



TAKE CONTROL OF

Your Online Privacy

by **JOE KISSELL**

\$14.99

**5TH
EDITION**

[Click here to buy the full 211-page "Take Control of Your Online Privacy" for only \\$14.99!](#)

Table of Contents

Read Me First.....	5
Updates and More	5
What's New in Version 5.1	6
What Was New in the Fifth Edition	6
Introduction	8
Online Privacy Quick Start	11
Understand the Evolving Online Privacy Landscape ...	13
The Curse of Free Stuff Continues	14
Major Data Breaches Are Increasingly Common	15
Hardware Bugs Pose Challenges	16
Big Data Is Harder to Get Away From	16
Privacy Laws Are Changing	18
What About Privacy Policies?	20
Your Own Privacy Is Only Part of the Problem	21
See How Bad Things Are.....	23
Is It Too Late to Protect Your Privacy?	24
Learn About the Risks	25
Learn What You Have to Hide	25
Learn Who Wants Your Private Data (and Why)	31
Your Risk Profile	42
What You Can't Control	45
Develop a Privacy Strategy	47
What I Wish I Could Tell You	48
Create Privacy Rules for Yourself.....	51
Remove Your Info from Google	53
Purge Your Info from Data Brokers.....	55
Cope with Special Cases	58
Take the Pledge	60
Keep Yourself Informed	63

Discover Apple-Specific Privacy Features	65
Sign in with Apple.....	65
Hide My Email	66
Mail Privacy Protection	68
Link Tracking Protection	70
Intelligent Tracking Protection	70
Privacy Nutrition Labels	70
App Privacy Report	72
Location Tracking Protection	72
iCloud Private Relay	73
Advanced Data Protection	74
Lockdown Mode.....	76
Confront the Social Media Threat	77
Understand the Privacy Risks of Social Media	77
Learn About the Facebook Problem	79
Check Your Privacy Settings	83
Use Other Social Media Precautions.....	85
Keep Your Internet Connection Private.....	88
Understand the Privacy Risks of Your Internet Connection	88
Prevent Snooping	92
Turn Off Unnecessary Services.....	112
Mind Your Camera and Microphone.....	113
Use a Firewall.....	114
Use an Outbound Firewall	116
Browse the Web Privately	119
Understand the Privacy Risks of Web Browsing	119
Choose a Better Browser	124
Go to the Right Site	131
Say No to Selling Your Personal Info	133
Manage Local Storage of Private Data	134
Block Ads	142
Protect Passwords and Credit Card Info	146
Search Privately	148

Browse Anonymously	150
Shop Online Privately	153
Improve Email Privacy	157
Understand the Privacy Risks of Email	157
Reduce Email Privacy Risks	160
Encrypt Your Email	171
Send and Receive Email Anonymously	176
Use Email Alternatives	176
Talk and Chat Privately	178
Understand the Privacy Risks of Real-Time Communication ..	178
Improve Your Real-Time Communication Privacy	181
Manage Your Mobile Privacy	184
Supercookies	185
Granting Apps Access Permission	186
Location Awareness.....	187
Photos and Videos	190
Spear Phishing and Impersonation	191
Spyware	193
Mobile Backups	194
Keep the Internet of Things Private	198
Smart TVs and Streaming Devices	198
Smart Speakers.....	200
Web-Connected Cameras	201
Other Connected Objects	202
Maintain Privacy for Your Kids	205
About This Book.....	208
Ebook Extras	208
About the Author and Publisher	209
Credits	209
Also by Joe Kissell	210
Copyright and Fine Print	211

Read Me First

Welcome to *Take Control of Your Online Privacy, Fifth Edition*, version 5.1, published in January 2025 by alt concepts. This book was written by Joe Kissell and edited by Geoff Duncan.

This book explains potential privacy risks in everyday online activities like web browsing and sending email, and suggests strategies for avoiding common pitfalls and improving online 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 © 2025, Joe Kissell. All rights reserved.

Updates and More

You can access extras related to this book 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, links to author interviews, and update plans for the ebook.

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 Version 5.1

This minor update makes the following changes:

- Mentioned the RockYou2024 data breach in [Major Data Breaches Are Increasingly Common](#)
- Made several edits to the list of data-removal services in [Purge Your Info from Data Brokers](#)
- Adjusted the wording in several spots to reflect minor user interface changes in macOS 15 Sequoia, iOS 18, and iPadOS 18
- Added a sidebar, [What Are TLS and SSL?](#), and adjusted the wording throughout to refer to “TLS/SSL”
- Added Orion to the list of [Browsers You Should Consider](#)
- Mentioned additional techniques you or a family member can use to avoid being scammed in [Spear Phishing and Impersonation](#)

What Was New in the Fifth Edition

The fifth edition was the biggest revision to this book since its original publication in 2013 (and that’s saying something). It would almost be easier to list what *didn’t* change than what did! Given the huge shifts in both the threats to online privacy and the tools to protect your privacy, I rethought much of my advice, rearranged the outline, added a considerable amount of new material, and deleted things that no longer seemed relevant.

Here are some of the biggest changes:

- Revised [Understand the Evolving Online Privacy Landscape](#) extensively, including the addition of new topics [Hardware Bugs Pose Challenges](#) and [Is It Too Late to Protect Your Privacy?](#)
- Combined what had been two chapters into [Learn About the Risks](#), with a bigger focus on advertisers ([Advertisers—and Beyond](#)) plus new information on [Your Risk Profile](#) and [What You Can’t Control](#)

- Added a series of sidebars (see [Additional Resources for High-Risk People](#)) with extra advice for people with unusually high risk for being individually targeted
- In the chapter [Develop a Privacy Strategy](#), added new topics: [What I Wish I Could Tell You](#), which explains some measures you could take to massively improve your privacy, but at a significant cost; [Remove Your Info from Google](#), which does what it says; and [Keep Yourself Informed](#), which urges you to keep up with privacy-related changes in the world
- Added an entirely new chapter, [Discover Apple-Specific Privacy Features](#), which details some of the extra privacy tools available to users of Macs, iPhones, and iPads
- Renamed the social media chapter [Confront the Social Media Threat](#) and thoroughly updated it, with a significantly expanded topic [Learn About the Facebook Problem](#)
- In the [Keep Your Internet Connection Private](#) chapter, largely rewrote [Use a VPN](#) and [Consider a VPN Router or Privacy Appliance](#)
- Expanded the [Browse the Web Privately](#) chapter with more information on [Browsers You Should Avoid](#) and [Browsers You Should Consider](#); advice on what to do [If You Have to Use Chrome](#); a new topic, [Say No to Selling Your Personal Info](#); additional information on [Private Browsing Modes](#); and revised advice on how to [Block Ads](#) and [Search Privately](#)
- In the [Improve Email Privacy](#) chapter, added the topic [Use Burner Addresses](#)
- Greatly revised [Manage Your Mobile Privacy](#), including new discussions of [Spear Phishing and Impersonation](#) and [Spyware](#)
- Beefed up [Keep the Internet of Things Private](#) with more information on [Smart TVs and Streaming Devices](#) and [Smart Speakers](#)
- Deleted the chapter “Share Files Privately” as it was out of scope for the book’s current direction

Introduction

“A book about online privacy? That’ll be pretty short!” my friend joked. It was his way of saying, “We both know there’s no such thing as privacy on the internet.”

