Click here to buy the full 254-page “Take Control of iOS & iPadOS Privacy and Security” for only $14.99!
# Table of Contents

**Read Me First** .......................................................... 5  
  What’s New in This Book .................................................. 5  
  Updates and More ........................................................... 7  

**Introduction** .................................................................. 8  

**Connect and Secure Quick Start** ...................................... 9  

**Connect to a Wi-Fi Network** ........................................... 11  
  Join a Network .................................................................. 11  
  Manage Wi-Fi Connections ................................................. 14  
  Drill Down to Network Details ............................................ 17  
  Turn Wi-Fi Off .................................................................. 23  
  Capture the Page ............................................................. 23  

**Troubleshoot Wi-Fi** .......................................................... 26  
  Correct Password Not Accepted ........................................... 28  
  No Internet Service after Connecting .................................. 28  

**Make a Mobile Hotspot** .................................................. 31  
  Work with Personal Hotspot Settings .................................... 31  
  Other Ways To Connect .................................................... 39  

**Choose Between Cellular Data and Wi-Fi** ......................... 51  
  Which Network Are You On? .............................................. 51  
  Select Which Service to Use ............................................. 52  

**Manage Cell Data Usage** ................................................ 55  
  Carriers Shift to Throttling ................................................ 55  
  Keep Usage Restrained .................................................... 57  

**Place Calls via Wi-Fi** ....................................................... 66  
  Enable Wi-Fi Calling on Your iPhone .................................... 66  
  Enable Wi-Fi Calling on Other Devices .................................. 70  

**Manage Airplane Mode** .................................................. 73  
  What’s Airplane Mode? .................................................... 73  
  When Radios Turn Off ..................................................... 75

Click here to buy the full 254-page “Take Control of iOS & iPadOS Privacy and Security” for only $14.99!
Welcome to *Take Control of iOS & iPadOS Privacy and Security*, version 1.0, published in September 2020 by alt concepts inc. This book was written by Glenn Fleishman and edited by Joe Kissell.

This book describes how to securely use your iPhone and iPod touch with iOS 14 and iPad with iPadOS 14 on Wi-Fi and cellular/mobile networks, making connections with ease while protecting your data and your privacy.

If you want to share this ebook with a friend, we ask that you do so as you would with a physical book: “lend” it for a quick look, but ask your friend to buy a copy for careful reading or reference. Discounted classroom and user group copies are available.

Copyright © 2020, Glenn Fleishman. All rights reserved.

What’s New in This Book

This book has had many lives, starting a decade ago. It was part of the Take Control series when the iPad was first released in 2010 as *Take Control of iPad Networking & Security*, and it then merged with the iPhone as *Take Control of iOS Networking & Security*. After a few updates, with a crush of other books to produce, the publishers agreed to let me release the book under my own imprint, while they offered it for sale to Take Control buyers.

Across six editions as *A Practical Guide to Networking & Security*, then as *A Practical Guide to Networking, Privacy, & Security*, and finally as *Connect & Secure Your iPhone & iPad*, I have continued to expand and update the title to encompass more concerns, reader feedback, and Apple and other companies’ ongoing changes.

With privacy and security foremost these days—including around COVID-19 tracing—and most of my readers part of the Take Control
family already, Joe Kissell agreed to bring this book back with its sixth name into the Take Control family as *Take Control of iOS & iPadOS Privacy and Security*.

If you purchased any previous incarnation of this title, you will be familiar with some of the contents of the book, but it’s thoroughly updated for iOS 14 and iPadOS 14. In particular, the following updates were made to reflect changes in the operating systems:

- **Wi-Fi private addresses**: iOS/iPadOS by default generates a unique identifier for the Wi-Fi radio in your device for each network you join. This deters tracking your device over different networks. See [Wi-Fi Private Addresses](#).

- **Apple fully blocks third-party cookies**: Browser tracking for advertising, marketing, and other purposes that rely on embedding cookies from other sites is now fully blocked. See [Safari Blocks Cookies](#).

- **Safari privacy report**: Safari in iOS/iPadOS (and newer versions of Safari for macOS) can produce a report of all the tracking attempts blocked on a page you’re visiting. See [See a Privacy Report in Safari](#).

- **Safari password warning**: Safari uses a secure method to check whether a password you’re entering on a webpage has been found in any previous password breach, and warns you of that. See [Examine Security Recommendations](#).

- **COVID-19 tracing**: Apple and Google built a privacy-respecting framework for tracking potential novel coronavirus points of contact between people. I added a chapter to explain the intricacies of the two companies’ joint approach, and how to understand your privacy risks, in [COVID-19 Tracing Preserves Privacy](#).

