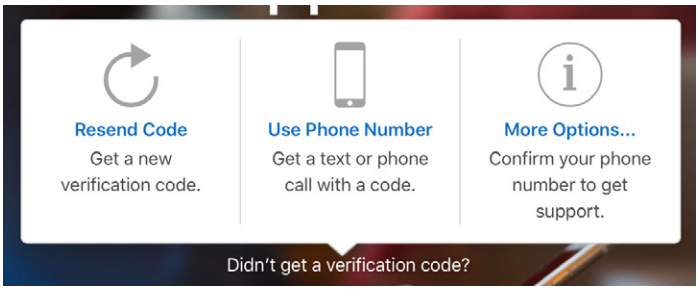

Figure 75: *You have several alternatives if the code doesn't arrive or you want to use a trusted phone number instead.*

3. You're prompted to Trust the browser (**Figure 76**). Clicking Don't Trust will disconnect you from the session; Not Now trusts the browser for just the current session.

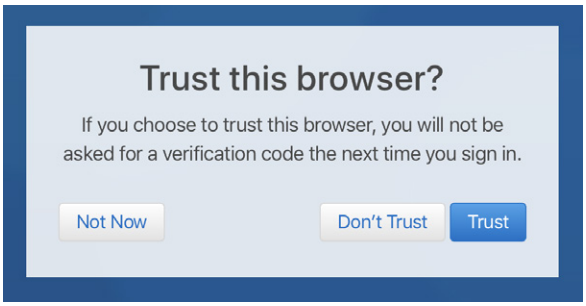

Figure 76: *Browsers can be trusted just like iPhones, iPads, and Macs.*

You May Be Asked For Your Device Passcode or Password

In some cases, the first time you log in using 2FA to a given device, you may be asked for your iPhone or iPad passcode or passphrase or your Mac's password (**Figure 77**). Is this a violation of Apple's security principles? Hold the phone (or iPad)! It makes sense.

Figure 77: *This seems wrong, right? But it's actually very secure.*

If you're using iCloud Keychain, Find Me, or other services in which each device in your set of iCloud-linked devices has unique encryption keys that Apple never possesses, then when you log in via 2FA, it can't add that new device to your set. Instead, it relies on something only you know. In some cases, you may be asked for an iCloud Security Code, which Apple generates from an existing device in the set and never sees, either.

However, it looks like Apple has moved more broadly over to relying on passcodes and passwords. It uses strong one-way encryption to add the passcode or password to the protected dataset. On the newly added device, entering that secret decrypts the data locally without Apple knowing or handling it. Apple could explain this more clearly!

Log In to Services with App-Specific Passwords

Because calendar events, contacts, and email can be used with non-Apple software, Apple lets you create up to 25 special *app-specific passwords* for use with third-party apps via the **Apple ID site**.

1. Log into the Apple ID site.
2. In the Security section, click Edit at far right.
3. Under App-Specific Passwords, for each password you need to create:

   a. Click Generate Password.

b. Enter a label that helps you remember for what purpose you created the password and click Create.

c. Copy the password that appears and paste it into the software with which you need to use it (**Figure 78**).

d. Click Done.

If you ever want to revoke an app-specific password, return to the Security section, click Edit, and then click View History. If you've lost track of which passwords are used for which services (even with your labels), the date and time created appear next to each. You can click the X next to each one to revoke it, or you can click Revoke All to start over.

Tip: These app-specific passwords can't be recovered. If you can't recall one, just generate a new one and revoke the old one.

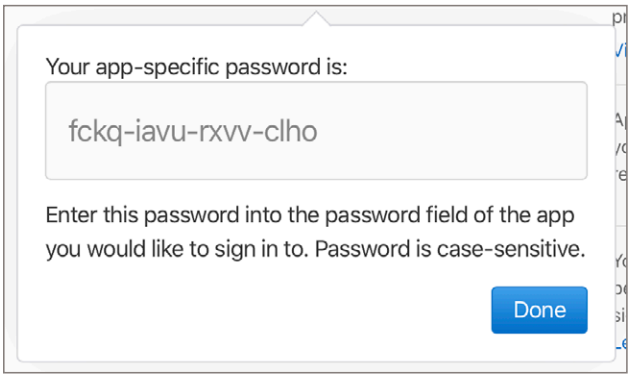

Figure 78: *I can show you this password because I immediately revoked it.*

WARNING! *App-specific passwords bypass two-factor protection and, if recovered, could be used to access contacts, calendars, and email.*

Manage 2FA Devices, Contacts, and Email

You may need to make changes to your Apple ID details after enabling 2FA. Adding trusted phone numbers, removing trusted devices and phone numbers, and managing a notification address are all handled in different ways.

Add or Remove a Trusted Phone Number

Add trusted phone numbers via iOS, iPadOS, macOS, or the **Apple ID site**.

- **iOS or iPadOS:** Go to Settings > *account name* > Passwords & Security, tap Edit next to Trusted Phone numbers. Tap Add a Trusted Phone Number to add one. Tap the red remove icon and then tap Delete to remove one.
- **macOS:** Open the Apple ID preference pane, click the Password & Security tab (**Figure 79**). Click + to add numbers or select a number and click – to remove it.

Figure 79: *Trusted phone numbers can be managed in several places, including macOS.*

- **Apple ID site:** In the Security section, click Edit at the far right, and then click Add Trusted Phone Number. You cannot delete trusted numbers via the site.

  In each location, you enter a phone number, choose whether to send a text message or receive a phone call, and then enter the verification code.

  If you don't get the verification code immediately, you can go to any of the above configuration locations and click Verify to try again.

Remove a Trusted Device

You can remove a trusted device via iOS, iPadOS, macOS, or the Apple ID site. The process is nearly identical in every place. Here are the instructions for iOS and iPadOS:

1. Tap Settings > *account name*.
2. Tap a device in the list (**Figure 80**).
3. Tap Remove From Account.
4. At the prompt, tap Remove to complete.

   You can add a device back by logging in to iCloud on that device. It will then rejoin the set of trusted devices.

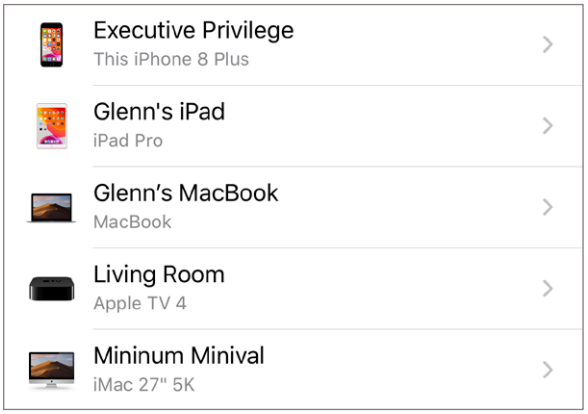

Figure 80: *All trusted devices are listed wherever you can log in to examine the details of your Apple ID account.*

Manage Your Notification Email

You can add a notification email that's used for critical messages, and that will aid you if you need to unlock or recover a two-factor account.

You have to use the **Apple ID site** to change this address or remove it. After logging in to your account:

1. In the Account section, click the Edit button at far right.
2. Under Notification Email, click Change Email Address.
3. Enter an email address and click Continue.
4. Apple will send you an email with the six-digit verification code. Check your email, and then enter that code and click Verify.

   You can later remove this address by returning to the same location, clicking Edit, and clicking the X next to the address.

Recover Account and Access

So you need two factors to log in: a password and a verification code. But what happens if you forget your password or you lose access to your trusted phone numbers and devices? Apple has responses for each.

> ***WARNING!*** *Apple used to let you easily reset your password with a trusted phone number, but now buries that option.*

Reset Your Password with a Trusted Device

You can reset your password from any trusted device without having the password. Follow these steps in iOS or iPadOS:

1. Tap Settings > *account name* > Password & Security > Change Password.
2. Enter your passcode and tap Done (**Figure 81**).
3. Enter a new password and type it again in the Verify field.
4. Tap Change.