He’s not far from the truth, but to be fair, the illusion of privacy extends far beyond the world of computers and networks.

If you want complete privacy, go live in a remote cave without any electronics. Don’t build a fire, because the smoke could give away your location. Never step outside, because a satellite or a passing drone might snap your picture. And avoid all human contact, because you never know who might be a spy. I hope you packed plenty of food, water, and clothing, too—you won’t be getting any more!

In other words, there’s essentially no such thing as total privacy, online or otherwise. People have to interact with each other to survive, and every interaction reveals something about each participant.

I don’t know about you, but I wouldn’t want it any other way. I like having family and friends who know me well, and who can get in touch with me whenever they want to. And I like the convenience of using my computer, phone, or tablet to communicate, find directions, and make purchases anywhere in the world. All these things involve revealing information about myself, so I wouldn’t want *complete* privacy.

And yet, the internet turns many of our everyday assumptions about privacy upside down. If I’m at home, I can close the curtains and feel reasonably confident that whatever I say or do inside my house won’t be seen or heard by anyone else unless I choose to reveal it. Not so with electronic communications. Whether I’m sending email, browsing the web, or doing a video chat with a friend, the only safe assumption is that strangers *might* be able to see that information—now or in the future.

Once something has traveled over the internet in any way, it’s potentially out there forever—and potentially public. I like to say, *What happens on the internet, stays on the internet*. You can delete a file

from your computer, but once data has gone into the cloud, there's never a guarantee that all copies of it have been eternally expunged. In fact, it's far more likely that any given piece of data on the internet will live on indefinitely. Not only that, but data tends to escape even strong restraints—hence the saying “information wants to be free.”

To be brutally honest, someone who wants badly enough to learn what you've transmitted or received on the internet can probably do so, given enough time, effort, and skill. Part of the reason for this book is to explain how your words, personal information, and activities could become known to individual strangers or even the public—and that knowledge may lead you to make different choices about how you use the internet. But I'm not saying you must give up any hope of basic privacy. On the contrary, common-sense strategies—the internet equivalent of drawing the curtains and locking your door—can significantly reduce the risk of having your personal information fall into unwelcome hands. And, when you have more sensitive or valuable data to protect, you can take appropriately stronger measures.

Of course, there are trade-offs—you may lose convenience, valuable social interaction, and even (paradoxically) personal safety if you choose to keep certain information private. For example, the same technology that can reveal your location to advertisers could also help someone trying to rescue you during a natural disaster or other emergency. Privacy cuts both ways. That's why I don't recommend attempting to lock down all electronic communication, all the time. You need the curtains open to see the sunlight, and you need the open internet too.

Since the previous edition of this book was published in 2019, new threats to online privacy have emerged, but so have new tools to protect yourself. As a result, I've thoroughly rethought and reworked my advice to reflect what's possible and reasonable in 2024.

This book isn't a guide for the paranoid—or for people with outrageously sensitive or scary secrets to protect. It's a book for ordinary people with ordinary privacy needs. You want to go about your business, enjoying the many benefits of modern technology without worrying that someone is snooping on you—whether to sell you something or for more sinister reasons. That's what I'll help you do, regardless of

whether you use a Mac or PC, iOS or Android device, smart TV, or any of a thousand other network-enabled gadgets.

I focus more on general principles than on nitpicky settings, particular apps, or elaborate technological rituals. I offer examples and pointers to more information as appropriate, but I don't dwell on minutiae. The lack of detailed, step-by-step instructions may come as a surprise to some readers, so let me spell out my reasons:

- Privacy settings are a matter of choice. There's no single right answer; each person's decisions about what information to keep private and how to do so will be different from the next person's.
- Each app, website, operating system, and device has its own way of doing things. Spelling out how to configure the privacy settings in every email client, web browser, telephony app, and other internet-connected software—on every version of macOS, Windows, iOS, Android, and other operating systems—would take hundreds of dull pages. And all those instructions would go out of date as soon as the next software or hardware update appears!
- I don't want to give you a false sense of security. Although you can certainly take steps to dramatically increase your privacy, I don't want you to think that some magical combination of software and settings will keep your online activities completely and permanently private. Knowledge and vigilance go a long way, however.

Think of this book as a primer on the things that affect your online privacy. It tells you what's going on, how it pertains to you, and why you might care. More than that, it puts privacy issues in perspective. If you feel overwhelmed by privacy concerns, you can take control of your online privacy by replacing paranoia and guesses with knowledge and smart choices.

Because I live in North America, most of my examples involve things I know or suspect to be the case here. But even though laws and policies vary from country to country, nearly everything I say here is applicable in some fashion to anyone in the world.

Online Privacy Quick Start

You can think of this book as being divided into general topics (the first four chapters) and specific topics (the rest). I recommend that you read the first four chapters before you do anything else in order to understand your overall privacy risks and the simple, preliminary steps you can take to reduce them. Then feel free to skip to whichever other chapters are of particular interest.

Identify your online privacy needs:

- Discover the (mostly negative, but occasionally positive) developments in the ever-changing world of online privacy in [Understand the Evolving Online Privacy Landscape](#).
- Think you have nothing to hide? Think again. Find out what you have to hide, who might be trying to invade your privacy, and why. See [Learn About the Risks](#).

Take preliminary steps:

- Come up with a plan to deal with most common privacy issues in [Develop a Privacy Strategy](#).
- If you're an Apple user (or think you might like to become one), be sure to read [Discover Apple-Specific Privacy Features](#).