- **WebAuthn support with Secure Enclave**: Apple has continued to expand support for a highly secure second-factor system that has broad industry adoption, called Web Authentication or WebAuthn. It’s now integrated with the Secure Enclave coprocessor in iPhones and iPads. See [A Secure Second Factor for the Web](#).
• **App Store privacy:** Apps will soon be required to spell out how they manage your privacy, which are explained in their App Store listings. See Apps Disclose Much More about Data Usage.

• **Obtain tracking permission:** Starting in early 2021, apps will also have to obtain your permission to use an advertising identifier and other tracking methods. See Users Control Advertiser ID Linkage

• **Location fuzziness:** You no longer have to share your precise location with apps that only need an approximate location. This can reduce ad networks and other organizations’ ability to aggregate information across apps to identify and track you. See Mediate Location Access.

---

**Updates and More**

You can access extras related to this ebook on the web (use the link in *Ebook Extras*, near the end; it’s available only to purchasers). On the ebook’s Take Control Extras page, you can:

• Download any available new version of the ebook for free, or buy any subsequent edition at a discount.

• Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our *Device Advice* page.)

• Read the ebook’s blog. You may find new tips or information, as well as a link to an author interview.

If you bought this ebook from the Take Control website, it has been added to your account, where you can download it in other formats and access any future updates.
Networking should be simple, privacy a human right, and security automatically configured to our best advantage. Apple tries very hard at all three of those; they often succeed, but not always.

This book helps you understand networking, privacy, and security as they relate to connecting and securing an iPhone, iPad, or iPod touch: I teach you everything you need to know to make the best use of the tools, defaults, and options that Apple provides, while filling in the spots that they haven’t addressed.

Apple’s approach isn’t perfect, and they sometimes offer confusingly worded messages that you have to decipher on your own. I walk through what those mean—such as why you’re asked to enter the password of a Mac to unlock iCloud Keychain on a new iPhone you’re setting up. I also provide workarounds and alternatives where Apple doesn’t rise fully to the task.

In the first part of the book, starting with Connect to a Wi-Fi Network, you’ll learn how to work with the three types of mobile wireless communication—Wi-Fi, cellular, and Bluetooth—for general data connectivity, for placing voice calls, and to enable a personal hotspot. I dig into Airplane Mode, AirDrop, and AirPlay as well.

The second part begins with Control Privacy Leaks, and I explain 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 final section, which commences at Create, Manage, and Use Strong Passwords, encompasses all manner of security issues, including passwords, two-factor authentication with your Apple ID, protecting your device, and dealing with when it goes missing—or is stolen.

Click here to buy the full 254-page “Take Control of iOS & iPadOS Privacy and Security” for only $14.99!
This book divides naturally into three parts: networking, privacy, and security, and chapters are organized sequentially in that fashion. You can also dive into particular topics across the book if you want to jump right into particular topics of interest.

**Connect your device:**
- Manage the details of a Wi-Fi network and work through problems; see Connect to a Wi-Fi Network and Troubleshoot Wi-Fi.
- Tether your devices to a hotspot; see Make a Mobile Hotspot.
- Work with the cellular network for data and calls while managing usage; see Choose Between Cellular Data and Wi-Fi, Manage Cell Data Usage, and Place Calls via Wi-Fi.
- Conquer Bluetooth’s peculiarities; see Set Up Bluetooth.
- Dig into Apple’s particular network transfer and streaming protocols; Pass Files with AirDrop and Stream via AirPlay.

**Understand and control privacy:**
- Learn how your privacy could be sacrificed; see Control Privacy Leaks.
- Understand Apple (and Google’s) COVID-19 tracing framework; see COVID-19 Tracing Preserves Privacy.
- Get into Safari’s many ways to block ad tracking, and how you can do even more; see Apple Blocks Tracking in Safari.
- Manage your overall device privacy; Control System Privacy.
Prevent intrusions and hijacking with good choices:
• Make good password choices; see Create, Manage, and Use Strong Passwords.
• Set up two-factor authentication and work through any problems; Use Two-Factor Authentication.
• Use a VPN for umbrella coverage; Connect with a VPN.
• Keep your device inaccessible to others; Protect Your Device.
• Find your iPhone, iPad, or Mac if it’s lost or stolen; When Your Device Goes Missing.
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:

1. Swipe to reveal the Control Center—swipe up from the bottom of the screen on iPhones with a Home button or swipe down from the upper-right corner on all iPads and all other iPhones.

