



Keep Safe USING Mobile Tech

by **GLENN FLEISHMAN**
\$14.99

2ND
EDITION

Table of Contents

Read Me First.....	4
Updates and More	4
What's New in the Second Edition	5
Introduction	8
Identify Your Risk.....	10
Know The Main Areas of Risk	10
What This Book Doesn't Cover	13
Control What You See	16
Apple's Aegis Differs by Age	16
Google Goes Global with Sensitive Content Warnings.....	21
Block and Deflect Abuse, Spam, and Scams	26
Stop, Screen, and Sort Unwanted Calls.....	27
Filter Messages	41
Block Incoming Communications	52
Secure Devices and Accounts	57
Tracking Your Items	57
Protect Encrypted Messages	80
Protect Device-Connected Accounts	87
Deal With Emergencies	93
Set Up Emergency Medical Information and Contacts	93
Detect an Automobile Crash	94
Lost or Injured and Need To Call	97
Earthquake Warnings with Google	109
Mind the Health Warnings	110
Protect Yourself Physically	120
Check In for Peace of Mind	121
Deter Stalking by Tracking	130
Perform a Safety Check (Apple)	136
Secure Your Device Passwords	140

About This Book.....	151
Ebook Extras	151
About the Author	152
About the Publisher	153
Copyright and Fine Print	154

Read Me First

Welcome to *Keep Safe Using Mobile Tech, Second Edition*, version 2.0, published in November 2025 by alt concepts. This book was written by Glenn Fleishman and edited by Joe Kissell.

This book describes how to protect your physical, psychological, and online security related to your private data, whereabouts, and health and safety with tools available from Apple and Google on mobile devices, desktop operating systems from Apple and Microsoft, and accounts in the Apple, Google, and Microsoft ecosystems.

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 © 2025, Glenn Fleishman. All rights reserved.

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.
- Access the book in both PDF and EPUB formats. (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.

What's New in the Second Edition

When I wrote the first edition of this book, I thought we might see a long period with no changes, as Apple and Google—as the biggest drivers of change—seemed to have staked out their personal safety perimeters. I was wrong! In the last year, and particularly since September 2025, both companies have pushed out a number of significant improvements and new features that required a substantial revision to the book you have in your virtual hands.

Apple Updates

Apple added powerful features to help deter scammers and fraudsters from ever reaching you in September 2025, with different features available in their three main communications apps, FaceTime, Messages, and Phone. These updates came with the release that month of iOS 26, iPadOS 26, macOS 26 Tahoe, and watchOS 26.

Note: Apple has switched to using the same version number for all their operating systems, based on the last two digits of the following year—"26" for fall 2025 releases.

Here is a list of these new features, with a note in parentheses about which apps include them:

- **Block spam calls (FaceTime, Phone):** Incoming calls identified as fraudulent are blocked by default. See [Sort Unknown Callers with Apple](#).
- **Silence and filter unwanted calls (FaceTime, Phone):** Incoming calls that aren't from a known caller (contacts and previous calls) and haven't been marked as spam are silenced and filtered. See [Sort Unknown Callers with Apple](#).
- **Screen and filter incoming text messages (Messages):** Messages from unknown parties are filtered as unknown or spam. See [Filter Messages with Apple](#).

- **Deactivated links and phone numbers in spam texts (Messages):** Any link or phone number is deactivated in a message filtered into the Spam category. This makes an accidental click less likely. See [Extra Protections in Spammy Texts](#).
- **Call Screening (Phone):** If you enable Call Screening, unknown inbound callers don't cause your Phone app to ring. Rather, they are asked by a machine-generated voice to provide their name and why they are calling. If they reply, this is transcribed and shown to you through a notification. See [Screen Calls with Apple](#).