Use online services privately:

- Social may be another way to say “public,” but you need not give up all your privacy when using Facebook, X, and other social networking services. See [Confront the Social Media Threat](#).
- Block the broadest and most likely privacy risks. See [Keep Your Internet Connection Private](#).
- Surf and shop without compromising your personal information. Read [Browse the Web Privately](#).
- Reduce the chances that email will be read by anyone other than the intended sender and recipient. See [Improve Email Privacy](#).

- Reduce the chances of eavesdropping when using instant messaging and other audio, video, and chat services. Read [Talk and Chat Privately](#).

Use devices other than computers privately:

- Learn about the extra steps you may need to take while using your mobile phone or tablet. See [Manage Your Mobile Privacy](#).
- Find out about the privacy implications of streaming boxes, internet-connected cameras and home automation products, as well as other “smart” objects. See [Keep the Internet of Things Private](#).

Help others with their online privacy:

- If you have children, you have the additional responsibility to take control of their online privacy. See [Maintain Privacy for Your Kids](#).

Understand the Evolving Online Privacy Landscape

Before we get into the nuts and bolts of online privacy, I wanted to step back for a moment and look at how the online privacy story is changing—partly for the good, but mostly not. Although everyone should be aware of these facts, they’re especially important for people who read earlier versions of this book and wanted to know what has changed.

I wish I could tell you that you can take a simple series of steps that will protect all your private data forever. I wish, especially, that I could tell the people who read the first edition of this book back in 2013 that the steps they took then are still sufficient. But online privacy is a moving target, and in the past few years things have changed dramatically. You can’t treat privacy as a set-it-and-forget-it thing. You must remain informed and vigilant (see [Keep Yourself Informed](#), a bit later).

On the plus side, there has been some good news. For example:

- More and stronger privacy laws have come into effect; see [Privacy Laws Are Changing](#), later in this chapter.
- As a result of the many public scandals, lawsuits, government inquiries, and major news stories about privacy issues, the public is becoming more aware of their need for privacy—and tech companies are, at least somewhat, responding to the resulting demands for more and better privacy controls.
- Apple keeps expanding their array of privacy tools and features, especially when using apps like Safari, Mail, and Messages. See [Discover Apple-Specific Privacy Features](#).

But the challenges are even more numerous, and I want to catch you up with the latest facts. I’d like to begin, if you’ll indulge me, with a brief sermonette about the rampant addiction to free stuff and what that has to do with your privacy.

The Curse of Free Stuff Continues

Imagine someone makes you an incredible offer: You can live in a nice, big house for free, indefinitely. All utilities included! The house is fully furnished and ideally situated in the middle of a dense urban center, close to everything. And you won't pay a penny.

Just one little detail: the house is made of glass.

Every bit of the house, including floors, ceilings, walls, and even furniture, is transparent. Curtains of any kind are forbidden. Everything you do inside the house will be clearly visible, all day and night, to the crowds outside.

But, again: it's free. Do you take the offer?

Perhaps your reaction is revulsion. Who would want to be on display like an animal in a zoo? Surely your privacy is too high a price to pay for a free place to live.

And yet, I'll bet you know what I'm going to tell you next: you've already taken that deal. You have already traded away your privacy for free stuff—stuff that's far less valuable than a place to live—countless times. That “free” email account, those “free” web searches, the “free” videos you watch and articles you read, and countless other things you consume with barely a thought are free *only* because they're paid for with extensive, personal details about what you do, where you go, what you say, what you buy, and so on.

As the oft-repeated saying goes, “If you're not paying for it, you're the product.”

We've all convinced ourselves that the exchange of privacy for free stuff is not only normal, it's inevitable. We do it because that's what everyone else does, and because we don't realize we have a choice.

You might be able to go about your life normally, oblivious to all the information about you that's being collected and circulated, until something goes wrong. Someone steals your money or your identity, harasses you online, or threatens your livelihood—all because some of

Learn About the Risks

As I've said already and will say again, I don't think it's helpful or appropriate to be paranoid when it comes to online privacy. I don't want you to live in fear, or to worry that the slightest misstep online will ruin your life. Instead, I want you to have a clear understanding of the facts.

This chapter provides an overview of what you *might* risk merely by using the internet in some way. That "might" is important, because so many variables are involved. We've all known people who rode bikes without wearing helmets and still managed not to suffer had injuries, or who smoked their entire lives and never got cancer. The same applies here: some people get away with online behavior I'd consider ill-advised. It's also true that some people have greater risks than others (see [Your Risk Profile](#)) and that some things are beyond anyone's control (see [What You Can't Control](#)). You can choose to do with this information whatever you like, but my view is that forewarned is forearmed.

Learn What You Have to Hide

I'm sure you're an honest, moral, law-abiding citizen. Good for you! But if you tell me you have nothing to hide, I'm going to laugh in your face. I'm sorry, but "I have nothing to hide" is an absurd statement, no matter who's saying it. Of course you have things to hide! We all have secrets, and that's as it should be. But you may not realize how much you want to keep private and how you might inadvertently give it away online.

Privacy nearly always depends on context. You may want to keep certain information from your employer but not your doctor; you may want to tell your spouse things that you wouldn't tell your kids; you may share information freely with your lawyer that you would prefer not to have repeated in court. Later, in [Learn Who Wants Your Private](#)

[Data \(and Why\)](#), I further explore that part of the question—private *from whom*? You can't keep all information private from everyone (and you wouldn't want to), but you can take steps to keep some information private from some people.

Things You Might Want to Keep Private

If you'll indulge me for a moment, I'd like to run down a list of some categories of information you probably want to keep private in the sense of controlling who it's shared with online. This is in no way intended as a complete list, but only as a few highlights:

- **Contact information:** You may hand out business cards freely, but are you willing to let any stranger know your name, telephone number, and home address? (Some people don't mind at all, but others find it problematic.) You enter this information nearly every time you make a purchase online, and in many other situations. The address book on your computer or mobile device may also include contact details for numerous *other* people, including some who may be sensitive about their data becoming public knowledge. So it's not only your own contact information you need to keep private.
- **Vital statistics:** Personal facts such as your date and place of birth, the names and ages of your parents and children, and your marital status are probably well-known among family and close friends. In the wrong hands, that data could help someone hack into your accounts, steal your identity, or even blackmail you. And yet, you've probably revealed much of this information on Facebook.
- **Location:** Unless you take deliberate steps to prevent it, the mere act of turning on a mobile phone or visiting a website on your computer can reveal your physical location, sometimes down to your street address. This information may be stored, too, such that your movements and online activity over time can be mapped out—and that, in turn, can often suggest what you have been doing in all those locations, or even with whom you've been doing it. Do you mind that someone you don't know can tell where you are now, and where you've been in the past?