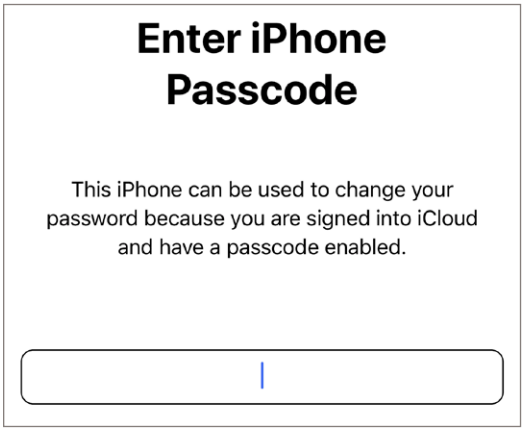

Figure 81: *You can reset your Apple ID password via a logged-in iOS device.*

On a Mac, you follow a fairly different process, because it forks:

1. Open the Apple ID preference pane and click Password & Security.
2. Click Change Password.

3. You may be prompted to enter your Apple ID password and your macOS username and password. Proceed entering both.
4. Enter your new password and then enter it again in the Verify field.
5. Click Change.

> ***WARNING!*** *Do not lose your Recovery Key. It's really the only way after it's enabled to regain access to your account if you lose access to all your trusted devices.*

Lost All Trusted Devices

Apple offers a last-ditch effort when you have no access to trusted devices or phone numbers. It calls this *account recovery*.

Apple warns that it could take several days or longer to get you back into your account, as it uses a combination of information it requires from you and a time delay to dissuade people who may be trying to hack your account from succeeding.

You can start recovery in a number of ways:

- In macOS, go to the Apple ID preference pane, click Password & Security, and click Change Password. Now click Forgot Apple ID or Password and follow steps.
- On the web, go to **iforgot.apple.com** and follow prompts.

> **Note:** Oddly, there's no way to start recovery in iOS or iPadOS while logged in, even if you can't recall your password.

Apple sends an email confirming that the process has started, and tells you when it expects to be completed.

You can go to **iforgot.apple.com** and check on progress. You might be prompted to enter your credit-card details for the account, which can shorten the recovery period.

If you remember your Apple ID and password and log in anywhere, or you regain access to a trusted device that's already logged in, account recovery cancels automatically.

Use a Recovery Key when Automatically Upgraded

If you were using two-step verification and then upgraded to iOS 11 or High Sierra or later, Apple upgraded your account security to 2FA. It also offered you one unique additional option to reset your password.

The two-step method had a last-ditch account reset option that required a uniquely generated Recovery Key. The 2FA system doesn't use it, but folks who were *automatically* upgraded have the option of creating a fresh Recovery Key. However, if you create a Recovery Key, Apple disables all other recovery methods, including the last-ditch one described above. Consider that tradeoff.

To generate a Recovery Key in iOS or iPadOS, go to Settings > *account name* > Password & Security and tap Recovery Key. On a Mac, go to the iCloud system preference pane, click Account Details, and click Security. Then click Turn On in the Recovery key section. Follow the steps in both places to complete the process.

Connect with a VPN

The data that travels to and from your iPhone or iPad isn't secure even when you're connected to a Wi-Fi network with a strong password. Any data you send that's not encrypted could be sniffed by anyone else on that network.

The same is true for any point between you and your data's destination or wherever you're running an active session, whether you're using a protected Wi-Fi network, an open one, or a cellular data connection: any party in between, for unencrypted services, can see exactly what you're doing.

Fortunately, nearly all the apps we use and most web sites now employ secure connections, checking that item off the list. But if you want to put a cherry on top, add a virtual private network (VPN). It makes sure that all your communications are wrapped inside encryption.

Umbrella Protection

A virtual private network connection is a nifty way to prevent any sniffing of your local network hookup. A VPN creates what's called an *encrypted tunnel* that extends between a device—an iPhone, iPad, or laptop, or desktop—and a VPN server somewhere else on the Internet. This lets your information traverse any local network with protection as well as every node on the Internet between you and the VPN server.

For corporations, VPNs can extend the aegis of corporate security to remote devices. For individuals, that's less the case. With a company, the VPN server is within the corporate network and any data leaving that server is protected by company firewalls and intrusion prevention.

But if you're using a VPN just to protect your local link (the connection between your device and the hotspot), data remains encrypted only

until it hits the VPN server, usually located in a data center. From that data center to its destination, data is unprotected (unless wrapped in an encrypted method, like TLS on the web, described earlier), but that's typically just fine. The main locus of risk is the local link.

> ***What about Other Data?*** *When I began writing this book years ago, I had to include instructions for securing email, web connections, and other services. In 2019, however, the web has largely moved to https for everything, email connections are encrypted by default nearly everywhere, and encrypted messaging apps are readily available. VPN adds to security, ensuring that anything that remains sent in the clear gets wrapped up, while also making your activities—to what you're connecting—invisible to peepers.*

And because major Internet sites—like Google, Apple, and the rest—have distributed sets of computers and even private links to big data centers, the hop from the VPN server to the destination network may be within the same building or close by.

Before you can set up a device, however, you need to find a VPN service.

Get VPN Service via an App

Many, many apps offer VPN services from a few hours or a fixed amount of data to unlimited monthly plans. With a VPN for hire, the connection you make—as noted above—runs from your device using the local Wi-Fi or cellular network, then goes through any intervening local area network routers and higher-level backbone routers. It winds up at one of the company's VPN servers located in a data center, where it's then sent over the open Internet.

> **Note:** You can also install a VPN app for the Apple Watch and Apple TV.

Pick a VPN app

Because it's exceedingly inexpensive for an app developer to set up VPN service, many thousands of offerings proliferate, and it's difficult to figure out which ones to trust.

I start with trying to find a reputable company, rather than seeing what features are offered in a VPN app, which are mostly comparable, or comparing pricing. Follow links from a company's App Store listing and then research the firm to see how long they've been in business, whether their reviews and Facebook page are riddled with negative comments and reviews, and how easy it is to find their technical support.

Several computing and mobile magazines and sites run VPN products through their paces and check privacy policies. If you're looking for reviews, avoid sites named something like TopBestThings or TheBestVPNAppYouCanFind—these are typically paid-placement sites masquerading as objective review sites. Instead, go to Macworld, Wirecutter, PCWorld, Ars Technica, or other well-known publications.

I'll provide a single recommendation, because I've used the service off and on: **Encrypt.me**. Encrypt.me is run by an established company, has good pricing, and routinely updates and improves its app. I'll use Encrypt.me as an example in the rest of this chapter.

I also suggest security and privacy-minded people take a hard look at **Guardian Mobile Firewall**, which is still in its early days. It's a combination of VPN and privacy firewall. The developers are security researchers who constantly update a list of undesirable tracking URLs embedded in iOS apps and add them to a block list. At present, Guardian is the only way to block or monitor app-based network activity comprehensively.

Set up a VPN app

To get set up in the OS, you download a service's app. Most apps offer a free trial period. On first launching a VPN, during the setup process for creating an account, you will be asked at some point to add a VPN configuration that includes all the server and connection details required. This is nice because you don't need to deal with the fiddly bits described in the manual setup section below. And if the profile needs to be updated because the service's details change, they can push a fresh one through their update, rather than asking you to reconfigure by hand.

1. Launch the app, which will detect during setup that no profile is available and request to install it (**Figure 82**).
2. Tap Allow.

3. Enter your passcode or use Touch ID or Face ID when prompted in the Settings app.

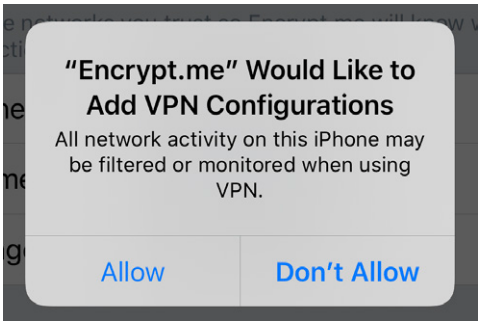

Figure 82: *Launch the app, and you're prompted to add a VPN configuration (left); on devices with Touch ID or Face ID, you use that method to approve.*

The profile is installed and you're returned to the app.