Also featuring in the fall 2025 updates for iPhone:

- **Check In changes:** Apple revised the Check In safety feature, adding a Workout category and more notifications when everything is OK. See [Check In with an iPhone](#).
- **Safety Check upgrades:** iOS 26 has more information about what you're sharing and with whom, including what you sharing publicly, in this feature designed to let you shut down some or all of your connections with others if you're in danger. See [Perform a Safety Check \(Apple\)](#).

Note: After another year since the name Apple Account replaced the old Apple ID moniker for Apple ecosystem accounts, this revision removes all mentions of Apple ID, except to note this backward-looking fact.

Google Updates

Google didn't sit still in this period, either. Since the last update to this book, Google has made a number of safety-related improvements:

- **Sensitive content warnings:** Google added sensitive content warnings to Google Messages in Android. See [Google Goes Global with Sensitive Content Warnings](#).
- **Call Screening:** Some Google Pixel phone models have automatic and manual options for screening incoming calls to avoid unwanted ones. See [Listen in to Calls on Google Pixel](#).

- **Live Voicemail:** Not yet released, Google reportedly has a Live Voicemail feature nearly ready. See [Listen to Voicemail Live with Google](#).
- **Message spam filtering:** Google rolled out new scam-detecting features starting in October 2024 that could help dramatically block scams and spam, and alert you to potential risk. See [Filter Messages with Google](#).
- **Find Hub:** Google quietly moved from branding their device and item tracking network as Find My Network to Find Hub in mid-2025. See [Find with Google](#).
- **SOS by satellite:** On Google Pixel 9 and later phones and the Pixel Watch 4 (with LTE), you can place emergency services calls by satellite. See [Connect by Satellite with Google](#).
- **Theft protections:** Google deployed a whole suite of options that will make a stolen Android phone dramatically less useful to a thief, protecting your data while also (hopefully) deterring robberies. See [Google Adds Stolen Device Protection](#).

Other Updates

Companies other than Apple and Google have added or updated features, too! Here's what you'll find in this version:

- **Direct to satellite:** T-Mobile offers a direct-to-satellite service that can be useful in quasi-emergencies, when you don't need emergency services but do need help. Supporting 60 phone models, it relies on the StarLink constellation of low-flying satellites. See [Connect Direct to Satellite](#).
- **Samsung watch fall detection:** Samsung added fall detection to their various watch models. See [Samsung Watch Fall Detection](#).

Introduction

Peace of mind is invaluable. Sometimes this can be hard to achieve. Technology often works against our sense of equilibrium in the world, providing us more to worry about instead of less. But you can leverage technology to take care of real risks and push away both reasonable and unfounded anxieties.

Keep Safe Using Mobile Tech provides a roadmap for your personal safety and well being by employing an ever-increasing array of tools, primarily offered through smartphones, that can help you remain safer.

Some elements of keeping safe are beyond our control. As an analogy, we can stop putting pesticides on our own lawns to avoid exposure, but can't prevent other people and giant companies from poisoning the land and water. Yet, we can create bubbles of safety that protect us from a lack of broader regulation and oversight by companies that would make more people safer by default, like adding a water filter that captures pollutants before we drink them.

These bubbles can include enabling features (some a checkbox, others an app's worth of options) to protect against message interception; the unwanted receipt of images with nudity, and spam and abusive incoming calls, texts, and video sessions; a way to lock down your devices against a potential active attack by a government or large-scale criminal intrusion; an option to have a safety buddy to check in with after a period of time or to confirm that you've arrived at a given destination; and satellite communications when lost or in an accident.

Some phones and wearables support crash detection and other health events, trying to get a response from you and providing your location automatically in the case of an emergency or a services call. Some also alert you to imminent earthquakes, help you with road service, and let you find where you are when you're lost and outside of cell range.

While I cover Android, iOS (iPhone)/iPadOS (iPad), macOS (Macintosh), watchOS (Apple Watch), and Windows, this book tilts somewhat towards Apple for the very good reason that the company has spent years adding an array of tools oriented at personal safety—not just data integrity and data protection—and integrates them across their several operating systems.