2. Touch and hold the network area.

3. Touch and hold the Wi-Fi icon.

4. Tap a network in the list that appears (Figure 1). You join the network immediately if there’s no password.
Figure 1: Touch and hold the Wi-Fi icon in the Control Center’s expanded network area to bring up a list of Wi-Fi networks to join.

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

5. A password-protected network asks you to enter that password. Enter the password and tap Join, and you’re connected.

Note: For more on connecting with a password or other methods, see Connect to a Secure Wi-Fi Network.

Note: In rare cases, a network’s name may be hidden and you need to enter its name. See Too Many Wi-Fi Networks for details on using the Settings > Wi-Fi > Other option.

If you don’t have a network’s password and you’re near someone you know who has previously logged in, note what the Enter Password dialog states (Figure 2). You can bring your iPhone near any iPhone,
Troubleshoot Wi-Fi

You may at times be unable to get a Wi-Fi connection to the internet. Here is troubleshooting advice for common cases.

Can’t See Any 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:

- **Wi-Fi disabled:** Swipe to reveal the Control Center, and touch and hold the network panel. Make sure the label beneath Wi-Fi is set to On. Alternatively, go to Settings > Wi-Fi and ensure the Wi-Fi switch is enabled.

- **Wrong network:** You may be connected to the wrong network. Go to Settings > Wi-Fi to see which network you’re connected to. Alternatively, reveal the network panel in Control Center to see the name below the Wi-Fi icon.

- **Range:** It’s possible that you are out of range of any network. 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.

- **Router:** The router may be at fault. Check with others around you, if possible, to see if the network is visible or usable by them.

- **Mobile device hardware failure:** I have seen cases in which the Wi-Fi radio in an iPhone or iPad fails, requiring replacement.

No Wi-Fi Signal Strength in the Indicator

You’ve joined a network, but the signal-strength indicator in the upper left still shows gray radio waves instead of black. This means that an
initial connection was made, but then you quickly moved too far away from the base station, or the base station was shut down or restarted with a new name or password. (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: hold the side or top 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. Go to Settings > Wi-Fi and slide down until you can tap the Other button (Figure 8). Enter the network name exactly—near misses don’t work.

![Figure 8: The Other Network option lets you type in a network name and enter a password if required.](Image)

Click here to buy the full 254-page “Take Control of iOS & iPadOS Privacy and Security” for only $14.99!
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 is Apple’s name for the feature that 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 since iOS 13.1 and iPadOS 13.1.
A Personal Hotspot has become something that any device logged in to 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 Low Data Mode for their connections to the hotspot Wi-Fi network in Settings > Wi-Fi > network name. You have to be connected to change the Low Data Mode setting. (See Low Data Mode for more details.)

macOS doesn’t 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. The label “Discoverable” appears only in the Control Center if you hold on the network area to reveal the Personal Hotspot button (Figure 9). In Settings, no label appears in this state! Yes, it’s very consistent.
Choose Between Cellular Data and 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 currently on and set the type of network to which your device connects. And you can even enable a hybrid mode to tap into cellular data when Wi-Fi is flaky.

Which Network Are You On?

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

- **Wi-Fi:** 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 iPhone 11 Pro or later and the newest Wi-Fi 6 gateways.

- **Wi-Fi (in text):** Wi-Fi Calling is enabled; see Place Calls via Wi-Fi for an explanation of that option. It’s a strange choice to use the Wi-Fi label just for calling, but there you go.
• **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 become much faster 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 if 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 choose among networks, 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.
Manage Cell Data Usage

When Apple introduced the iPhone, they convinced its first carrier, Cingular (subsequently bought by AT&T), and then other carriers to offer unlimited data plans in the United States 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 swung way back. 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 in many countries have largely disappeared. In the European Union, you can even roam among the member nations at no expense or little expense, depending on your domestic plan.

Carriers Shift to Throttling

All three major U.S. cellular carriers removed overage fees a couple of years ago and more recently switched to what are semi-accurately described as “unlimited” plans, in that there is no hard limit at which data is throttled. (Sprint was acquired by T-Mobile, and it no longer offers new Sprint plans.)

In these unlimited plans above a base tier, each line gets 50 GB or more a month of prioritized data. The entry-level tier and lines that exceed their monthly priority are then subject to congestion-based availability. If you’re in an area with heavy usage by other customers of the carrier, their throughput needs are handled first. This means you can get anything from modest to perfectly normal performance; there’s no guarantee, however.
Carriers also used to allow either no hotspot usage on a plan or as much as your plan limit. With these no-cap plans, carriers now have per-line hotspot restrictions, too.

**Note:** Carriers also restrict video streaming and other high-data-usage services based on service level. Some plans only include 480p video, no matter how much other data you’re consuming. Carriers use various techniques, including detecting video streams and throttling their bandwidth, even with secured connections that don’t let them snoop on what the content or service is.