After installing a profile, you can use the app or Settings > VPN to start or end a connection. A VPN label will appear in the status whenever the connection is active. You can find more information about these options in **Make a VPN Connection**.

VPN services like Encrypt.me can initiate a VPN connection "on demand," too: Go to Settings > VPN, tap the info ⓘ button, and then turn the Connect on Demand switch on. However, it's usually better to set up connection defaults in the app.

Encrypt.me lets you set it to connect automatically when you join Wi-Fi networks, as well as pick trusted Wi-Fi networks to bypass. You can also choose to trust or distrust the cellular connection by default: When trusted, the VPN won't engage when you switch from Wi-Fi to cellular; untrusted, and it always engages.

Country-hopping with a VPN

There's one more trick up the sleeve of VPNs: They can connect you to data centers in countries other than the one you're in, making it seem as if you're in that country. This can be handy when you want to access a service from a different country, or when you might distrust an ISP, cellular network, or entire country that you're in. (This isn't a joke: Many countries routinely monitor and suck down data that's sent, in the clear and otherwise.)

It was once useful as well to evade certain per-country licensing limitations on free and subscription online video streaming and other services. These services started tightening requirements in 2016, and it's now very difficult to bypass them with these workarounds.

You can also pick a different part of the country you're in, too, which can reduce latency. VPN services try to pick the closest "topological" location—the data center on the Internet the fewest hops and shortest latency from where you are—but you might want to force the matter by picking San Francisco or Miami.

In Encrypt.me, you tap a location icon in the lower left, pick a location from its Transporter menu, then click Done. To revert, return to Transporters and tap Fastest Available.

Pricing options for VPN apps

Every VPN service is paying not just for servers and the overhead of staff and the like, but for the bandwidth you consume as well: Every gigabyte you send through a VPN is one gigabyte inbound and outbound, and that has to be paid for somehow. Some users will consume 500 GB a month; others, a trickle.

However, because the cost of bandwidth at data centers has plummeted in recent years, complicated offerings of times past have also seemed to evaporate. Most VPN services now have general plans that offer unlimited data usage for a period of time.

Encrypt.me, for instance, has non-recurring "passes," for a week ($4), a month ($10), or year ($100); a subscription to the monthly and yearly service are the same price. A Mini Plan at Encrypt.me is $3 a month, and includes 5 GB. Some VPN services have a free tier instead of a trial offering, and include a minimal amount of data a month in that tier.

Encrypt.me's monthly and yearly pricing is about the same as that charged at nearly every other service; a few well-reviewed ones are $10 or $20 less per year.

You're often better off signing up for a VPN plan through a company's web site instead of in an app. Web site plans often allow multiple users logged into the same account and have family or small-business options.

There are free VPN services, and my general opinion is that free is worth the price you paid for it: A free service has to pay its bills, which means

it is showing you advertisements, examining your habits to sell for marketing purposes, or otherwise engaged in some kind of "monetizable" behavior. Free services also don't have to make promises about availability or customer service. Do yourself a favor, and pay for a VPN.

Configure a VPN Manually

There are several kinds of VPN protocols, and the OS supports the most popular: IKEv2, L2TP/IPsec (listed as L2TP), and Cisco IPsec (listed as IPsec). The first two are generic, widely used standards. The last is a Cisco VPN flavor proprietary to its systems. Other corporate standards can be provided via VPN apps.

> **Note:** Apple long supported PPTP, but dropped it for security reasons: it's too easily broken and has no advantages over newer VPN flavors.

Almost any server operating system that offers VPN software at all can support one of these protocols, including macOS Server and Microsoft Windows Server.

Set up a VPN profile

Start by making sure you have all the server settings provided by your VPN host or network administrator at hand, since you'll need to enter several pieces of data.

To set up a VPN profile, follow these steps:

1. Launch the Settings app, and tap General > VPN. (If you've configured a VPN before, it may show up in the top level of Settings.)
2. Tap Add VPN Configuration. The Add Configuration view appear.
3. In the Add Configuration view, tap Type if the default IKEv2 isn't what you want. L2TP, PPTP, and IPsec are also available. The choice here affects which options appear for configuration.
4. Then, fill in the settings:
   - The description appears in the VPN view after you create the configuration; enter something short and expository.

- Server (all), and Account and Password (all but IKEv2) tell the OS which Internet host to connect to using which credentials.
- Remote ID is exclusive to IKEv2 and required; Local ID is also part of IKEv2, and required.
- RSA SecurID (L2TP and PPTP) should always be off unless your employer provided you with a physical key fob.
- Secret (L2TP and IPsec) is a shared bit of text that's used as an extra level of security.
- Use Certificate (IPsec only) is enabled when you have a stored certificate to validate your identity.
- User Authentication (IKEv2 only) can be set to Username, in which case Username and Password appear; or to Certificate, and then a certificate needs to be selected.
- Group Name (IPsec only) is set if a network admin provides a group.
- Encryption Level (PPTP only) is typically left set to Auto.
- Send All Traffic (L2TP and PPTP) is typically left on. If it is off, you can filter which traffic is not encrypted and which is.
- A Proxy option can be ignored unless you've been told otherwise.

5. Tap Save.

   You now have a configuration profile that you can use.

Make a VPN Connection

The easiest way to make a VPN connection if you have an app installed is via the app. Launch the app or install its widget via the Today view (swipe right from the home screen, swipe to the bottom, and tap Edit).

To turn a VPN on or off from iOS and iPadOS's controls, go to Settings > VPN. Tap the VPN switch to connect or disconnect with the currently selected profile listed below the switch.

In some cases, you may see VPN Configurations and Personal VPN as separate lists, each of which will have a separate switch for enabling and disabling.

WARNING! *VPNs can be disrupted when you move between networks. If this happens to you, toggle VPN on to off to on to reset the connection.*

You can tell that a VPN connection is active because a VPN indicator appears in the status bar and a status entry appears in the Settings app that reads Connected.

To get more information about the status of your VPN connection, tap the info ⓘ button to the right of the currently active VPN configuration profile in Settings > VPN. This provides a variety of technical details (**Figure 83**). The Server Address field provides a clue to the facility at which your VPN terminates. You can also toggle Connect On Demand in this view.

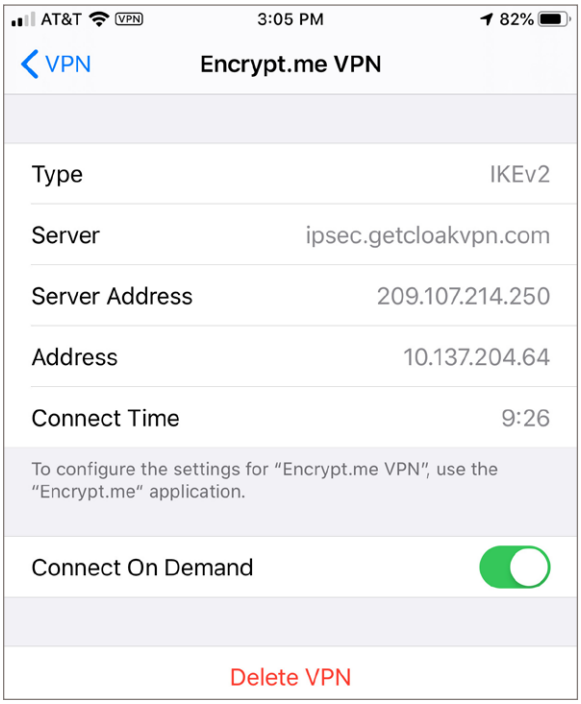

Figure 83: *Connection details reveal where the VPN terminates.*

You can cancel a VPN connection in process (before the connection is completed) by tapping the Cancel VPN Connection button that appears in the VPN view. To turn off a VPN connection, set VPN to off in Settings > VPN; or use the app, when that's an option.

Protect Your Device

Now that you know how to keep your data from being intercepted in transit, how can you prevent your stored data from being rifled if your iPhone or iPad is outside your control?

Apple has three robust ways to secure a device: with a passcode, Touch ID fingerprint-recognition system, and Face ID. All iPhones and iPads that support the latest operating system include either Touch ID or Face ID and associated robust hardware encryption.