Fortunately, however, Google has stepped up to the plate by expanding options for Android phones and tablets (particularly their own Pixel models), Wear OS smartwatches, compact Bluetooth-based tracking items, and related account services.

Phone makers and cellular carriers have even expanded to eyes-in-the-sky: Apple, Google, and T-Mobile now have options that let you send both emergency messages, your current location, and routine texts by relaying through low-flying satellites. While you may want to be off the grid at times, having a safety backup without carrying an expensive satellite phone and maintaining a subscription for its usage is a significant advantage for your wellbeing.

Apple's focus on personal safety seems to have provided a competitive bump that has led other companies to expand features. I hope we will still see more novel features not yet conceived of, designed to keep you safe, healthy, private, mentally well, and physically secure.

Note: I discuss Mac and Windows operating systems in this book because—even though they do not fall into the “mobile” category of devices like smartphones, tablets, or smartwatches—issues related to device theft, account safety, and certain aspects of personal safety still apply. Macs, in particular, have synced and linked features with iPhone, iPad, and Apple Watch.

Identify Your Risk

The world is a semi-dangerous place: figuring out where you're actually at risk is one of the most important ways to sort out what you need to worry about. In this section, I help you sort out how to evaluate what aspects of your privacy, safety, and well-being are at risk.

For clarity, I then explain areas outside of the focus of the book, and where to find more help in those matters.

Know The Main Areas of Risk

Keep Safe Using Mobile Tech addresses four main areas in order of the likelihood of most to least likely to happen to you.

How to deter unwanted digital contact:

The world of online and digital communications lets people contact you in ways never before conceived, which allows people to engage in targeted attacks that rely on details obtained about you or in less-specific, but direct waves of harassment. This can include insulting messages, threats, and unwanted images (particularly nudes).

- **Who causes it:** This may come from strangers, commercial entities, governments, domestic partners (or former ones), or people targeting you or your children.
- **Likelihood:** If you engage in social media, run a retail operation, or have some public-facing volunteer, paid, or elected role, you may encounter it. But, really, anyone could be a target.
- **How to protect:** Tools help you block, deter, and report people or groups for their behavior, such as call-blocking lists and incoming communications filters, which can include unwanted images with nudity. Some advanced features from Apple in their fall 2025 releases up the ante for deflecting and blocking. See [Block and Deflect Abuse, Spam, and Scams](#) and [Deter Stalking by Tracking](#).

How to respond to health emergencies and personal and natural disasters:

A lot happens to us and around us every day. Many things are far beyond our control. Technology increasingly offers us ways to predict, mitigate, and respond.

- **Who causes it:** Generally not who, but what: A sudden flash flood or fire, a slippery road, or one's own internal organs causing sudden betrayal could lead you to need help—sometimes within moments. Or, leaving the well-trod path, intentionally or otherwise, you face dangers or even death that result from being lost.
- **Likelihood:** Depending on where you live, what you do routinely, and your health, you may have a good sense of how often you might need technological help. However, we can always get lost.
- **How to protect:** Apple and Google have built a number of automatic monitoring tools into their phones and Apple into their Apple Watch. These monitors can track car crashes, falls, heart abnormalities, and other issues; Google also offers earthquake alerts, buying you critical seconds to improve your safety. Apple, Google, and T-Mobile offer satellite-based emergency access on certain phone models and plans in particular countries. They also have non-emergency satellite access that can help in still-challenging situations. See [Deal With Emergencies](#).

How to protect against physical risks from others:

It's unfortunate that other people can be what we need to guard against. Until about three years ago, mobile operating systems offered little in the way of deterrence, protection, or response to violence. Now, options have multiplied and are improving year over year.

- **Who causes it:** An unknown criminal, a stalker or acquaintance, or a domestic partner may engage in *threatened or actual violence* to get your smartphone password. This could include a credible verbal threat, a physical attack, drugging, or detaining or kidnapping you.