Here’s how the carriers provide data service along with hotspot data, including an older, limited plan AT&T still offers:

- **AT&T (limited):** AT&T is the only remaining carrier with a shared data plan in which all lines and hotspots on the plan draw from the same monthly pool of either 3 GB or 9 GB at 4G speeds. After that, all lines are throttled to 128 Kbps.

- **AT&T (unlimited):** AT&T has three tiers of plans: the lowest is always congestion throttled and has no hotspot access; each line on the middle gets 50 GB of priority data and 15 GB of 4G hotspot data; and the top, 100 GB of priority data and 30 GB of hotspot data. On those two top plans, hotspots are slowed to 128 Kbps after a line exhausts its allocation.

- **T-Mobile:** T-Mobile offers 50 GB of priority data per line on its two higher-tier plans, and only congestion-based access on its lowest-tier plan. The three plans all include unlimited hotspot access: the lowest-end is always at 3G rates; the middle includes 3 GB of 4G per line; the highest-tier plan includes 15 GB of 4G per line.

- **Verizon:** Verizon has a matrix of five plans. The lowest-tier and a kids’ oriented plan is always congestion priced with no hotspot service (the kids plan is capped at 5 Mbps), while three plans include 50 GB of priority data per line and unlimited hotspot access (15 GB or 30 GB per line, then throttled to 600 Kbps).
Cellular phone calls are just data. The stream of audio data that comprises 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 don’t charge extra for it; in fact, it saves them money.

**Note:** All 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 both HD Voice (high-quality cellular voice compression) and Voice over LTE (VoLTE), which is a method of routing voice calls over LTE mobile networks. I discuss both in Use Cellular Data while Talking.

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 iPhone

To enable Wi-Fi calling, start in Settings > Phone > Wi-Fi Calling (Figure 29) on your iPhone. Once you tap the switch, you’re prompted to enable Wi-Fi Calling.
Figure 29: 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, 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 30).
Manage 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 United States 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 as required during some stages of flight or for the entirety of some flights, depending on the airline, region, and other rules.

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.
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 button—the operating system turns off three separate radio systems on an iPhone, cellular iPad, or 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**

At one time, 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 side or top button on your device to put it to sleep, you might think it stops doing everything. 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 operating system 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.
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.

**Note:** Bluetooth can provide internet service by connecting an iPhone or iPad to another piece of hardware, such as an iPhone with Personal Hotspot enabled, a laptop, or a cellular router with Bluetooth as an option. See 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.

**Note:** Apple has some additional wireless technology it builds in to its AirPods and AirPods Pro, among other devices, that lets them connect to Apple equipment more quickly and simply than with the standard Bluetooth connection. However, the earbuds work with other hardware and use standard Bluetooth for audio streaming.
Bluetooth is handled from 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 Access via iCloud Devices).

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. Go to 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.
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 39).

![Figure 39: Control Center is where you set AirDrop access.](image)

To enable AirDrop, follow this sequence:

1. Touch and hold the networking panel, which displays the AirDrop icon and its status at bottom left (cellular devices) or upper right (Wi-Fi iPad).
2. Tap the AirDrop button.
3. Tap one of the options (Figure 40):
   - 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 40:** Pick how AirDrop advertises itself on a network.

**Warning!** A number of 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 except at times you need to change it momentarily to receive an item from someone not in your contacts.

Regardless of this setting, anyone who has your iCloud account email address in their contacts will appear for you in the latest operating system 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 41).
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 operating systems 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 47).
Figure 47: Available AirPlay destinations are identified by type.

Your device is shown at the top with a checkmark. Other items appear with various icons or options:

- Bluetooth audio devices appear with an audio Bluetooth $\mathcal{B}$ icon.
- Other audio-capable devices are shown with a stereo speaker $\mathcal{S}$ icon.
- Video-capable devices are shown with an Apple TV $\mathcal{TV}$ 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 tap to add them, instead of switching to them.

4. If the operating system is currently playing media, you should see a play/pause button you can tap to return to the playback view.
Control 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 operating system, 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 operating system 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 website.** 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. This might include a stream of location data, identifying exactly or roughly where you were and at what time.

• **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 often diffuse storage within a data center, among servers across a country, and spanning 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 Apple. Almost all of the following requires permission from a user (discussed in *Apple Blocks Tracking in Safari*), unless a malicious app was installed, which is unlikely.
It’s no surprise to you reading this book that a pandemic occurred starting in early 2020. Along with the death and morbidity experienced by millions worldwide, the economic and academic disruption, and policy uncertainties, it also caused many people to consider the privacy implications of government tracing of people who were in contact or proximity with those later diagnosed with an infection.