Develop a Privacy Strategy

Online privacy is, as you now know, a complex problem with no definitive solutions. But it doesn't have to be overwhelming. In this chapter, I help you think through a high-level strategy you can use to inform your decisions about specific tasks such as web browsing, email, and messaging (all of which I cover later in the book).

Here are the major suggestions I make in this chapter:

- First, read [What I Wish I Could Tell You](#): an overview of the five things that, if you *could* do them, would do the most to improve your online privacy—but they all come at a cost.
- Next, [Create Privacy Rules for Yourself](#). These simple statements focus on a few types of information you always want to take extra care with and a few people you always want to communicate with privately.
- [Remove Your Info from Google](#) to keep as much private information as you can out of the world's biggest advertising powerhouse.
- Although it requires both time and a frustrating amount of effort, I now also recommend that you [Purge Your Info from Data Brokers](#) to the extent possible.
- On occasion, you may have to [Cope with Special Cases](#). Troubling situations may come up that require extra privacy but for which you don't have an existing system. Think through the possibilities in advance and prepare so you don't make a foolish decision on the spur of the moment.
- For extra credit, [Take the Pledge](#): promise me, yourself, and the rest of the world that you won't do stupid things online.
- [Keep Yourself Informed](#) about the ever-changing risks to your privacy (and tools to help you protect it).

What I Wish I Could Tell You

Here we are, about a quarter of the way through a fairly lengthy book about online privacy, and I can't help but think: I could make this all so much easier. I could save you the time and effort of reading the rest of this book and working your way through dozens of additional steps by boiling down my advice to essentials. I could tell you how, by doing just five "simple" things, you could eliminate the vast majority of your online privacy risks and be done with it.

Problem is, every one of those things comes with a BUT. You're going to say, "Oh no. I couldn't do *that* because..." And you're not wrong. That's why I can't actually tell you to do these five things. If I *could*, here's what I'd say:

- **Ditch Facebook:** As I discuss in detail later (see [Learn About the Facebook Problem](#)), I consider Facebook (along with Instagram and Threads, all owned by Meta) to be the number-one threat to your online privacy. Your data would be so much safer if you deleted your Facebook, Instagram, and Threads accounts. Meta also owns WhatsApp, though it poses a lower privacy threat.

BUT: Some people genuinely depend on Facebook and have no reasonable alternatives.

- **Shun Google:** Stop using Google for web searches (see [Search Privately](#)). Replace Chrome with a better browser. Switch from Gmail to a more secure and privacy-friendly email provider. Choose from the many alternatives to Google Drive, Google Docs, Google Photos, and all the rest. Find videos somewhere other than YouTube. Use an iPhone rather than an Android phone. If you keep your distance from all Google properties, you significantly reduce the amount of data Google collects from you.

BUT: Even though alternatives to Google services exist, you may not always have a choice. Plus, millions of websites embed Google resources of various kinds (fonts, videos, and so on), and even if you never deliberately visited a Google site, the company could still

Discover Apple-Specific Privacy Features

Apple [makes a big deal](#) about the superior privacy of their devices and operating systems. To be sure, some of that is just marketing, because other devices and operating systems also have good privacy measures built in, even if they're not quite the same as what Apple offers. But it's also true that Apple is unique among big tech companies in making the vast majority of their money from selling products and services rather than from advertising. And, by making privacy part of their brand, they're hoping you'll trust them enough to keep buying expensive gadgets from them. Thus it's in Apple's financial interest to (mostly) protect your privacy, even if it's not entirely for altruistic reasons.

Apple's [Privacy Control](#) page lists many, but not all, of Apple's privacy-related features, and it's worth reading. That page lists even some features I don't cover in this book, but I want to call your attention to a number of tools that do in fact give Apple users significant privacy—as long as you know how to enable and use them.

Sign in with Apple

When you visit a website that asks you to create an account, you can generally supply your email address and a password to do so. But many sites let you use your account from a different site (such as Google, Facebook, or GitHub) to sign in. Apple is another of these providers, via its service called Sign in with Apple. Provided that you've enabled Apple's two-factor authentication, if you're using Safari and visit a site that supports this service, you can click a button or link, supply your Apple Account credentials, and let Apple create a random email address and password for you. The credentials are stored automatically in iCloud Keychain, and Safari can autofill them for you on your next visit.

Note: Although Apple’s service is similar to those provided by other sites, some observers, including Wired, think [‘Sign In With Apple’ Protects You in Ways Google and Facebook Don’t](#).

If the site sends email to the randomly generated address, Apple forwards it to you. But because the site doesn’t know your actual address, you have a layer of anonymity. (Of course, if you later supply your real name, address, or other personal information to the site, you lose that anonymity; the only fact you withhold is your real email address.) If you start receiving spam from the site, you can disable the address. (Manage this data in Settings/System Settings > *your name* > Sign In & Security > Sign in with Apple.) For more details, read Apple’s [How to use Sign in with Apple](#) page.

Just one word of caution. In order to reduce spam, Apple forwards *only* email messages that come from the domain you signed up with. But sometimes a company uses multiple domains or passes your information along to a different entity for legitimate purposes—in which case, email sent to you from another domain would be discarded without any notice to you. (This can be a particular problem with sites like Kickstarter and IndieGoGo, which pass on your information to the creators you fund and let those creators email you from their own domains.) In such cases, you may instead opt to use Hide My Email (covered next), which requires a couple of extra steps but won’t restrict forwarded email by domain.

Hide My Email

Starting in macOS 12 Monterey and iOS 15/iPadOS 15, Apple extended the [Sign in with Apple](#) concept to work anywhere—not just in Safari, and not just on websites. Instead, as long as you’re a paid iCloud+ subscriber with Apple’s two-factor authentication enabled, you can use your Apple device to create a random email alias whenever you like and use it for any purpose. On a Mac, you can create these in System Settings > *your name* > iCloud by clicking Hide My Email (in Sequoia or later) or the Options button next to Hide My Email (in Sonoma or

Confront the Social Media Threat

At the risk of stating the obvious, *social* implies interaction with other people, which is somewhat at odds with privacy. On the internet, it's best to think of "social" as synonymous with "public" (even though that's not necessarily true), because once you've shared something online—in any of a hundred senses of sharing—whoever you've shared it with can, in turn, share it with someone else. And, since most social media is ad-supported, both the services themselves and the advertisers that pay to promote their stuff on them would like to know as much about you as possible—again, a situation hard to reconcile with any definition of privacy.