Control What You See

In this chapter, I look at what ecosystems offer in two broad areas. First, I look at features related to controlling the viewing of images and videos with nudity on mobile devices (Apple and Google) and desktops (Apple). Adults have options for themselves and for accounts of children they supervise that warn about sending media with nudity, and blur images and videos received that appear to contain it. Apple and Google take a similar approach, with key differences in how warnings are shown for children and adults.

Apple and Google offer an on-device analysis that identifies nudity in incoming images and videos, and lets you control what you see or your children see in some cases. This analysis happens entirely on your devices—no media is sent to Apple or Google.

Apple's Aegis Differs by Age

Apple has two related but distinct systems for handling sensitive images: Communication Safety covers children under 18; Sensitive Content Warning is for adults.

Protect Your Children with Communication Safety

Communication Safety provides parents with the ability to influence their under-18 children who might be sending and receiving images and videos that contain nudity.

Note: This feature requires at least iOS 15.2/iPadOS 15.2, watchOS 8.3, and macOS 12.1 Monterey. The feature is enabled by default starting in iOS 17/iPadOS 17 or later, macOS 14 Sonoma, or watchOS 10 or later, versions which are also required to screen videos.

The feature sweeps in minors passing around pictures from online porn, taking videos of themselves without clothes on, or snapping photos at a nude beach or naturist resort, among various possibilities. Communication Safety allows a parent to enable steps that their child sees but that the parent isn't aware of.

Note: By focusing on nudity in general, Apple bypasses trying to analyze whether an image involves harm or abuse.

The feature covers images and video in different ways depending on the device type:

- **iPhone and iPad:** Photos and video sent or received using Messages or AirDrop; images in the Contact Poster option for phone calls between iPhones (Phone app, Contacts app); FaceTime video messages; and photos in some third-party apps that support the Communications Safety framework
- **Mac:** Photos and videos sent or received in Messages and with some third-party apps
- **Apple Watch:** Photos and video sent or received in Messages, Contact Posters, and FaceTime video messages

Children aren't prevented from seeing or sending images with nudity. Rather, they are given a moment's pause. When someone attempts to send them an image or video that appears to contain nudity, or if the child attempts to send one, they see a highly blurred image and a warning. The warning offers guidance on seeking help.

Communication Safety has two prerequisites:

- A child must be under 18 and part of an iCloud-based Family Sharing group.
- The adult and child must have at least the minimum versions of the operating systems noted above.

The system has children's interests in mind. If a parent enables the warning feature, children can generally avoid seeing both images of a

Block and Deflect Abuse, Spam, and Scams

Every technological breakthrough has a downside. When the telephone was invented, suddenly people could interrupt your dinner. Voice calls plus mobile devices mean incoming callers have access to you everywhere and can use that for lots of malicious purposes, including convincingly faking who they are.

The availability of text messaging for instant communication with anyone else who had a cell phone also seemed like a huge win for personal and business interactions: getting together for a drink, passing along information during meetings, and chatting with friends.

But text messaging wasn't designed for the possibility of harassment. When it was invented, this wasn't part of the set of concerns built into its design, making it difficult or impossible, depending on your phone and carrier. Anyone who acquired your phone number could send you unwanted texts. When blocking became an option, you typically had to pay your phone carrier a recurring fee, and could only ban numbers individually.

Fortunately, that's changed. It's much easier to let your phone maker or a phone carrier block, deter, or mark incoming texts and phone calls, reducing their distraction and the potential that someone will convince you to act against your interests.

In this chapter, I look at how you can manage unwanted incoming communication. Apple and Google have made substantial improvements in late 2024 through late 2025 that put more tools—and more powerful ones—at your fingertips. The balance of power may briefly be on your side?