Because SARS-CoV-2—the virus’s official name—has an asymptomatic early contagious period and many people remain infectious without having full-blown COVID-19 consequences, millions of people have had inadvertent points of contact with the virus.

Early efforts at tracing involved people having to leave their contact information whenever they walked into a restaurant or other space, or had to install an app to scan a 2D code at that location.

Simultaneously, government health departments tried to release tracing apps they managed that would complement the labor-intensive task of people-based contact tracing. That requires large numbers of people who, after someone is diagnosed, get in touch with everyone that person may have intersected with while infectious. (It’s remarkable how many traces of ourselves we leave through credit-card purchases, security cameras, and other means that have been used to notify people of potential infection.)

Some countries’ apps required that a smartphone was constantly awake and unlocked. There are ways to use accessibility features in iOS and Android to do this, effectively making the touch screen non-responsive except in certain cases, and reducing screen brightness to preserve battery life. Many also centralized location tracking, meaning whenever you were using the app, government agencies had a constant set of information about where you had been.
But what was really needed were fundamental, low-level changes in the two biggest operating systems worldwide: iOS (iPhone only) and Android. And, wouldn’t you know, Apple already had a model it could pursue for tracking with privacy preservation—a crowdsourcing system it developed for Find My, discussed in Use Find My for Tracking.

Apple and Google privately had a quick series of discussions in March about making this possible. Engineers on both operating systems worked up a prototype by April, which the companies announced jointly.

In this chapter, I explain how what the two companies describe as “privacy-preserving COVID-19 tracing” works, and the privacy implications of it—including how to disable it, if you don’t find the explanations compelling.

---

**How To Trace Individually But Anonymously**

The challenge with the novel coronavirus is that it is actually relatively difficult to pass in many circumstances. The best current epidemiological and clinical research strongly supports that you need to be in the vicinity of someone with the disease for some period of time and inhale enough viral particles that they overcome your immune system’s basic response. If everyone is masked, asymptomatic, several feet apart, and either outdoors or in well-ventilated and filtered areas, the odds are low to nil for contracting the disease at all.

In less ideal circumstances, people typically have to be close enough together for a period of time to pass the virus. There are many exceptions, but the vast majority of infections appear to fall within those parameters.

---

**Note:** People who have symptoms, like coughing and sneezing, can spread the disease much more readily. But folks in those circumstances are also more easily screened and barred from entering spaces or interacting with people.
Apple Blocks Tracking in Safari

Advertising-technology companies have built elaborate ways to track us across websites, apps, and even real-world purchases that we make. They extract location information from ads and trackers embedded in apps that let them overlay our physical location—without our explicit permission or knowledge—with our digital activities. It’s incredibly creepy and a huge violation of trust. In some countries and regions, it’s outright illegal.

The goal isn’t just to invade our privacy. Rather, ad-tech networks assemble a valuable profile of us, full of demographics (our age, race, income, and so on) and our purchasing habits. This allows them to charge the highest fees from advertisers, who believe super-targeted ads produce better outcomes.

**Note:** There’s evidence that some kinds of targeted ads work. But ad-tech companies charge so much, go to such lengths to obscure their workings, and provide such poor results overall, that the majority of the premium paid for targeting is basically wasted by advertisers, who are starting to get wise.

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.

Apple has taken a strong stance in this area, and in each new release of Safari across all its platforms in the last few years has added additional features designed to block unwanted tracking—particularly tracking that uses loopholes or isn’t disclosed in an ongoing way—while also providing more information to users about exactly what’s going on.

In this chapter, I look at some long-term Safari behaviors and several additions Apple has put in place over the last few years that limit how
ad-tech companies can match us to existing profiles or track us over time and place.

---

**Safari Blocks Cookies**

A browser cookie is a short piece of text that a web server sends a browser as part of its response to a page or media request. The browser, based on various rules, may store the cookie and hold it for a period of time. On subsequent requests to the same web server, the browser sends back the text.

Browser cookies are often used to store a unique identifier after someone logs in or across a visit. That allows the server to preserve state, or continuity of a session for a browser across the site. (The web was designed to be **stateless**, so that each page or media request stands alone. That’s great until you want to accomplish any task on a site, including setting a default text size.)

Starting in 2017, Apple revamped how they approach 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.

Since then, 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 websites 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.
Set Up for Privacy

It’s a privacy conundrum. When you’re setting up an iPad or iPhone from scratch, Apple encourages you to enter personal or private details and connect your mobile device to their services before they let you fully choose how you want to share data.