As a result, the very best advice I can give you about privacy when it comes to social media is *not to expect any*, regardless of your privacy settings. You may imagine that the things you post or tweet are just between you and your friends (or "friends," as the case may be), but that's optimistic at best. Instead, assume anything you put online using social media—including chats and private messages on Facebook, direct messages on X, and profile details such as your name, location, and date of birth—could be discovered by anyone, and could be online forever. If you're unwilling to make any of that information public, don't share it in the first place.

However, there are still better and worse approaches to social media, and you should know how to protect yourself to the extent possible.

Understand the Privacy Risks of Social Media

Wait, didn't we just cover that? Yes, any data you put online using any social network can potentially become public. I know you know that.

What I'd like to emphasize here is how that could be a problem for you.

As I mentioned early in this book, everyone from [Local Villains](#) to [Big Data](#) can easily find you on social media. You might be astonished how much private data could be culled from years of Facebook updates and likes, tweets, LinkedIn updates, Instagram pictures, Yelp reviews, YouTube comments, blog posts, and a long list of other social media activities.

It's easy to discover not only basic facts about you and your family but also where you've been, who you hang out with, which causes you support, what your political and religious beliefs might be, and, perhaps most important of all, *what sort of person you are*. Even if no individual statement tells the story, the combined data from all these sites and services can do something akin to browser fingerprinting (see [On a Web Server](#))—it can often paint a vivid and surprisingly precise picture of you. So...

- If you're trying to get a job, a prospective employer may use social media to determine whether you're likely to be trustworthy, polite, punctual, and loyal—and to see how you've behaved in other jobs.
- If you're applying to a college or university, admissions officers may use online profiles to judge your seriousness and confirm any personal details you've submitted.
- If you're dating, someone thinking about starting a relationship with you could also learn a lot about your tastes, biases, character, and history with previous partners.
- If you're ever suspected of a crime, the police or prosecutor could scour social media for evidence of bad behavior—or a defense attorney could try to demonstrate a pattern of selflessness.
- If you ever get involved in politics (national, local, academic, or any other kind) or run for political office, anything you've ever said online can and will be used against you by your opponents. (Whether that proves effective or not is another question.)

Keep Your Internet Connection Private

Whether you're on a Wi-Fi, cellular, or wired connection, keeping your *link* to the internet private is an important step that affects all the other traffic your devices send and receive—web, email, video, and everything else. In this chapter I discuss some of the ways in which another person or company could eavesdrop on your internet activities or even misdirect you into connecting to bogus sites in order to steal information from you. Then I describe steps you can take to reduce the most serious of these risks.

Understand the Privacy Risks of Your Internet Connection

The connection between your device (computer, smartphone, streaming box, etc.) and a server (web server, email server, streaming video server, etc.) may involve numerous steps. For example, your laptop may connect to a wireless router via Wi-Fi, which then connects to a cable modem via Ethernet, and then to your ISP over coaxial or fiber-optic cable. Your ISP, in turn, sends requests for data through a series of routers and network operators until they reach the desired destination. The simple act of visiting a webpage can involve requests going back and forth between dozens of routers and servers all over the world.

So, although you may have the impression that your computer is talking “directly” to a server somewhere, that’s almost never the case. Internet connections, by their nature, are indirect. And at any point between your device and the remote server, the data could be monitored or intercepted.

To get the bad news out of the way first, let's look at some of the likely trouble spots:

- **Wi-Fi connections:** If your device connects to the internet wirelessly, as most do, someone nearby (even in another building) could “sniff” the Wi-Fi signal and watch or record all the data transmitted and received. This is easy to do when Wi-Fi connections are open, or unencrypted, but even encrypted connections can be unsafe. An early security method called WEP is trivially easy to break—fortunately, it's rarely used these days. A replacement standard, called WPA2, is much better, but still crackable. And while the newest generation of Wi-Fi encryption, [WPA3](#), is more secure, it has only begun to appear in consumer devices in the past few years.

A compromised Wi-Fi connection can lead to not only passive snooping but also active attacks. For example, a [man-in-the-middle attack](#) is one in which two parties think they're communicating directly but are instead manipulated into channeling their data through a third party, who can monitor and alter it in transit. (A man-in-the-middle attack can occur anywhere, but it's especially easy to perpetrate on an open Wi-Fi network.)

If I used a man-in-the-middle attack on an instant messaging conversation, I would see what each party types, but they would see only what I relay—which may or may not be exactly what the other person said. (See [this photo](#) on Reddit for a humorous illustration.)

- **Cellular connections:** The cellular data connection between your phone or tablet and your ISP can be monitored and intercepted. Unless you work for the carrier (which can presumably monitor anything that's not encrypted), doing so requires the use of specialized equipment and skills. It's not something a kid in a coffee shop is likely to pull off, but it's certainly within the capabilities of law enforcement and sophisticated operations. (See [Manage Your Mobile Privacy](#) for more on this topic.)
- **DNS disruptions:** DNS (Domain Name System) servers translate domain names (such as [apple.com](#)) into IP addresses (such as [17.149.160.59](#)). But if your device were tricked into using the wrong

Browse the Web Privately

In the previous chapter, I told you how to keep your connection to the internet private. That can close quite a few holes that might put your privacy at risk—but even if you do all that, as soon as you open a web browser, new risks emerge.

Simply browsing the web reveals a great deal about you personally, your computer, your location, and your habits. There are many steps you can take to reveal less about yourself, although some entail a loss of convenience. Never is this more the case than when shopping on the web. This chapter explores the risks, the measures you can take to avoid them, and certain negative consequences of those measures.

Understand the Privacy Risks of Web Browsing

Assuming you've taken *all* the steps in [Keep Your Internet Connection Private](#), browsing the web privately comes down to two main things:

- Preventing information about your browsing activities from being stored on your own device (see [On Your Device](#))
- Preventing the sites you visit (including search engines) from collecting information that can identify you personally (see [On a Web Server](#))

(If you have *not* taken all the necessary steps to secure your internet connection, there's a third factor to worry about—having information intercepted in transit on its way to or from a website you visit. We'll come back to that momentarily, in [In Transit](#).)

These categories are often misunderstood, and your actual risk may be greater or less than you imagine.