I've broken this chapter into three parts:

- Blocking, filtering, and screening incoming phone calls (and, for Apple, incoming FaceTime audio and video calls)
- Blocking and filtering messages
- Blocking a broad category of incoming communications

Tip: This chapter is about protecting yourself from people trying to communicate with you and how to block and deter them and their actions. The next chapter, [Protect Yourself Physically](#), is about deterring and protecting against physical and emotional distress and harm.

Stop, Screen, and Sort Unwanted Calls

I would wager most people hate incoming phone calls at this point in technology's evolution. Some people never want to be on the phone, and most of us just need a break from incessant spam and scam calls. Fortunately, help has arrived from Apple and Google.

Note: With Apple, there's a bit of a blurred line between FaceTime calls and regular phone calls. When discussing incoming calls, I include both the FaceTime and Phone apps, and discuss any relevant differences.

Apple and Google now offer what I'd categorize as three approaches to reduce the bother:

- **Spam/scam identification:** Android phones and the Apple Phone app use proprietary algorithms to mark some calls as spam. You can take action (such as not ringing the phone or sorting into a special category) based on that analysis. Third-party apps can help with this, too.
- **Call screening:** An automated agent can ask an incoming caller for more information to deter unwanted calls or let you know in real time. This helps you avoid wasting your time while still being able to answer the call if it's one you want to take.

Secure Devices and Accounts

Part of keeping yourself safe is knowing who has access to your hardware, accounts, and private messages, either by getting hold of your devices or by finding ways to stick a wedge into your personal hardware or accounts.

This book doesn't deal with *how* someone gets your stuff or gets into your personal data—it could be a mugging, burglary, government-scale undetectable physical or data break-ins, or malware, for example. Rather, it's how you can prepare and respond to such invasions.

In this chapter, you learn about how to set up tracking on your devices and how to deal with a theft. I also cover the Apple-specific feature Lockdown Mode, an option for people to harden their operating systems against attacks by a government, associated contractor, or large-scale criminal enterprise.

A few messaging systems offer a way to determine whether someone has subverted their systems or your end-to-end encryption, and I explain how to set up and watch for that behavior—although very few people are at risk.

Finally, get to know the details of establishing the highest level of protection for Apple, Google, and other accounts that are tied directly to your devices.

Tracking Your Items

A friend once had their laptop stolen from their car. While they didn't have any tracking software installed—this was many years ago—they did use Backblaze, an encrypted online backup service that, as an option, let you turn on tracking. Their backup software connects continuously to archive files as they're modified and could be set to

retrieve location information among other data and report it to you. (The company [still offers this feature](#).)

Unfortunately, my friend hadn't enabled it before the computer was stolen, and because location data relates to privacy, he had to have the computer in front of him to authorize the software to track—it couldn't be applied remotely or retroactively.

This is true of a lot of “horse is already out of the barn” scenarios: you need to make sure you set up tracking (just like backups) before the event you dread has happened.

Apple, Google, and Microsoft offer Find My *Blank* services that are easy to enable and can provide tracking information if your hardware goes missing—whether lost or stolen—the next time it has an internet connection or, with crowdsourced networks from Apple or Google, is within Bluetooth range of a supported item on one of those networks. One third-party, Tile, has its own tracking network that works only with devices sold by Tile.

How Does Crowdsourced Location Work?

Crowdsourcing location is very clever: because so many computers, smartphones, and smartwatches are out in the world, and most of them can determine their coordinates with some precision, Bluetooth-tracking items don't need GPS or other location data.

Instead, Apple and Google have these items transmit an encrypted Bluetooth network name that's in a format nearby internet-connected devices can detect. Without knowing anything about the trackers or who owns them, the devices relay their own location paired with the Bluetooth network name.

Apple and Google store this information such that only someone with the right account information can retrieve the encrypted payloads and decrypt the location. Apple and Google can't determine to whom the location data belongs, either.