In this brief chapter, I explain what you need to do when setting up a new device or erasing one to share as little as possible from the get-go. In each case, I explain how you can choose to set up a feature or share your data at a later point if you wish.

After starting setup and selecting a language and country, Apple guides you through setup, which involves a number of decisions about what you disclose.

**Note:** This assumes you bypass the Quick Start process, which using wireless networking to copy settings from a physically nearby phone you’re currently using. You don’t make privacy decisions, since they were made and stored previously for that device.

You may see all or just some of the following screens (and potentially a few different ones), although they should appear in this order:

- **Choose a Wi-Fi Network:** 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 56). The moment you do this, some information about your activities starts transmitting immediately—although it’s not much at this point!
Figure 56: You have to pick a network to proceed.

- **Data & Privacy**: Apple alerts you that in using iOS or iPadOS, you see the icon shown in the screen whenever Apple wants to use your personal information (Figure 57). This step collects no information.
Control System Privacy

Apple states repeatedly that they are committed to keeping their customers’ data private, and they do seem to do a better job than other companies because they’re primarily interested in selling us products—hardware, software, and services—rather than treat us as the product for advertisers or advertising.

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 they promises to handle your personal data and information about you.

Much of the information iOS/iPadOS 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 they need, and when they need to make a connection between you and that data, they associate 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 tap.

In this chapter, I examine the many places 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:** Enable Screen Time in Settings > Screen Time, and its Content & Privacy Restrictions options let you lock all privacy settings in whatever state you like. You can choose to unlock them, but it creates a static default state.
Apple Doesn’t Track for Its Ad Services

Apple used to engage in some permission-based tracking for ads served by its own ad platform. In iOS 14/iPadOS 14, however, Apple no longer does. It states via a link at Settings > Privacy > Apple Advertising “that it does not link user or device data collected from our apps with user or device data collected from third parties for targeted advertising or advertising measurement purposes, and does not share user or device data with data brokers.”

The one setting that remains in that area is a switch for Personalized Ads, off by default. If you enable it, Apple will deliver “relevant” ads, but it doesn’t explain exactly how it determines what’s relevant.

Manage Siri Privacy

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.

Apple says they generate a random identifier that can’t be connected back to you and associate with it a variety of information for up to six months: computer-generated transcripts of what you said, audio (only if you opted in; see sidebar, next), approximate but not exact location (if you allow it), device specifications, and performance statistics. For Safari-based suggestions, which contain potentially more sensitive requests, the random ID changes every 15 minutes.
Keep 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.

Apple added the first blocking tools several years ago and gradually broadened since then. In this chapter, I look at built-in, automated, and third-party options for blocking unwanted contact.

What Apple Doesn’t Block

Despite Apple and third-party options, the company still provides too many ways for targeted harassment and spammy patterns of contact to occur, both of which should be well within their ability to curtail.

✦ You can’t create a list of permitted phone numbers representing the only calls you want to receive at all or have your phone notify you about.

✦ Management tools for blocked phone numbers are extremely poor—basically a list. There’s no good way to manage the block list described below and you can’t create wildcard matches, like “all numbers starting (939) 555-“.

✦ You can’t block SMS/MMS messages from unknown recipients (they are placed in a separate tab, as noted below).

✦ Your iPhone doesn’t let you block a frequent pattern of calls, either from unknown sources (no Caller ID), from similar numbers, or over short periods of time. Some third-party tools may help.

You’d think given the severity of phone and text harassment, Apple would advance further on these fronts.
Block Numbers and Email Addresses

Apple lets you block incoming voice calls, text messages, iMessages, FaceTime calls, and email messages by specifying a phone number or email address.

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. Block lists are also synchronized across appropriate software on iOS, iPadOS, and macOS on all devices logged in to the same iCloud account.

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 Info button, 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 this Contact/Caller,” all associated information is added to the Blocked or Blocked Contacts list (Figure 77).
Create, Manage, and Use Strong Passwords

Apple’s built-in password-management system creates, manages, and fills in strong, unique passwords for every website 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 websites that purport to reveal the quality of password you picked.

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

- If you have to enter a password by hand or memorize it, pick one that is long and made up of words you can easily remember and type or tap in.

- Rely on a password manager, such as the one built into iOS, iPadOS, Safari for macOS, and Keychain Access in macOS. Have it generate a complex password if you never need to enter it by hand.

- When forced to use a complex password (letters, numbers, and symbols), it should 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.
• 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 the most part, you should be using a password manager, and can use a complicated and long password without worrying about the details, since you’ll never enter it by hand.