If information is stored on your computer, it's available to anyone who has physical or network access to your computer (assuming it's not

protected in some other way, such as by using full-disk encryption or keeping it in a locked cabinet). To use the obvious example, your spouse, roommate, or employer might peek at the list of websites you've visited when you're not looking. But some of this stored information, including cookies (see [Live Data](#), later in this chapter), is *also* available to advertisers and other online entities as you browse the web. One person may not care whether someone in their home or office sees what's on their computer, but may have a principled objection to advertisers knowing about their browsing habits. For another person, the opposite may be the case—advertisers might be irrelevant, but it would be problematic if a family member, coworker, or (let's just say) the FBI found out what sites they've visited.

Even if your computer is squeaky clean, every site you visit may record what pages you've read, what search terms you've entered, and much more (see [On a Web Server](#), ahead). Unless you've logged in to a site with a username and password, it probably won't know who you are by name, but the other information the site logs could very well be enough to identify you uniquely, given sufficient effort and ingenuity.

Finally, all information moving in either direction between you and a website could be intercepted in transit. If you use an encrypted Wi-Fi connection, you eliminate one avenue that could be used to eavesdrop on your web surfing. If you activate a VPN, you eliminate another. And if you connect to a site that uses HTTPS (as nearly all do these days), you reduce the likelihood of in-transit eavesdropping to the point that most of us need not worry about it at all. In the absence of any of these protections, I'd be extremely hesitant to enter or view any sensitive personal information on the web.

That's a long list of risks. But before freaking out about all the potential privacy risks of web browsing, remember to ask yourself what data you're trying to keep private, and from whom. Do you care what someone could find if they had physical access to your computer? Do you care what advertisers know about you? Both? Neither?

If you're downloading stuff or doing things online that could lead to jail time, a lawsuit, a divorce, losing your job, or a combination thereof,

Improve Email Privacy

When we began discussing this book, former Take Control publisher Adam Engst told me that his rule is, “don’t write anything in email that you couldn’t stomach appearing on the front page of the *New York Times*.” I said I didn’t think that was a very good rule, and we discussed it (by email, naturally) in what became an increasingly contentious debate. I won’t repeat the entire exchange here, because I’m sure you’ll read it soon enough in the *New York Times*.

But to summarize, Adam was trying to make the point that you can never have an ironclad guarantee of privacy when it comes to email. In that respect he’s absolutely right, for reasons I’ll explain in a moment. My point was that in many cases, email is the only practical means of communication, and yet it’s completely infeasible for me to avoid ever sending personal facts, business secrets, colorful language, or anything else by email that wouldn’t cause serious problems if made public. I think I’m right about that, too.

But email privacy is extraordinarily difficult to achieve, and the more control you try to exert, the more cumbersome it becomes. By the end of this chapter, you should have a better appreciation of what makes email privacy so tricky. But you’ll also learn how to keep most email safe from casual snooping, how to make top-secret email messages as private as they reasonably can be, and when it’s best to choose an entirely different means of communication.

Understand the Privacy Risks of Email

If you send me an email message, you might have the impression that you and I are the only two people who can read it. Such assumptions are unwise. Let’s look at a few of the places email might be visible to someone other than the sender or recipient:

- **On your end:** Your email client may keep a copy of the messages that you send. If so, anyone who gained access to your device

(including thieves and people reading over your shoulder—not to mention your employer) could see what you’ve sent. And, if you have more than one device logged in to the same email account, each device could include a copy of each of your sent messages.

- **In transit:** At minimum, an email message must travel from the device where you compose it to a server, and from a server to the recipient. (If both you and the recipient happen to use the same email server, no further hops are required, but usually messages go to an outgoing email server and then take one or more steps over the internet to the recipient’s email server.) An email message could be intercepted along any segment of this journey—for example, by someone “sniffing” an open Wi-Fi network, or by ISPs, corporations, or government agencies monitoring a router. As I’ll explain shortly, the message data might be encrypted during part of its journey across the internet, but you can’t count on this, even if you use TLS/SSL to communicate with your email server.
- **On email servers:** The email server you connect to in order to send a message may hold onto that message only for as long as it takes to send it, and then delete it. Or it may cache the message for much longer—even indefinitely. Unless you run the email server yourself, you have no way to know for sure. (And trust me, you *don’t* want to run your own email server—I’m speaking from experience.) Once it reaches the recipient’s email server, it’ll stay there at least until the recipient reads it, but more likely it’ll stick around forever, because most modern email systems work best when the server stores the master copies of incoming messages, which then sync to client devices. In any case, for however long the message is on a server somewhere, anyone with access to that server could conceivably read the message without you or the recipient ever knowing.

Note: Barring a sealed wiretap order, U.S. state and federal governments typically need a search warrant to access *unopened* email stored online for 180 days or less—older unopened messages can be obtained with a (simpler) subpoena. But don’t assume anything is off limits; the laws are murky enough that any message on an email server could be fair game.

Talk and Chat Privately

I am old enough to remember the days when, if someone wanted to converse with another person who wasn't nearby, both people would talk into analog devices called "telephones" to have real-time audio conversations. Perhaps you've seen such devices in old movies or read about them in antique documents called "books."

I kid, but analog telephones are rapidly becoming extinct. These days, it's normal to have only a mobile phone, not a landline, and even if you do have a landline, it's probably not POTS (plain old telephone service) but rather a VoIP (voice-over-IP) telephone service offered by your phone, cable, or internet provider or a third-party company such as [Vonage](#). (If your phone connects to a box with a network connection, rather than simply to a jack in the wall, it's VoIP.)

You almost certainly own a smartphone, of course. But, for most of us, actual audio telephone calls are increasingly rare; we're more likely to use an app such as FaceTime, Messages, SnapChat, Skype, Slack, Telegram, WeChat, or Zoom for audio, video, and text chats. That's equally true when we're using computers and tablets. Xbox, PlayStation, and Nintendo game consoles all support messaging and voice chat too.

The question is: How private are any of these real-time communication services?

Understand the Privacy Risks of Real-Time Communication

One of the best ways to acquaint yourself with the risks of real-time communication is to watch the HBO TV series [The Wire](#). Yes, all five seasons. (Go ahead and do that, if you haven't already, and then come back to this page.)

I've mentioned *The Wire* because a lot of it has to do with electronic surveillance (hence the name)—but the main target of this surveillance is ordinary mobile phones. On the show, law enforcement agents need both special equipment and legal permission to monitor the mobile phone use of suspected criminals. But the process ultimately poses little technological challenge, and the people being monitored have no way to know their conversations aren't private.