When a device is on and locked, its data is inaccessible until a passcode is entered or Touch ID/Face ID accepted, which unlocks the encryption keys needed to read stored information.

WARNING: *If you forget the passcode and Touch ID or Face ID isn't available (such as after a reboot), your data stored only on the device is lost forever. iCloud and other cloud-stored data remains available as long as you have that account information.*

Use a Passcode

Your best single protection against anyone unauthorized having access to data is enabling the passcode lock. This allows you to set a six-digit code required to wake and gain access to the device.

When Touch ID or Face ID are enabled, you must also have a passcode set, and Apple will ask you for that passcode on a regular basis.

Let's start with setting up a strong passcode, and then move on to when you'll be prompted for one.

Set up a Passcode

To set the passcode lock, follow these steps:

1. In Settings, tap Passcode. On Touch ID–equipped devices, the option reads Touch ID & Passcode; with Face ID, Face ID & Passcode.
2. Tap Turn Passcode On.
3. If you want to use the default, a six-digit passcode, tap it in and re-enter it when prompted.

   You can also opt to tap Passcode Options and pick an alphanumeric password of letters, punctuation, and numbers; a custom numeric code; or a four-digit numeric code (**Figure 84**).

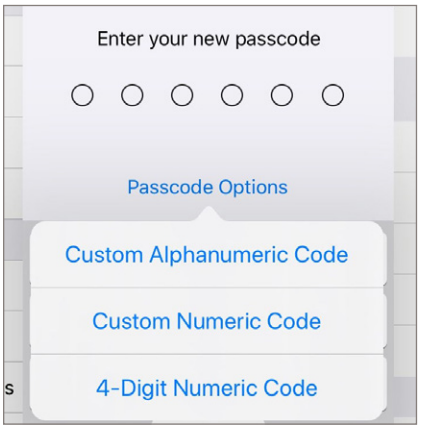

Figure 84: *You can opt for a more complicated or shorter passcode.*

> ***WARNING:*** *Many mobile security gurus say not only is four digits too few to resist cracking, but six isn't enough, either. They recommend picking a memorable short phrase that's easy to enter but impossible to guess. See* ***Create, Manage, and Use Strong Passwords*** *for advice.*

You can also enable the passcode lock remotely if you have an active iCloud account and Find My iPhone enabled on the device. See **When Your Device Goes Missing**, ahead.

The Require Passcode option offers a few choices if you don't enable Touch ID or Face ID, depending on your device:

- With Immediately, you're asked for the passcode whenever the device wakes, the only option for Touch ID and Face ID. (You can set it to sleep automatically, using Settings > Display & Brightness > Auto-Lock.)
- Longer intervals let the device be unlocked without a passcode for up to the time duration you've chosen from the list.

In the Allow Access When Locked section, you can also set which services are available when your device is locked, which is a good way to prevent leakage of information, such as viewing appointments, having access to Siri, or using Messages to reply.

As a nuclear option, you can set your device to self-destruct—destroy its data, at least—if there are more than ten failed attempts to enter the passcode correctly by switching on Erase Data. What do you lose? Only items created since the last backup and sync; see **Erase Device**.

When a Passcode Is Required

Apple wants to make sure that someone can't easily coerce you to unlock your phone with your finger or your face, and that you will remember your passcode by requiring it at frequent-enough intervals it won't disappear from your brain.

You will be prompted to enter the passcode in a number of circumstances:

- After you shut down or restart your device.
- After 48 hours of not using Touch ID or Face ID to unlock. (This counter resets whenever you use your passcode, Touch ID, or Face ID.)
- Once five unsuccessful attempts have been made to unlock your phone or tablet via Touch ID or Face ID.
- If you've put the device into Lost Mode via Find My. (If you didn't set a passcode, you must set one via Find My to enable Lost Mode.)
- As an extra memory aid, you have to unlock your device regularly with your passcode. Apple enforces this by starting an eight-hour timer after it has been six days since you last used the passcode to unlock. During that eight-hour period, if you use Touch ID or Face ID, the timer resets. Once the eight-hour timer runs out, however, you must use your passcode to re-enable Touch ID or Face ID.

Reverting to a Passcode for Safety

There will be times when you will want to revert to a passcode instead of Touch ID or Face ID for personal safety, extra security, or in certain legal situations. In the United States, while the law isn't yet fully established, it appears that in criminal proceedings, the government can compel the use of a fingerprint but can't compel you to give up your password.

If you want to force the OS to disable Touch ID or Face ID, you can:

- In Settings > Touch/Face ID & Passcode, turn off iPhone/iPad Unlock, Apple Pay, iTunes & App Store, and Password AutoFill. You're prompted that Touch ID or Face ID will be disabled.
- Power down your device. On restart, it's disabled.
- Five presses in a row of the Wake/Standby button lets you make an emergency call, but also temporarily disables Touch ID and Face ID until you enter your passcode.
- With all new phones starting in 2017, holding down either volume button and the Wake/Standby button disables Touch ID and Face ID, while bringing up the Slide To Power Down option. On earlier phones, it just brings up the power-down slider.
- Make five bad login attempts with your finger or face.

Use a Biometric Login

Biometrics refers to using some part of yourself that can be uniquely identified to authenticate that you should have access. That includes fingerprints with Touch ID and, with the iPhone X and 11 series and the iPad Pro (2018 models), your face with Face ID. Both methods share a lot in common.

Touch ID and Face ID unlock your phone and also authorize Apple Pay payments, make iTunes purchases, make App Store and in-app purchases, and unlock passwords to auto fill in Safari and in apps. Third parties can also tie into both to unlock themselves or allow a login, such as with banking and password apps.

WARNING: *When using biometric ID, remember that although it increases the relative security of your data while improving the speed and simplicity of use, you also open yourself up to your device being unlocked via coercion. If someone—a government agent, criminal, abusive spouse, etc.—can force your finger onto a Touch ID sensor or force you to look attentively into a device with Face ID, they can gain access to your information.*

Now let's look at how you set up and use both kinds of biometric ID.

Use Touch ID

Apple's Touch ID lets you turn to your fingertips to secure your device, training your iPhone or iPad on equipped models to recognize up to five fingerprints.

You select which of the Touch ID associations you want in Settings > Touch ID & Passcode and then tap Add a Fingerprint. The OS guides you through enrolling a fingerprint. When it's finished, it names the entry Finger plus a number. As this isn't descriptive, tap that entry, then name it with something you remember. In that way, if the OS "forgets" your fingerprint, you can delete the appropriate entry and retrain it.

Touch ID allows fingers from different people, which is convenient, as you and others could all use Touch ID to unlock the same phone or tablet, or you could enroll a partner's fingerprint as an emergency fallback if they need to access your device.

Note: Matthew Green, a well-known security researcher, **tweeted this cautionary tale** in November 2014: "I woke this morning to find my 7 y/o levering my finger onto the Touch ID sensor of my phone. Maybe time to go back to passwords."

Use Face ID

Face ID uses an infrared laser and sensor to project and measure 30,000 separate data points on a person's face to create a profile while also capturing other flat views. Subsequent logins repeat those tasks and add randomization to compare to the stored profile and defeat face forgery.

iPhone and iPads with Face ID can recognize just one face plus an "alternate appearance," or a common secondary appearance of yourself, like with any or different makeup, hat, or glasses.

Tip: Some people use the alternate appearance to add a second person.

Enrollment uses a similar process to Touch ID: You use Settings > Face ID & Passcode, and choose Enroll Face. The process has you move your head in a circle framed onscreen, until enough information has been gathered.

Apple says it tracks and retains temporary updates when it finds a good match that falls outside its ideal parameters. These temporary updates are good for only a "finite" number of unlocks, which is a little vague. Maybe it's to cope with temporary clothing choices or eyebrow plucking? A change in glasses?

Face ID relies on an "attentive" expression when you log in. This prevents unlocking the phone or tablet when you're just glancing past the lock screen, and it requires someone to have their eyes open. Apple says you can unlock wearing sunglasses. The emitters and sensors are designed to be used in all lighting conditions, indoors and outdoors. The alternate appearance helps here, too.