However, if you need a password that you have to enter routinely—like in iOS or iPadOS every several days or after restarting—pick one that’s made up of three to five words and is at least 20 characters long—some people recommend at least 32 characters! Choose unique words, ones that aren’t from a common poem or that make sense together, and that you can memorize. Make up a story, 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 website 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 website 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 website 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
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.

For anyone setting up Wi-Fi security for a network, you can read up about the kind of security to deploy and how users with mobile devices can connect.

**Note:** Cellular networks have their own security methods that users can’t change or control.

**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. That’s changing with WPA3 (see WPA3 Provides More Discrete Encryption, below), but it’s not in deployment yet. When you connect, I recommend using only secured services, and you might consider a virtual private network (VPN) service, too. Read Connect with a VPN for details.

Connect to a Small Network

Nearly all home and small-office networks with wireless security enabled require the entry of a password. Enter the password when prompted, tap Join, and, if entered correctly, you’re done.

The password is stored in iOS/iPadOS, and the next time you’re near the same network it’s automatically supplied. 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 works only while you’re connected to the network.) See Forget This Network for more information.

**iCloud Syncs Wi-Fi Passwords**

If you have [iCloud Keychain](https://support.apple.com/en-us/HT202822) enabled, entering a Wi-Fi network password synchronizes it against all devices connected to the same iCloud account. You won’t have to enter the password on any of those devices after the next time they have internet service. Thus, you might connect to a network via the operating system that you’ve already connected to in macOS and not be prompted, and vice versa.

Because this data is synced only via a local network or the internet, I recommend connecting your non-cellular device or devices first to a new network. They will sync the Wi-Fi password once connected to your iPhone or cellular iPad if those devices have mobile connections, and then they will automatically connect.

**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 re-syncs 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: via Bluetooth and with 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—it requires just a single tap. Both the person already connected and the person connecting must have Bluetooth enabled, and the sharing person needs the other person’s iCloud account email in their Contacts.
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 trusted elements 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 many purposes in iOS and iPadOS: for iCloud sync, iCloud Drive, App Store purchases, iMessage, and more. However, unless you make 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 that lets you prove your identity.

In Apple’s implementation, when you enable 2FA, you keep your existing Apple ID password, and add at least one phone number that can receive SMS (text) messages or voice calls, and one or more trusted devices, which can be an iPhone, iPad, iPod touch, or Mac.
**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.

**Note:** Apple initially offered a harder-to-use two-step verification for improved account security. The company 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. If you’re still managing two-step verification, my book *Take Control of Your Apple ID* might be helpful, including in transitioning to 2FA.

### The Risk of SMS 2FA Factors

Apple’s system doesn’t rely primarily on SMS codes to deliver a second factor. Some other companies that use 2FA also now prefer their own system (like Google’s device-based app approval for logins). Many also emphasize authentication-app generated code that uses time-based one-time passwords (TOTPs), which can be managed in 1Password, Authy, Google Authenticator, and other code and password software.

But Apple and nearly all of these other companies allow SMS as a fallback option. Apple doesn’t let you disable trusted phone numbers entirely. That’s unfortunate, because text messaging has become an unreliable way to deliver a security token, even though you might think it won’t affect you.

People engaged in identity theft, particularly to siphon cryptocurrency from wallets and real currency from bank accounts, use a combination of social engineering (talking people into something, like customer-service reps), phishing, and account hacking to move a phone number from the authorized party’s phone to one under their control.
Connect with a VPN

The data that travels to and from your iPhone or iPad isn’t necessarily 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 websites 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. By 2020, 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.
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 for fingerprint recognition, and Face ID for facial recognition. All devices with Touch ID or Face ID support the latest iOS and iPadOS, as well as having robust hardware encryption. (Apple’s current iPhone and iPad models include either Touch ID or Face ID, as do iPhones and many iPad product lines dating back several years.)

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 single best protection against anyone unauthorized having access to data is enabling the passcode lock. This allows you to set a code required to wake and gain access to the device.

When Touch ID or Face ID is 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 101).

![Figure 101](image)

**Figure 101:** You can opt for a more complicated or shorter passcode.

**Warning!** Many mobile security gurus say not only are four digits too few to resist cracking, but six aren’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.
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/iPadOS device is, unless the owner has disabled letting that person or anyone see their 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. However, iCloud.com still shows those services as separate entries.
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 provide details using Wi-Fi; iPhones and cellular iPads add cellular radios and GPS.

**Note:** Find My works on devices that can run iOS 5 or later; for Lost Mode, iOS 6 is the minimum; for Activation Lock, iOS 7. On Macs, OS X 10.7.5 Lion or later is required.