It's likely that all the phones, tablets, and computers you own have built-in tracking. If you want to track other stuff—your car, a bike, a

Deal With Emergencies

Accidents and emergencies can be terrifying. Most arise with no warning, and may be followed by having no way to reach someone for help or to let them know you're OK. One of the promises of the always-with-you, always-connected world seemed to be safety, but those promises have often fallen short.

However, it feels as if we have moved into a new phase in recent years, in which some kinds of accidents, natural disasters, and other emergency situations can be prepared against or responded to with a computational and digital advantage.

In this chapter I look at four main areas that have started to live up to what the “future” was always expected to bring. I start with crash and related accident detection, available on some wearables (like the Apple Watch) and some smartphones. I look into what to do when you're lost or injured and have no cellular or other network coverage.

Then I get into slightly more specific areas that I hope to explore more in future updates and editions: earthquake warnings that are specific to where you live, providing seconds to minutes of advance warning that can help you get to safety; and health warnings, such as your heart rate going out of controlling or exhibiting other medical anomalies.

Let's start by filling out a profile that will help in case of an emergency.

Set Up Emergency Medical Information and Contacts

Apple and Google both let you set up emergency medical information and emergency contacts on their smartphones. Paired smartwatches can access the same information. If you enable access to this information when your device is locked, someone viewing it can tap a phone number listed for an emergency contact to place a call.

On an iPhone, open the Health app, tap your profile picture in the upper-right corner, and tap Medical ID. You can provide your health profile and add emergency contacts. Enable Show When Locked to let people view from the Lock Screen.

To see emergency details on an iPhone, on the Lock Screen, tap Emergency > Medical ID. (You can also press volume up and the side or top button, hold it, then swipe on Medical ID. This also disables Face ID and Touch ID.) On an Apple Watch, press and hold the side button until a Medical ID slider appears and slide it to the right.

On an Android phone with the Personal Safety app, open it and use Medical Information to add details, and Emergency Contacts to add people. Navigate to “Allow access to emergency info” > “Show when locked” to allow Lock Screen access.

To view emergency information, press and hold the volume up and power buttons until Emergency appears. Tap “View emergency info.” On a Pixel Watch paired with a Pixel Phone, press the crown until Medical Info appears. (A Pixel Watch must be paired with a Pixel Phone for this to work.)

Tip: In Android, make sure information is sent to emergency services during a call by also enabling “Share during emergency call.” This is always available on iPhone and Apple Watch.

Detect an Automobile Crash

I’ve been fortunate enough to have only a few very minor fender benders in my life—taps, not crashes—and I hope you are in the same boat. However, we know that being in a vehicle and being hit by, or hitting, someone or something is all too common. What if, when that happened, you were carrying a device that could check whether you’re capable of responding—and if not, would automatically place an emergency call?

Certain Google Pixel, Pixel Watch, Apple iPhone, and Apple Watch models include automatic detection of a car crash (**Figure 33**).

Protect Yourself Physically

In the past, electronic security meant keeping your passwords private and your computers safe from intrusion. Now, it can also encompass physical safety. You can use devices you carry with you or use every day to help keep yourself safe from strangers out in the world or from people you know no matter where you are.

This chapter examines the relatively new field of physical security enhanced by digital tools. I break the chapter down into four areas, two of which are, so far, proprietary offerings from Apple that I hope will spread further.

First, I look at features that let you alert others if you don't check in within a period of time or don't reach (or divert from) a specified location. Another set of digital eyes can help reduce anxiety and offer assistance in the event that something bad does happen.

Next are the much broader issues of how to be aware of and deter stalking using Bluetooth-based crowdsourced tracking items. While Apple has the broadest footprint with their AirTag and Find My network, Google joined the club in 2024 with their Find Hub technology and network. A number of third parties make compatible hardware for both systems.

Tracking devices can be troubling enough, but facing safety issues from a domestic partner or other person known to you is often more fraught. In the third section, I explain how to use Apple's Safety Check available on iPhones, iPads, and Macs.