Now, think about that and consider the fact that monitoring real-time communication over the internet is potentially *easier*. And, although government and law-enforcement entities have greater access to this sort of data than ordinary citizens, professional hackers and even casual snoops likely have the capability to see (or hear) far more of this data than you might suspect.

As with everything else I've discussed in this book, precisely what that means to your personal privacy depends on what you say and to whom, but in principle there's almost no limit to your potential risk. However, let me now backpedal a bit and point out a few mitigating factors:

- Audio data is more difficult to store and analyze than textual data, and video data poses a bigger challenge than audio data. Due to the inconvenience of dealing with such large amounts of data, it's slightly less likely that audio or video calls will be kept or searched than email, text messages, or chats. Of course, if your VoIP connection were compromised, a computer could transcribe every word of a conversation and turn it into searchable text without having to store the audio or video. So although there are no guarantees, on the whole, I consider voice and video communications over the internet to be marginally safer than any sort of text-based communication.
- The previous point notwithstanding, available technical details and anecdotal reports suggest that Apple's encrypted iMessage service—which can be used for text messages and file transfer among Macs, iPhones, and iPads—is highly resistant to hacking and eavesdropping. (See the sidebar just ahead for more information.) Other secure messaging services include:

- ▶ [KeeperChat](#)

Manage Your Mobile Privacy

Everything I've discussed so far about online privacy applies when you're using a computer to access the internet. Your smartphone or tablet is *also* a computer that can connect to the internet, and I've called out a number of issues that affect mobile devices as much as their desktop counterparts (including private web browsing and email access) But mobile devices pose additional, unique challenges:

- Smartphones—along with some tablets and smartwatches—connect to cellular data networks, which give mobile carriers additional tools to track users' behavior, such as [Supercookies](#).
- Apps try to access all kinds of data on your device; some of it is for legitimate purposes, and some not. You can control which app can do what; see [Granting Apps Access Permission](#).
- Because your mobile device is much more likely than your computer to be with you all the time, the fact that it (and, by extension, other entities on the internet) can determine your physical location can become a problem. See [Location Awareness](#).
- Your mobile device is also a camera! In fact, it may be your main camera. If you take photos or videos of anything, *ahem*, sensitive in nature, you now have to think about whether or under what circumstances they might be automatically uploaded to the cloud. I talk about that in [Photos and Videos](#).
- Your mobile device is also a short range radio! Although it's becoming less likely that Wi-Fi and Bluetooth signals will identify you uniquely, their mere operation can be aggregated into larger profiles based on location, timing, behavior, and other factors.
- [Spear Phishing and Impersonation](#) are ways of stealing information or money that depend on the attacker having gathered some per-

sonal information about you in advance, and your mobile device is likely to be part of that attack.

- Your mobile phone could be infected with [Spyware](#) that snoops on your location and activities even if you haven't taken any action, such as installing an app or clicking a link.
- Do you back up the data on your mobile device? I hope so! But some methods of backup could inadvertently expose your private data to hackers. Read [Mobile Backups](#) for details.
- If you're traveling across international borders, all your electronics—but especially your mobile devices—may be subject to scrutiny, putting your privacy at risk. See the sidebar [Privacy and International Travel](#) to learn more.

Note: In this book I've largely assumed that you have either an iPhone or an Android phone, and thus are running a mobile operating system from Apple or Google. In fact, there *are* other options, and although I can't get into the details in this book, you may find the Wired article [/e/OS Is Better Than Android. You Should Try It](#) interesting reading. The article also mentions other alternative mobile operating systems for non-Apple phones, such as [GrapheneOS](#).

Supercookies

When your smartphone or tablet happens to be connected to a Wi-Fi network, the same rules apply as for any other device—for example, make sure you're using encryption wherever possible, connect via a VPN if you have to access sites without encryption, and consider using a third-party DNS server (see [Prevent Snooping](#)). But when you're using your carrier's cellular network (LTE, 4G, or whatever), you have to worry about an additional problem.

Back in 2014 the public learned that two large mobile carriers in the United States—AT&T and Verizon Wireless—had been using a technology nicknamed *supercookies* to track all the websites users visited while using their mobile phones on cellular networks and sell that data

Keep the Internet of Things Private

Computers, smartphones, and tablets aren't the only devices that connect to the internet. My television, Apple TV, HomePods, DVR, Blu-ray player all have internet connections too. So do game consoles and many newer scanners, printers, cameras, and storage devices. So do a wide variety of home-automation devices, including "smart" door locks, light switches, light bulbs, thermostats, outlets, garage door openers, security systems, and sprinklers. And appliances such as refrigerators, washers, and dryers. In fact, even objects as mundane as suitcases, bicycles, utility meters, and pet food dispensers may have radio transmitters and IP addresses. The list will only get longer and wackier with time.

Welcome to the Internet of Things—a truly horrid term for everyday objects that wouldn't normally be considered computing devices, but which nevertheless are accessible online. It's worth asking to what extent you need to worry about online privacy for those devices.

Smart TVs and Streaming Devices

Let's start with the first group—entertainment devices, including smart TVs and streaming devices hooked up to a TV, such as an Apple TV, Roku streaming player, or Amazon Fire TV Stick. (Such gadgets no longer go *on top* of your TV, the geometry of flat-screen televisions being what it is, but they're still sometimes called "set-top" devices.) Such products can tell providers and advertisers a lot about your tastes and interests. For example, if you stream videos from Amazon or Netflix to your TV, the provider knows what you watch and at what time of day; from this, they could attempt to deduce your age, gender, political persuasion, and whether there are any children in your home—as well as when you're home and when you're away.

That's just the start. Here are a few other ways a smart TV or streaming box might infringe on your privacy:

- A streaming box (or your TV itself) might include a camera and microphone for video calls, and your remote control might also include a microphone. These cameras and mics can be misused just like the ones on your computer (see [Mind Your Camera and Microphone](#))—without your knowledge, other people could see you and hear what you say in your own living room.
- Devices like Xbox Kinect can often accurately determine how many people are in a room, as well as their gender and even age.
- A Blu-ray or DVD player may send information about discs you play and features you use to online services such as [Gracenote](#), as well as to the manufacturer and its partners.

Furthermore, your privacy controls are typically much more limited than what you could configure with a computer. Most modern streaming devices support at least some VPNs, though you may have considerably less luck finding a VPN that runs directly on your smart TV. ([Consider a VPN Router or Privacy Appliance](#) to help with this problem—it can provide a VPN connection to all your devices, albeit with a speed penalty. But if video providers don't block you for using a VPN, they will still know who you are and what you watch because you must log in, so you're not gaining much privacy that way.)