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. *Triilateration* 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.
Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments.

You can access extras related to this ebook on the web. Once you’re on the ebook’s Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook’s blog. You may find new tips or information, as well as a link to an author interview.
- Find out if we have any update plans for the ebook.

If you bought this ebook from the Take Control website, it has been automatically added to your account, where you can download it in other formats and access any future updates.

This is but one of many Take Control titles! We have books that cover a wide range of technology topics, with extra emphasis on the Mac and other Apple products.

You can buy Take Control books from the Take Control online catalog as well as from venues such as Amazon and the Apple Books Store. But it’s a better user experience and our authors earn more when you buy directly from us. Just saying...

Our ebooks are available in three popular formats: PDF, EPUB, and the Kindle’s Mobipocket. All are DRM-free.

Click here to buy the full 254-page “Take Control of iOS & iPadOS Privacy and Security” for only $14.99!
About the Author

Glenn Fleishman never stops writing about technology and its implications. He’s in his third decade of writing for publications as varied as *American History*, *Fast Company*, the *Economist*, *Smithsonian* magazine, Increment, the *New York Times*, *Macworld*, and TidBITS, and many others. In 2012, he was a two-game champion on Jeopardy!

Acknowledgments

This book has gone through so many incarnations, it’s hard to remember what it started as. However, Tonya Engst deserves the credit for suggesting the title when the iPad was introduced, and the book was part of four Take Control ebooks released at once to help support new iPad buyers. Since then, I had her help and that of Adam Engst, Jeff Carlson, Scout Festa, and Joe Kissell in varying ways to keep it moving along. Thanks for a decade of help!

Shameless Plug

I don’t write just ebooks—I also produce ones of actual physical matter, too. My latest is *Six Centuries of Type & Printing*, a title that traces the technology and advancements in making type, composing it into words and pages, putting ink on it, and pressing it to paper from before Gutenberg’s perfection of metal printing types through the digital era in which type transcends the printed page.

Click here to buy the full 254-page “Take Control of iOS & iPadOS Privacy and Security” for only $14.99!
The type for the book was composed on a hot-metal Monotype casting system and printed by letterpress in London. The page is a 64-page cloth-bound hardcover book with foil stamping that comes in its own slipcase, bound in Germany. It unfolds nearly 600 years of printing and is a work of art in its own right. You can order a copy directly.

---

**About the Publisher**

alt concepts inc., publisher of Take Control Books, is operated by Joe Kissell and Morgen Jahnke, who acquired the ebook series from TidBITS Publishing Inc.’s owners, Adam and Tonya Engst, in May 2017. Joe brings his decades of experience as author of more than 60 books on tech topics (including many popular Take Control titles) to his role as Publisher. Morgen’s professional background is in development work for nonprofit organizations, and she employs those skills as Director of Marketing and Publicity. Joe and Morgen live in San Diego with their two children and their cat.

**Credits**

- Publisher: Joe Kissell
- Editor: Jeff Carlson (iOS 8 through iOS 13/iPadOS 13), Joe Kissell (current edition)
- Cover design: Sam Schick of Neversink
- Logo design: Geoff Allen of FUN is OK

Click here to buy the full 254-page “Take Control of iOS & iPadOS Privacy and Security” for only $14.99!
Copyright and Fine Print

Take Control of iOS & iPadOS Privacy and Security
ISBN: 978-1-947282-64-3
Copyright © 2020, Glenn Fleishman. All rights reserved.

alt concepts inc., 4142 Adams Ave. #103-619, San Diego CA 92116, USA

Why Take Control? We designed Take Control electronic books to help readers regain a measure of control in an oftentimes out-of-control universe. With Take Control, we also work to streamline the publication process so that information about quickly changing technical topics can be published while it’s still relevant and accurate.

Our books are DRM-free: This ebook doesn’t use digital rights management in any way because DRM makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, they should buy a copy. Your support makes it possible for future Take Control ebooks to hit the internet long before you’d find the same information in a printed book. Plus, if you buy the ebook, you’re entitled to any free updates that become available.

Remember the trees! You have our permission to make a single print copy of this ebook for personal use, if you must. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Caveat lector: Although the author and alt concepts inc. have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed “As Is,” without warranty of any kind. Neither alt concepts inc. nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

It’s just a name: Many of the designations in this ebook used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

We aren’t Apple: This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are registered trademarks or service marks of Apple Inc. If you’re into that sort of thing, you can view a complete list of Apple Inc.’s registered trademarks and service marks.

Click here to buy the full 254-page “Take Control of iOS & iPadOS Privacy and Security” for only $14.99!