Finally, I dig into the upsetting issue of real-world password attacks, where criminals distract or assault you to obtain your device password. While infrequent in practice, you can still practice some deterrence in your behavior when unlocking your Apple or Google devices and in how you secure your accounts online.

Check In for Peace of Mind

One of the greatest fears we have is that either we or a loved one won't make it safely from Point A to Point B. It's sort of unreasonable: the vast majority of people who leave their homes to go somewhere else, sometimes multiple times a day, arrive without issue. Only a small number of people experience a problem—having delays, getting lost, suffering an injury, or even being abducted.

But the anxiety is real, no matter the statistics. You can gain a little extra piece of mind using technology. Google Pixel phones and Pixel Watch models and Apple iPhones let you set up conditions in which a device automatically contacts a trusted person or people.

There are two ways to approach this implemented so far (described from the initiator's point of view):

- **A timer (Pixel phone, Pixel Watch, iPhone):** You start a timer that, either before or when it stops, requires you to indicate you're OK. If the timer goes off and you don't respond, one or more people is alerted to that fact.
- **A location (iPhone):** You set a location that you're headed to, including the method you're using (walking, by car, or via transit). If you deviate too far from the path, there's a hold up, or you don't reach the location, and you don't respond to an alert, the system alerts emergency contacts.

Note: If this location feature sounds familiar, it's close to what [Uber](#) and [Lyft](#) offer, a "share my" route option introduced several years ago after concerns about a small number of drivers assaulting or waylaying passengers. The not-quite-taxi services share your route as you're underway, though, not just on arrival or when delayed.

Safety Check with Google Pixel

Google supports a timer in several Pixel phones and smartwatches via the Personal Safety app's Safety Check feature. Before starting, you

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your [comments](#).

Ebook Extras

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.
- Access the book in both PDF and EPUB formats. (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.

More Take Control Books

This is but one of many Take Control titles! We have books that cover a wide range of technology topics, with extra emphasis on Macs 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 two formats, PDF and EPUB, which are viewable on any computer, smartphone, tablet, or e-reader. All are DRM-free.

About the Author



Take Control Books Executive Editor Glenn Fleishman never stops writing about technology and its implications. Among other pursuits, he was a two-game champion on Jeopardy! in 2012.

After nearly 30 years of writing for publications like *American History*, *Fast Company*, the *Economist*, *Increment*, the *New York Times*, *Macworld*, and *TidBITS*, Glenn now focuses his time on Take Control Books, *Six Colors* (columnist), and his own micro-publishing endeavor.

You can find Glenn on [Mastodon](#) (@glennf@zeppelin.flights) and [Bluesky](#) (@glennf.com). Reach him by email at glenn@glennf.com.

Shameless Plug

I have two recent books about technology that—mostly—aren't about computers. [*Six Centuries of Type & Printing*](#) is a brisk yet thorough look at the technological development that has taken us from Gutenberg (and even before) to the present day. You can order a copy of the print, ebook, or audiobook edition [directly from me](#).

[*How Comics Are Made*](#) traces the history of newspaper comics in North America from 1896 to the present, looking at the path from a cartoonist's hand to the printed page. You can [order a signed copy](#) from me, or purchase a regular copy at [bookstores worldwide](#). ([Check your local library as well!](#))

About the Publisher

alt concepts, 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 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 Saskatoon, Saskatchewan, Canada, with their two children and their cat.

Credits

- Editor and Publisher: Joe Kissell
- Cover design: Sam Schick of [Neversink](#)
- Logo design: Geoff Allen of [FUN is OK](#)

Copyright and Fine Print

Keep Safe Using Mobile Tech

ISBN: 978-1-990783-83-8

Copyright © 2025, Glenn Fleishman. All rights reserved.

[alt concepts](#), 419 8B-3110 8th St. East, Saskatoon, SK S7H 0W2 Canada

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 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 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.