As privacy concerns go, I have trouble working up much anxiety about smart TVs and streaming devices, and there's not much I could do about it anyway (other than stop using them). But you should at least be aware of the sorts of data you may be giving away. And if you're in the market for a new device in one of these categories, look carefully for any hints that the manufacturer offers you control over privacy settings—that's definitely a selling point.

Maintain Privacy for Your Kids

Everything else in this book has been about managing your own privacy. But if you're a parent of a young child, you have an additional challenge: maintaining your child's privacy. Speaking as the father of three (from elementary age to adult), this isn't as easy as you might think.

At a certain age, your child will begin making their own decisions about what to share online. I can't tell you what that age is or should be; I can only say it will be too young and you will likely be horrified at some of your child's choices. You'll have to sit down with your child and have the online privacy talk, which could be even more stressful than the sex talk. You'll try to lay down the law, but your child will push back and find ways around whatever controls you exert. Regardless of when and how this plays out, you should brace for the certainty that your child's online privacy will eventually be out of your control, and remember that kids always make poor decisions on their way to learning how to make good ones.

Note: In the United States, 13 is a "magic" age when it comes to online privacy. [COPPA](#) (Children's Online Privacy Protection Act) prohibits websites or online services aimed at children from collecting personally identifiable information from children under 13 without parental consent, a requirement that many sites meet by refusing to let younger kids have accounts at all.

I want to talk about what comes before then—the time between your child's birth and the moment you hand over the keys to the digital world. This is the period when your child's online privacy depends mainly on you, and the choices you make now can affect your child forever.

My mother has snapshots of me as a young child that were great for embarrassing me in front of college girlfriends, but the photos were kept in boxes or albums and dragged out only on special occasions. At worst, a girl might tell a story about a picture she'd seen, but she couldn't show anyone else.

But pictures don't work like that anymore. If you snap a cute shot of your young daughter in some comically brilliant situation, it's much more likely to go on Facebook or X than on paper in an album. A few years from now, her classmates will be able to see it. All her future friends, love interests, employers, and children will be able to see it—so will unsavory characters you'd like to protect her from. And anyone who sees it will be able to share it with anyone else in the world. Is there any possibility your daughter might live to regret your choice?

Everything you say about your child online—every picture and video, every story told or fact revealed—becomes part of your child's *permanent* internet record. You can't ever take it back, and you can't ever control how it might be used. And things that seem innocent now might cause all sorts of problems for your child in 10 or 15 years.

None of this means you should never talk about your child online or post photos or videos. It only means you should do so circumspectly and sparingly. You'll have to determine your own rules, but here are my tips:

- Never post anything online that could be used to predict your child's location (including a route to or from school), at least when a parent isn't around. This includes images with signs or landmarks in the background.
- No matter how cute your kid is in the bathtub, seriously, don't post any nude photos online. (You did [Take the Pledge](#), right?)
- Blog posts and other stories about your child's behavior problems might have far-reaching consequences. Keep it positive.
- Kids say and do the darnedest things, but even though your children's antics may entertain other adults, they could result in untold cruelty in the hands of a class bully a few years from now. Be super

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.

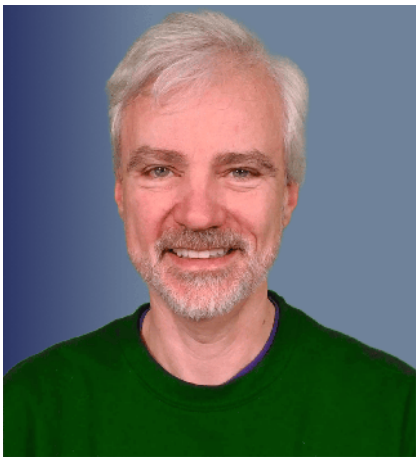
More Take Control Books

This is but one of many Take Control titles, and I'm just one of many Take Control authors! 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 Book 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 and Publisher



Joe Kissell is the author of more than 60 books about technology. In 2017, he also became the publisher of Take Control Books, when alt concepts—the company he runs along with his wife, Morgen Jahnke—acquired the Take Control series from TidBITS Publishing Inc.’s owners, Adam and Tonya Engst.

Joe previously wrote for TidBITS, Macworld, and Wirecutter (among other publications). Before he began writing full-time in 2003, Joe spent nearly eight years managing software development. He holds a bachelor’s degree in Philosophy and a master’s degree in Linguistics.

In his rare non-work hours, Joe likes to walk, cook, eat, and practice tai chi. He lives in Saskatoon, Saskatchewan, Canada, with Morgen and their sons. To contact Joe about this book, [send him email](#) and *please* include [Take Control of Your Online Privacy](#) in the subject. You can follow him on Mastodon ([@joekissell](#)) or Bluesky ([@joekissell.com](#)), or visit his personal website, [JoeKissell.com](#).

Credits

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

Also by Joe Kissell

Click any book title below to add more ebooks to your Take Control collection!

[*Take Control of 1Password*](#): Use this powerful password manager to create, store, enter, and sync personal data on all your devices.

[*Take Control of Apple Mail*](#): Learn the ins and outs of Apple's email app for Mac, iPhone, and iPad.

[*Take Control of Automating Your Mac*](#): Work more efficiently on your Mac with time-saving shortcuts of all kinds.

[*Take Control of Backing Up Your Mac*](#): Protect your Mac's valuable data from any sort of mishap.

[*Take Control of DEVONthink 3*](#): Master this powerful information management tool.

[*Take Control of iCloud*](#): Make the most of Apple's online service for storing, syncing, and sharing data.

[*Take Control of the Mac Command Line with Terminal*](#): Master your Mac's command-line interface and learn basic Unix skills.

[*Take Control of Sequoia*](#): Discover what's new in macOS 15, and get all the information you need to upgrade safely.

[*Take Control of Solving Mac Problems*](#): Learn how to maintain, troubleshoot, and speed up your Mac.

[*Take Control of Your Digital Legacy*](#): Make sure your important digital information is preserved for future generations.

[*Take Control of Your Paperless Office*](#): With your computer, a scanner, and this ebook, you'll finally eliminate the chaos of overflowing paper.

[*Take Control of Your Passwords*](#): Overcome password overload! Stay safe while eliminating the hassles and confusion of passwords.

Copyright and Fine Print

Take Control of Your Online Privacy, Fifth Edition

ISBN: 978-1-990783-50-0

Copyright © 2025, Joe Kissell. 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.