Users report Face ID being delightful, as you merely raise an iPhone or iPad to wake it and while glancing attentively, the device unlocks. It feels seamless. (I haven't purchased a Face ID model two years in!)

With Apple Pay in a store, you have to invoke the Wallet before tapping: Double-click the side button (iPhone) or top button (iPad), glance, and then tap to pay.

Although I recommend setting a strong passcode, you may wind up entering your passcode more frequently with Face ID than with Touch ID for a few reasons:

- Face ID is good but not perfect, especially in situations with bright light.
- Some models of sunglasses and some brands of sunglasses use optical filters that apparently prevent a good or reliable match.

- When the sensors can't perform as exact a match as required, they defer to the passcode. This appears to happen routinely but not constantly.
- You cannot use Face ID to confirm an Ask to Buy request, used for parents or guardians to approve children's purchase requests in the OS. While Touch ID may be used, on Face ID–equipped devices, only a passcode works.

Block Unwanted USB Connections

In early 2018, reports began to surface that an exploit existed in the OS that allowed quick brute force entry and cracking using a Lightning-connected device over USB. With this method, a four-digit passcode could be broken in minutes for common codes to hours for longer ones. Six-digit passcodes are also susceptible, even though it takes much longer to cycle through all possibilities.

This exploit was confirmed later in the year. At least two companies that offer cracking services to governments claim to offer such capabilities. However, any crack can be used for good or for ill.

Apple opted to revamp the USB driver software that manages connections—apparently having discovered flaws within it—as well as to add an option (enabled by default) that locks the USB port for data interactions after one hour.

The feature (which first appeared in iOS 11) can be configured in Settings > Touch ID/Face ID & Passwords: It's labeled USB Accessories. When off, as it is when you upgrade the OS, you must unlock your device if an hour has passed since the last time it was connected for any data-related purpose, like syncing. Charging in most cases should be unaffected.

The notion is that any crack attempt would have to occur within an hour of your last unlock, and without someone compelling you to unlock it.

You can opt to enable it, however, and then the Lightning port is always available.

When Your Device Goes Missing

Your mobile device is a desirable item for thieves. It's compact, it has a high retained value, and there's a huge market for used models.

Without freaking you out about theft, I want to tell you how you can protect your data when your device has disappeared, make it impossible for a thief to use your device, and find your device if it's stolen or lost.

How Find My Works

You can find the last reported position of any iPhone, iPad, or Mac via Find My, which is linked to your iCloud account. You can see the device's location, play a sound on it, lock it or mark it lost, or erase it!

Note: U.S. phone carriers also offer phone-tracking services, which can work across a family account and different smartphones and dumb phones. Each comes with a separate fee and various enhancements and limitations. If everyone in your family is using an iPhone, there may be no advantage.

With Family Sharing turned on, anyone in the group can see where an iOS device is, unless the owner has disabled letting that person or anyone see his or her current location. With that user's password, all Find My features are available through other Family Sharing members' accounts.

Note: Apple combined Find My Friends and Find My iPhone into the single Find My app in iOS 13, iPadOS 13, and macOS 10.15.

How Find My Sends Its Location over Wi-Fi or Cellular

The feature relies on a device sending Apple's servers a regular update of location information derived from Wi-Fi, cellular, and GPS signals and data. All devices that can use Find My (back several years) provide details using Wi-Fi; iPhones and cellular iPads add cellular radios and GPS.

With Find My active, a device with GPS and cellular regularly sends updates over Wi-Fi or cellular networks derived from its GPS receiver and from ranging information it has about nearby cell phone towers that allow it to trilaterate.

> **Note:** You may be more familiar with the term *triangulation*, which relies on using known fixed positions and measuring angles. *Trilateration* uses the intersection of geometric areas, such as the radius of signal strength from cell towers.

However, all iOS and iPadOS (and macOS) devices also scan for nearby Wi-Fi networks and send a snapshot of that information to an online system run by Apple whenever the device has an Internet connection.

Apple integrates that with information fed to it by iPhones and iPads with GPS built in and examines signal strength of Wi-Fi gateways, allowing it to figure out fairly precisely where each is located. (Gateways broadcast a unique hardware network identifier along with a network name, which can be scanned without connecting to a network.)

> **Note:** Apple **caches some information** about location on the phone for up to seven days to avoid frequent network access to look up information, or to use Wi-Fi positioning in an area you've been recently even if you don't have current Internet access.

This is a two-way connection: Through Find My on one of your other devices or via iCloud.com, you can push a sound and message, as well as lock or erase the hardware.

Using Find My also tells your remote devices you're looking for them, and when they receive that message, they update their position more regularly, typically even if they're in a standby mode.

There's a flaw with this finding process, of course: A lookup requires an active connection.

How Find My Discovers Disconnected Devices

What if you've lost your device and it's in a place where it can't reach a Wi-Fi network and either has no active cellular data plan or can't reach a cellular base station? What if it's stolen, and the thief has disabled network access through Control Center?

Apple came up with a fiendishly clever solution for this scenario that relies on Bluetooth. To use this feature, you have to have previously paired at least two of your devices that use the same iCloud account, much like setting up iCloud Keychain.

This pairing exchanges encryption information between your devices without Apple or a third party knowing those secrets or having access to them. That's particularly critical with location-based data.

While Apple hasn't released detailed information about the process, it's possible to infer how it works:

1. Whenever one of your devices can't make a connection to the Internet, it begins to send a Bluetooth beacon that contains an encrypted message.
2. Any Apple device in the vicinity with an Internet connection, owned by anyone and running iOS 13, iPadOS 13, or macOS 10.15, picks up the broadcast and relays it to Apple, appending location information the other person's device has obtained or inferred.
3. Apple stores this information, but doesn't do anything with it.
4. If you mark your device as lost or lock it, any of your existing paired devices can make a very particular sort of query using shared encrypted information to Apple, and Apple provides matching results.
5. Your device then decrypts the data and shows you where it has been spotted.

   It's a beautiful system, in that neither Apple, the owner of other equipment, nor anyone sniffing in the area around your device can determine who owns the hardware or what's in the broadcast.

   This is a one-way system, though: You can't send a lost or locked message to the device, so it can't be locked or erased.

Use Find My for Tracking

Find My requires an active Apple ID associated with iCloud. You likely set up Find My when upgrading or setting up your iPhone, iPad, or Mac. You can also enable finding on a Watch or AirPods.

To enable Find My on an iPhone or iPad device, if you haven't logged in with an Apple ID account yet, go to Settings > *account name* > iCloud and enter your credentials.

Once you're logged in, tap Settings > *account name* > Find My for more actions. This is where you can turn off Find My, but it's also where you can set important finding enhancements:

- Enable Offline Finding uses the crowdsourced mode just described; it's turned on by default.
- Send Last Location ensures that if its battery is nearly depleted, it uploads its last location to Apple, so it can be sent to you.

WARNING: *Apple added a feature a few releases ago called Activation Lock that prevents your iPhone or iPad from being erased and then used by someone else. An erased, locked device requires its passcode to proceed. You can disable this by entering your iCloud password to disable Find My before erasing. However, it obviously also disables tracking. (This feature is also on Macs with Touch ID.)*

Note: To enable Find My in macOS, enable the Find My checkbox in the Apple ID preference pane in iCloud settings. If your Mac has Wi-Fi turned off with an active Internet connection (such as cabled Ethernet), it can still be contacted to perform actions, but it may not display a location. Click the Options button to modify Offline Finding.

View Your Device's Location

To view your device's location, you can choose between two similar tools: the Find My web app at iCloud.com or the Find My app on an iPhone or iPad (or in macOS). The two options have similar interfaces and nearly identical features.

Lost a second factor, too? *Apple lets you use Find My with an account with two-factor authentication enabled even if you can't access a second factor to log in—say, all your devices were stolen! At iCloud.com, after entering your account name and password, you'll see Find My as an option below the area to enter a six-digit 2FA code. This is also a security loophole, as I describe later in this chapter.*

Find My app

The preferred way to use Find My starting in iOS 13, iPadOS 13, and macOS 10.15 is via the Find My app, which is included with every device. By activating Find My, you're also automatically logged into the app on all those operating systems, too.

Tap Devices, and the default view shows all your hardware in a list at the bottom of the screen and plots their locations in a map shrunk to fit them all (**Figure 85**). Each device appears as an icon of its exact model. Your location is also plotted on the map as a blue dot if you're near or between any of your devices, as is likely.

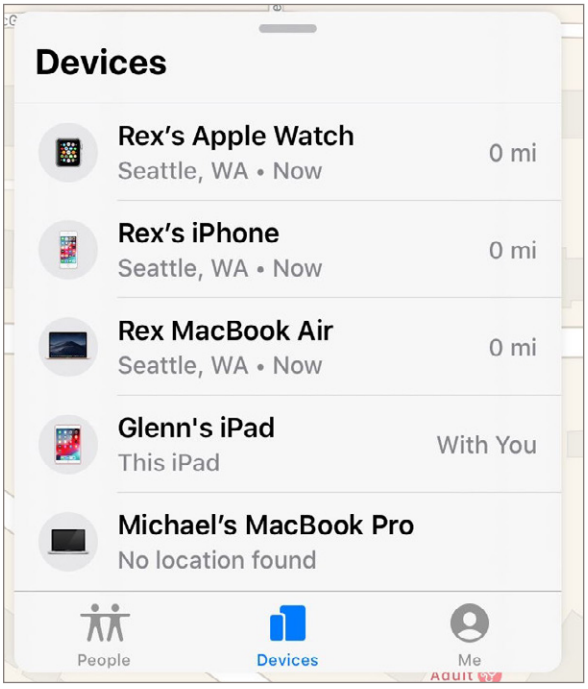

Figure 85: *The Find My app shows all your connected devices in a list.*

The screen has typical map actions, like an info ⓘ button to switch units and views. You can zoom, rotate, and move between 2D and relief views.

Tap a device in the list and it's selected and centered on in the map, and an actions sheet appears at the bottom of the screen (**Figure 86**). Tap the X close button at the upper-right corner to return to the full device list.

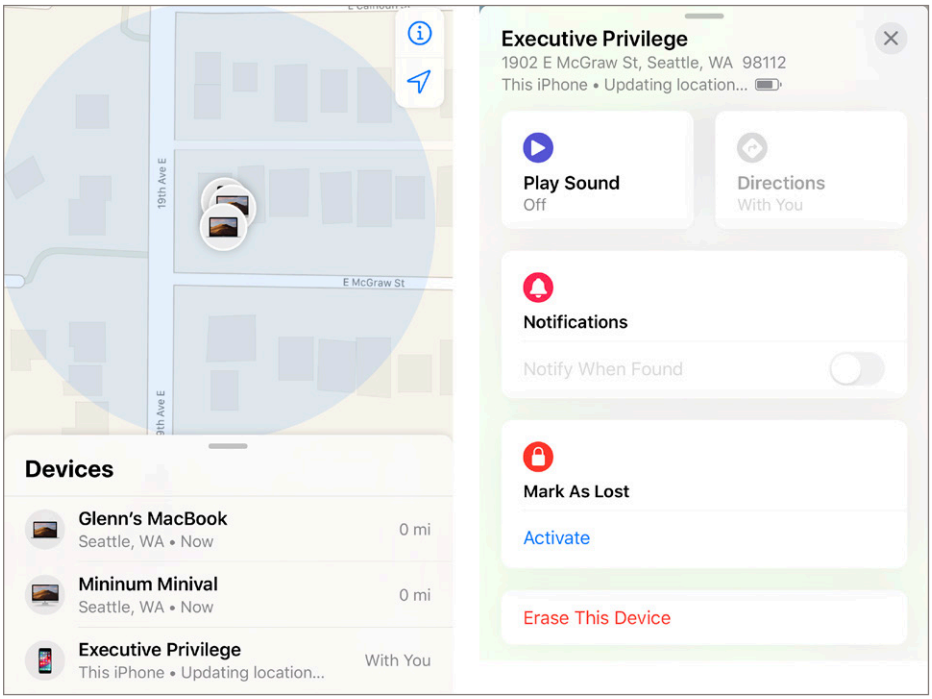

Figure 86: *Devices are shown plotted on a map (left); tap any device and an actions sheets gives you options (right).*

Find My shows the location of the device on the map as a tiny dot with its model avatar hovering above it. The dot is the center of a blue shaded area if a device can be pinpointed; the shaded region is larger and shows as green otherwise. The radius of shaded area indicates the amount of confidence in the location.

With AirPods, they also have to be out of their case and near any of your iOS devices, and show the location of only one of the earbuds at a time. A device offline for more than 24 hours displays as No Location Found. It may take Find My up to 3 minutes to fix a precise location for a device.

Find Me may list an exact street address beneath the device's name. It also tells you how recently the location information was updated (how long ago, "Now," or "Updating Location"), and displays a nifty battery indicator—handy for knowing how much juice is left on a lost device!

> ***WARNING!*** *If you know your device was stolen, take the location information to the police before trying to entice the thief to give it up.*

Find My on the web

You can also use the Find My web app, which is both an alternate to the app and the only way for someone without one of their other devices to log in and track their devices.

> **Note:** As I finish this edition of the book, the Find My section of iCloud looks outdated compared to the new Find My apps—it's even still named Find My iPhone. It's possible it will change, and I'll update the book later to reflect that if so.

Follow these steps:

1. Go to **https://icloud.com/#find**.
2. Log in with the correct Apple ID.
3. Select one of your devices from the All Devices menu (**Figure 87**).

> **Note:** iCloud.com allows you to stay logged in, but prevents unauthorized access to Find My by asking for a password even when you're already logged in to another part of the site. The Find My login times out after 15 minutes.

In the All Devices list, the dot beside each device name indicates the status: Gray ● means trying to connect or offline. A green ● means online, and it shows the last time it was located. Each device appears as a small green circle on the map. Devices that can't be found are marked Offline.

To select a device, either have All Devices selected and choose a device, or click any green dot on the map. A popover menu appears with options for actions, described just ahead, and the last time a fix was made on device's location.

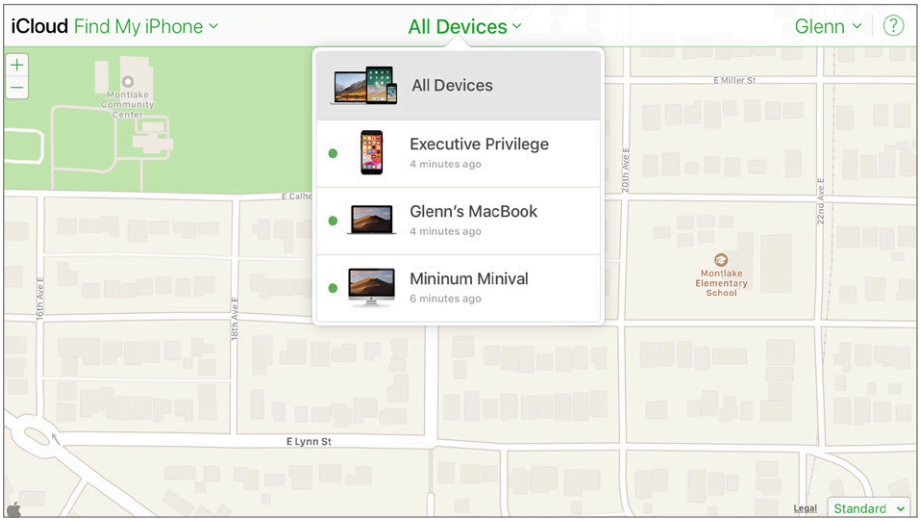

Figure 87: *The Find My iPhone web app shows devices in a drop-down list at center and their locations on a map.*

Take Remote Action

You can now take action on your remote device, with several options that vary in utility based on whether your device has fallen behind a couch cushion, or has been misplaced or stolen. Whatever action you take, iCloud sends an email message to your Apple ID address.

> **Note:** Pick any of the following actions when a device is shown as offline, and iCloud triggers that action when it comes back online and it still has Find My active. If the trigger executes, you get an email message.

Notification and Driving Directions

For any device that can't currently be located, you can enable the Notify When Found button and be alerted via email when it comes back on the radar. (In Find My for the web, the label is Notify Me When Found.)

Tap Directions, and the OS opens the Maps app in directions mode with the device's current location as the destination.

Play Sound

When you can't find a device but think it may be nearby, the Play Sound option should help you locate it. Tap or click Play Sound, and for two minutes either a loud pinging noise will play (if sound is active) or the device will vibrate (if muted).

If it's unlocked, a notification appears that reads "Find My *Device* Alert" (**Figure 88**). If an iPhone or iPad is locked, it has to be unlocked to disable the ping or vibration. On a Mac, the dialog can be dismissed at a login screen.

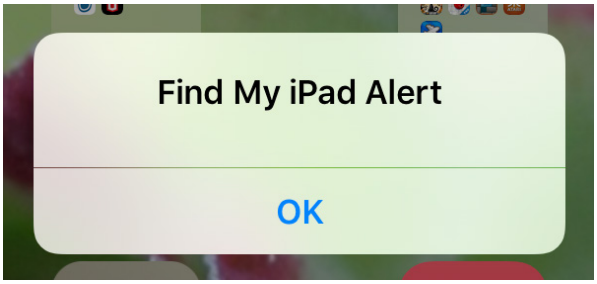

Figure 88: *iOS shows this message when Play Sound is triggered.*

Mark as Lost

This option helps you recover a lost or stolen device. You can offer a reward and provide your phone number. It also puts the finder on notice that you know approximately where it is. ("I'm a block away. There's a reward.") Were your hardware stolen, this is a way to tell a thief that you have her location and other data, and advise her to give it up.

> **Note:** At iCloud.com, the Find My service calls it Lost Mode for all devices except Macs, where it uses the Lock label.

This Lost Mode option has up to four steps:

1. After tapping or clicking Mark As Lost, you have to confirm by tapping Continue for an iPhone, iPad, or Watch, or Lock This Mac for macOS (**Figure 89**). (Click Cancel to back out.)

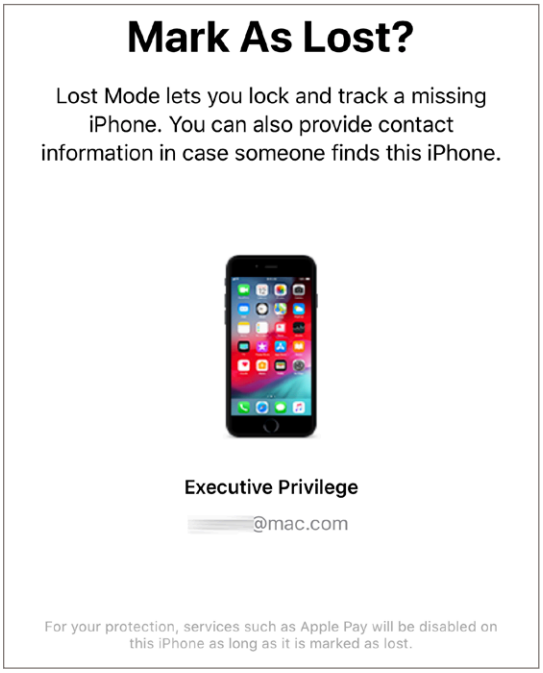

Figure 89: *Marking an item as lost lets you keep tracking it and add info.*

2. If a device doesn't have a passcode set—as unlikely as that seems—you are prompted to enter and verify a passcode.
3. Optionally, set a phone number for a call back (**Figure 90**). On an iPhone, the phone may be used to call *only* that number. On other devices, the call-back number is displayed but can't be used.

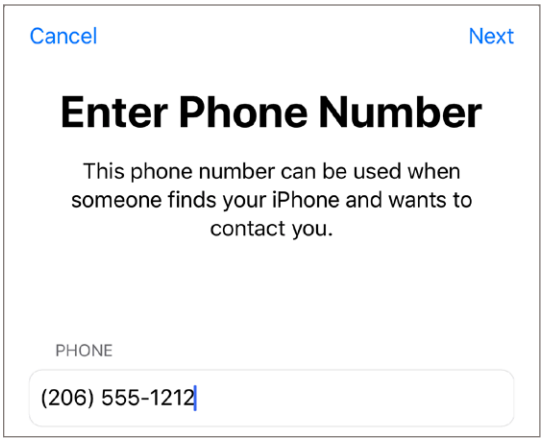

Figure 90: *You can opt to enter a call-back number.*

4. Optionally, enter a message to appear on the device (**Figure 91**). In this step, the dialog shows that a passcode has already been set and will be used to lock the device.

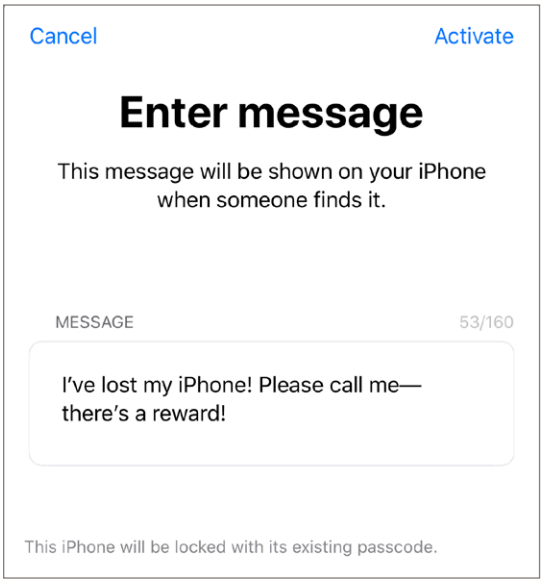

Figure 91: *Choose to add a message.*

After you activate Mark as Lost, the action is passed to the device if it's online, and an email message is sent to the address for the Apple ID account for the device, confirming what you've done.

How Mark as Lost works with an iPhone or iPad

Once the action is sent to an iPhone or iPad:

- If the device is connected to the Internet and asleep, the next time it's woken, a passcode must be entered to gain access.
- If the device is online and in use, the OS drops the user into the Lock screen where the passcode-entry dialog or keypad is shown (**Figure 92**).
- If the device is offline, the next time it accesses any network with an Internet connection, the passcode lock is put into place.

> **Note:** Mark as Lost immediately disables Apple's side of Apple Pay for a lost device. Thus, if you mark your device as lost, Apple will not approve even an offline transaction made by someone who has the device passcode!

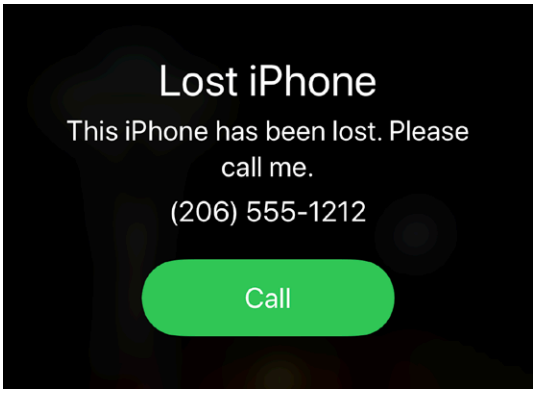

Figure 92: *On your phone marked as lost, an optional message and phone number appears, along with the ability for the finder to call you at the number you set.*

Mark as Lost also enables tracking the next time the device is online. A tracked path appears in a map as a dotted red line. This lets you see wherever a device has gone—so long as it remains online. Even neater, if Location Services has been turned off, Mark as Lost re-enables it so you can track your device.

If you recover your iPhone or iPad, enter its passcode—Touch ID and Face ID are disabled. You're also prompted to enter your iCloud password; once entered, that reactivates all your stored Apple Pay cards. (You'll also get a slew of notifications, one for each card!)

How Mark as Lost works with a Mac

Mark as Lost works differently with a Mac. When you mark a Mac lost, you set a six-digit code that can be used to unlock it. That code is then entered at the unlock screen (**Figure 93**).

Instead of just performing the equivalent of Lock Screen on a Mac, which would require a password to regain access, Mark as Lost—still labeled at iCloud.com's Find My as "Lock"—locks a Mac. It freezes the interface, shuts it down invisibly, then restarts it using the Recovery partition into a special locked mode.

Note: I realize this book is about iPhones and iPads, but since you can lock your Mac from one of those devices, I feel compelled to tell you how to unlock it, too!

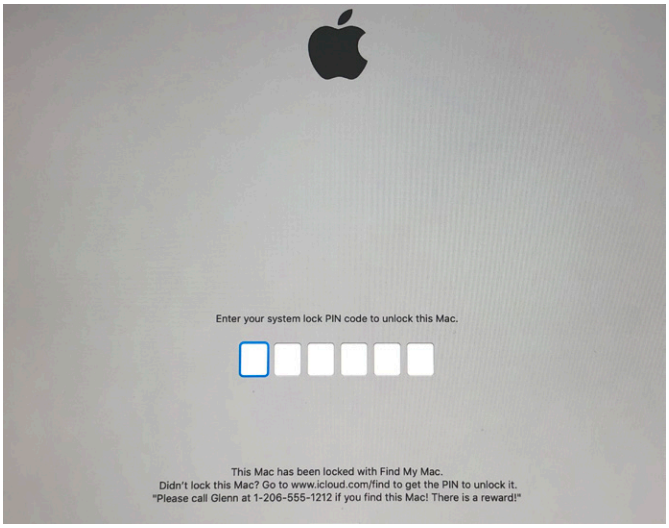

Figure 93: *A Mac reboots into a special locked mode.*

If someone manages to steal or figure out your iCloud account, even with 2FA enabled, they can lock your Mac with a code you don't have. However, you can log into your iCloud account and retrieve the code. Then change your password!

Erase This Device

The last resort in some cases (or first in others) is a remote wipe, in which all the user data on the iOS device is erased.

An erased device that has Find My enabled before erasure and remains associated with an Apple ID cannot be unlocked without the account password due to the Activation Lock feature mentioned earlier.

The erase option lets you provide a phone number and message so that a person who found (or stole) your device can get in touch. The iOS device is essentially useless to them without the password.

WARNING! *After erasing a device, Find My can't update its location.*

Note: You can remove a device from your Find My list after erasing it by following Apple's instructions **in a support note**.

It's a multi-step process to prevent accidental erasure:

1. In the web app or the iOS app, tap Erase This Device (or Erase *Device* at iCloud.com).
2. You're warned that everything is about to be erased. Tap or click Erase This *Device*, but there are more steps ahead (**Figure 94**).

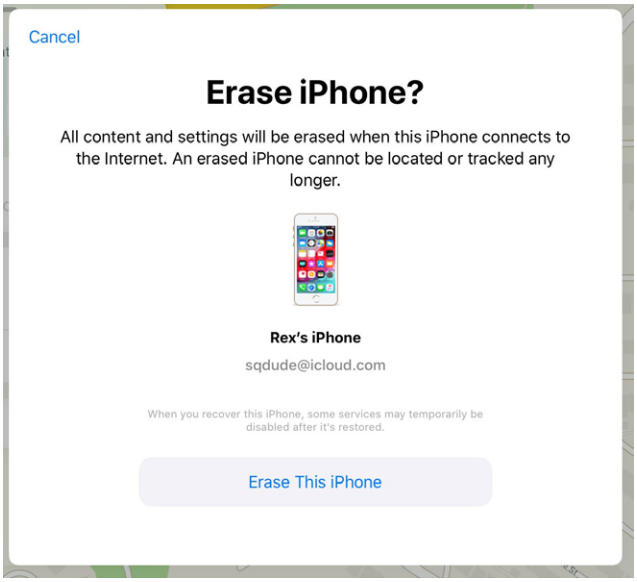

Figure 94: *This step seems like you're about to erase your device immediately, but there are more steps ahead.*

3. Enter a phone number at which you can be reached after it's erased, and tap Next.
4. Enter a message you want to appear along with the phone number. You'll notice there's a Done button.
5. Tap Erase. (If you're using **two-factor authentication**, the device is removed from your set of trusted devices.)
6. Enter your Apple ID password. (If this is another member's device, accessible via Family Sharing, enter her or his Apple ID password.) Tap that, and the remote device is erased—there's no going back!

   If the device is online, the Erase action immediately wipes all your data off it. If it's offline, the erase begins as soon as it next comes online through any networking method.

The erasure happens quickly. To "erase" stored data, an encryption key that protects your device at a hardware level is thrown away and a few other settings rewritten. Everything is now completely unrecoverable.

Note: Macs with FileVault enabled in the Security & Privacy preference pane similarly have their boot drives rendered unreadable. (The drive can still be erased and a new system installed, however.)

However, wiping your device isn't as bad for your data as it sounds. All iOS and iPadOS devices are set by default to back up the unique data that's stored on them, like settings, passwords, and documents created by or associated with apps. These backups can be either local to a Mac on a particular computer or remote to iCloud.

Apps are stored centrally, not in a backup, and restored from Apple's servers; the same is true with books, purchased music, and purchased movies and TV programs. If you use iCloud Photos and iCloud Music Library, that media is stored in the cloud and synced. (If you're not using either, it's likely you are syncing music with a Mac or Windows system. This is a good time to check that you're up to date with syncing.)

If you erase your device, and then either recover it or obtain a new device, you can restore from your most recent backup. If you were syncing any items to your device through Photos, Music, or other apps or tools in macOS, you can then sync them back to the device. For items stored in iCloud, the restore process downloads them again.

Tip: You can accelerate restoring by placing one iOS device near another. Your device being restored can pick up your settings from the other using a feature called Direct Transfer. It locks both devices while the transfer is underway, however.

If any unique data was syncing from your iPad or iPhone to iCloud, Dropbox, Exchange, or another service, you likely won't have lost any of that data up to the moment the device was lost or disconnected from a cellular or Wi-Fi network. You will lose any changes made on the device between the last sync (push, fetch, or manual) for each account and the remote wipe.

Update History

version 1.0 (September 19, 2019)

Initial release for iOS 13.0.

version 1.0.1 (September 20, 2019)

Bug fixes. Added details about Sign In with Apple and controlling sharing location when sharing photos.

version 1.0.2 (September 24, 2019)

Minor changes to update for iOS 13.1 and the release of iPadOS 13.1. Expanded information about joining a Wi-Fi network via the Control Center's networking area and by sharing a password with someone in your contacts who is nearby. Expanded details about photo and Bluetooth/iBeacon sharing.

version 1.0.3 (September 26, 2019)

Late changes in iOS 13.1 and iPadOS 13.1 led me to overhaul the Personal Hotspot chapter to better reflect how Apple now conceives of the feature.

Acknowledgments

I dedicate this book as always to my wife, Lynn, and kids, Ben and Rex. On this journey through life, we are trying our best every day. They ground me and remind me to leave the house at times.

Thanks to Jeff Carlson for technical editing and proofreading on this edition, and Charles Fleishman, Scout Festa, and Jeff for their varied editing assistance across several editions!

Thanks to Joe Kissell, publisher of the Take Control books series, for his interest and support in distributing this independently produced book.

About the Author

Glenn Fleishman was trained as a typesetter, received a degree in art, and works as a journalist, type historian, and programmer. Glenn appears regularly in Macworld, *Increment*, TidBITS, *Fast Company*, and other publications where he writes about security, copyright, punctuation conventions, printing history, and much more.

He spent 2017 as the Designer in Residence at the School of Visual Concepts in Seattle, printing his book *Not To Put Too Fine a Point on It*. In 2018, he released the book *London Kerning*, about typographic museums and memory in that city. In 2019, he launched the Tiny Type Museum & Time Capsule, a project to build 100 tiny museums full of printing artifacts. In October 2012, he appeared on the *Jeopardy!* quiz show and managed to win—twice!

His blog is **glog.glennf.com**, and he overshares on Twitter at **@glennf**.

Copyright and Fine Print

Connect and Secure Your iPhone and iPad
Covers iOS 13.1 and iPadOS 13.1

ISBN 978-0-9994897-9-6 (ebook) / 978-1-7334954-0-0 (print)
Aperiodical LLC, 1904 E. McGraw St., Seattle, WA 98112-2629 USA

http://glennf.com/guides